

KAUNAS UNIVERSITY OF TECHNOLOGY

MARTYNAS VAIDELYS

SELF-ORGANIZING PATTERNS IN
INFORMATION HIDING APPLICATIONS

Doctoral dissertation
Physical Sciences, Informatics (09P)

2018, Kaunas

This doctoral dissertation was prepared at Kaunas University of Technology, Faculty of Mathematics and Natural Sciences, Department of Mathematical Modelling during the period of 2013–2018.

Scientific Supervisor:

Prof. habil. dr. Minvydas Kazys RAGULSKIS (Kaunas University of Technology, Physical Sciences, Informatics, 09P).

Doctoral dissertation has been published in:
<http://ktu.edu>

Editor:

Armandas Rumšas (Publishing Office “Technologija”)

© M. Vaidelys, 2018

ISBN 978-609-02-1481-7

The bibliographic information about the publication is available in the National Bibliographic Data Bank (NBDB) of the Martynas Mažvydas National Library of Lithuania.

KAUNO TECHNOLOGIJOS UNIVERSITETAS

MARTYNAS VAIDELYS

SAVAIME BESIFORMUOJANTYS RAŠTAI
INFORMACIJOS SLĖPIMO UŽDAVINIUOSE

Daktaro disertacija
Fiziniai mokslai, informatika (09P)

2018, Kaunas

Disertacija rengta 2013–2018 m. Kauno technologijos universitete, Matematikos ir gamtos mokslų fakultete, Matematinio modeliavimo katedroje.

Mokslinis vadovas:

Prof. habil. dr. Minvydas Kazys RAGULSKIS (Kauno technologijos universitetas, fiziniai mokslai, informatika, 09P).

Interneto svetainės, kurioje skelbiama disertacija, adresas:
<http://ktu.edu>

Redagavo:

Armandas Rumšas (leidykla “Technologija”)

© M. Vaidelys, 2018

ISBN 978-609-02-1481-7

Leidinio bibliografinė informacija pateikiama Lietuvos nacionalinės Martyno Mažvydo bibliotekos Nacionalinės bibliografijos duomenų banke (NBDB).

ACKNOWLEDGEMENTS

I would like to express my special appreciation and thanks to my advisor Professor dr. Minvydas Ragulskis for the opportunity to work together, for encouraging my research and for allowing me to grow as a research scientist. Dear Professor, Your advice on research has been priceless, and Your guidance has been helping me during the time of research and the process of writing this thesis.

I am grateful to the staff of the Department of Mathematical Modelling for the opportunity to aspire to the PhD studies. I am especially grateful to Professor Dr. Vidmantas Pekarskas for directing me towards Prof. Ragulskis research group.

My deepest feelings and gratitude are sent to my wife, family and friends. Thank you for your patience, support and love.

I also wish to place on record my sense of gratitude to everyone and all whoever, directly or indirectly, have helped me during my research and writing of this thesis.

CONTENTS

1. Literature Review	12
1.1. Information Hiding Techniques.....	14
1.1.1. Cryptography.....	15
1.1.2. Visual and Dynamic Visual Cryptography.....	17
1.1.3. Steganography.....	19
1.1.4. Watermarking.....	21
1.2. Self-Organizing Patterns.....	22
1.2.1. Chaotic logistic map.....	23
1.2.2. Nonlinear Competitively Coupled Maps.....	24
1.2.3. Atrial Fibrillation Model.....	25
1.2.4. The Spiral Wave Model.....	27
1.3. Image Processing Techniques.....	29
1.3.1. Thresholding.....	30
1.3.2. Mapping Functions.....	30
1.3.3. Hyperbolic Tangent Contrast Enhancement.....	31
1.3.4. The Difference Image.....	31
1.4. Linear Recurrent Sequences.....	32
1.4.1. General LRS.....	33
1.4.2. 1-LRS over \mathbb{C}	33
1.4.3. 2D Sequences.....	34
1.4.4. The Order of a 2D Sequence.....	34
1.5. Concluding Remarks.....	35
2. Visual Information Hiding. The Use of Self-Organizing Patterns	36
2.1. Competitively Coupled Maps for Hiding Secret Visual Information.....	37
2.1.1. Self-Organizing Patterns.....	37
2.1.2. A Communication Scheme Based on Self-Organizing Patterns.....	38
2.1.3. Sensitivity of the Communication Scheme to the Perturbation of Parameters.....	41
2.2. Image Hiding Scheme Based on the Atrial Fibrillation Model.....	42
2.2.1. The Generation of Self-Organizing Patterns Based on Atrial Fibrillation Model.....	43
2.2.2. Initial Conditions.....	43
2.2.3. Parameters of the AF Model.....	44
2.2.4. A Communication Scheme Based on Self-Organizing Patterns.....	45
2.2.5. The Sensitivity of the Communication Scheme to Perturbations of System Parameters.....	48
2.3. Digital Image Communication Scheme Based on the Breakup of Spiral Waves.....	49
2.3.1. The Formation of the Difference Image.....	50
2.3.2. The Experimental Scheme.....	51
2.3.3. The Proposed Scheme.....	54
2.3.4. The Communication Algorithm.....	60

2.4. Concluding Remarks	62
3. Dynamic Visual Cryptography Scheme Based on Finite Element Grids	65
3.1. Image Hiding in Time-Averaged Moiré Gratings on Finite Element Grids..	66
3.1.1. Preliminaries.....	66
3.1.2. Deformable Moiré Grating; Nonlinear Deformation Field	70
3.1.3. Dynamic Visual Cryptography Based on Deformable Moiré Gratings on Finite Element Grids.....	72
3.2. Dynamic Visual Cryptography Scheme on the Surface of a Vibrating Structure	76
3.2.1. Optical Relationships.....	77
3.2.2. Ronchi-Type Moiré Gratings on Finite Element Grids	82
3.2.3. Dynamic visual Cryptography Based on Deformable Moiré Gratings on Finite Element Grids.....	83
3.3. Concluding Remarks	86
4. The Pseudo-Order of a 2D Sequence and the Complexity of Digital Images	88
4.1. Pseudo-Order of a 1D Sequence.....	88
4.2. Pseudo-Order of a 2D Sequence.....	89
4.3. A Synthetic Numerical Example	90
4.4. 2D Sequence Pseudo-Order of Self-Organizing Patterns	92
4.5. Optimal Time Period of Pattern Formation	95
4.6. Concluding Remarks	96
5. Conclusions	98
References	99
List of Author's Publications.....	109

SYMBOLS AND ABBREVIATIONS

ANN	Artificial Neural Network
AF	Atrial Fibrillation
BZ	Belousov-Zhabotinsky
DVC	Dynamic Visual Cryptography
FEM	Finite Element Method
HVS	Human Visual System
LRS	Linear Recurrent Sequence
LSB	Least-Significant Bit
MEMS	Micro Electro Mechanical System
SOM	Self-Organizing Map
SOP	Self-Organizing Pattern
VC	Visual Cryptography

Introduction

Relevance of the Work

The importance of hiding information when transferring data has been highlighted since the early days of communication. Even though initially information hiding was mainly used in military areas, the exponential growth and the widespread use of the internet in the public domain fueled the need to secure business, medical or personal data, money transactions, and other sensitive areas of information exchange. Depending on the information type, cryptography, steganography or watermarking techniques are used. They are usually interrelated with each other to ensure a higher level of security. In the areas where privacy, undetectability and confidentiality is required, steganography and visual cryptography take an important role. However, these techniques alone are prone to attacks as soon as the algorithm of encoding becomes public. Thus reliable, steganographically secure and fast-working information hiding techniques are required.

The complex self-organizing patterns emerging from the biological, chemical or physical processes have been successfully adapted for hiding and communicating secret visual information. The Beddington-DeAngelis type predator prey model with self- and cross-diffusion has been successfully employed in a secure steganographic communication algorithm. SOP induced by prisoner dilemma type interactions between competing individuals has also been exploited for hiding and transmitting secret visual information. These communication schemes require the generation of two patterns while the difference image reveals the secret. Computational speed issues and the system insensitivity to small local perturbations of these approaches influences the further development of the communication schemes based on SOP. DVC scheme based on the optical time-averaging moiré technique has also been developed for information hiding. This approach is denoted by advantages over SOP because the secret image embedded into a moiré grating can be interpreted by a naked eye when the image is oscillated or deformed; also, it does utilize only a single image during communication. A natural extension of DVC could be the employment of a physical process describing the deformation law in encryption and decryption of the secret information in a stochastic deformable moiré grating.

Various pattern formation mechanisms and parameters result in different characteristic images which require the evaluation of complexity and feasibility for information hiding applications. Standard approaches, such as Shannon entropy, row/column correlation, image pixel analysis, or detection of steganographic characteristics, have been successfully used in image analysis. However, physical processes could form complex patterns and conceal additional information – e.g., small scale spatial chaos could be mentioned in this context; hence, novel approaches towards identification are required.

The object of the research is visual information hiding based on self-organizing patterns.

The aim of the work is to develop mathematical models and algorithms for visual information hiding and communication based on self-organizing patterns.

The Main Tasks of this Research Are:

1. to develop an effective and steganographically secure digital image hiding schemes based on self-organizing patterns which can be used to transmit secret visual information;

2. to build the mathematical foundation for the formation of cover images on the surface of structures performing harmonic oscillations;

3. to develop novel algorithms for the assessment of the complexity of self-organizing patterns.

Methods, Software, and Experimental Tools

- Information visualization and processing methods have been used for the creation and realization of dynamic visual cryptography conception based on non-linear oscillations.

- The mathematical apparatus and the theory of the optical moiré method was used for the researches. Its application is extended and further developed.

- The Euler method (the forward Euler method) was applied to simulate a chemical reaction and to numerically integrate differential equations.

- The theory of linear recurrent sequences was employed for the construction of algebraic approximation of any 2D image.

- Matlab R2016a was used for developing computational and experimental tools.

- COMSOL Multiphysics (the scientific package for physics-based finite element method modeling) was employed for the simulation of the deformation field.

Defended Statements

- Typical steganographic techniques are usually prone to steganalysis and do not guarantee the security of communication. Self-organizing patterns emerging from biological, chemical or physical processes can be successfully employed as an additional layer of security in concealing secret visual information.

- Dynamic visual cryptography schemes based on harmonic oscillations of the deformable harmonic moiré grating according to the predefined Eigen-shape enable to hide secret information by using only one share. Scheme adaptation for Ronchi grating makes the formation of the stochastic cover moiré image on the surface of physical objects easier.

- It is important to consider the feasibility of an image used in secure communication. 2-LRS pseudo-order can provide a deeper insight on the pattern complexity.

Scientific Novelty and Significance

- The proposed techniques for information hiding based on SOP amend and overcome the drawbacks of the previously introduced similar schemes. The ability to avoid the necessity of using random initial conditions and the perturbation of initial conditions for the generation of a self-organizing pattern is a serious enhancement in terms of the security of the communication scheme.

- An image encoding scheme in deformable one-dimensional moiré gratings oscillating according to a predefined Eigen-mode describing a physical process is implemented for the construction of two-dimensional digital dichotomous secret images. The Eigen-shape of the structure serves as the decoding key for a visual communication scheme.

- 2-LRS can be used to analyze the complexity of self-organizing patterns. Unlike Shannon entropy, the order of 2-LRS can be applied to estimate the complexity of self-organizing patterns with respect to each spatial coordinate and to detect the transformation from a small scale spatial chaos to a large scale spatial chaos.

Approval of the Results

The major results of the thesis have been presented in 8 publications, 6 of which were delivered in journals listed by the Institute for Scientific Information (ISI) as the main list of publications with citing indexes; the two remaining articles were announced in peer-reviewed conference proceedings. The topics covered in the dissertation were presented at two international conferences.

Scope and Structure of the Dissertation

This doctoral dissertation consists of the introduction, 4 major sections, conclusions, a list of references and a list of the author's publications. In total, there are 53 figures and 2 tables in the thesis. The list of 143 cited sources within the main part of the dissertation is added to the main body of the dissertation.

The relevance of the work and its scholarly problem are discussed in the introduction. Also, the aim of the work and its main tasks are formulated and outlined. The investigation methods, the software in use, and the applied experimental tools are provided in this section as well together with the defended statements, the scientific novelty significance and the approval of the obtained results.

The analysis of the scholarly literature which is relevant in terms of the aim and objectives of this thesis is presented in Chapter One. The visual communication scheme between two communicating parties based on self-organizing patterns is presented in Chapter 2. The image hiding scheme based on time-averaged moiré fringes on finite element grids is proposed in Chapter 3. The application of the order of a 2-sequence for the analysis of digital images is introduced in Chapter 4. Finally, the thesis is generalized by delivering its conclusions, bibliographic references, and a list of the author's scientific publications.

1. LITERATURE REVIEW

Data security was invented many years before the beginning of wireless communication. The importance to secure information arose from the early days of communication, and especially in the military sector, where it was necessary to provide some mechanism to protect the confidentiality of correspondence and to have some means of detecting tampering. It started with physical security, concealment and simple cipher algorithms, e.g., the Caesar cipher, where letters are replaced by a letter some fixed number of positions down the alphabet. It was followed by machines, e.g., the Enigma machine used in WWII to encrypt and decrypt the data of warfare whereas now computing equipment is employed to scramble and unscramble information (Simon, 2011). The exponential growth and the widespread use of electronic data processing and electronic business conducted through the internet, along with numerous occurrences of international terrorism, fueled the need for better techniques of protecting the computers and the information they store, process and transmit no matter who it belongs to – the military, the government, businesses or civilians (Killingback et al., 2013).

With the development of network and multimedia technology, information security and privacy become more and more important (Ling *et al.*, 2011; Nagaraja *et al.* 2016). The threat of an intruder accessing secret information has been an ever-existing concern for data communication in the public domain (Kaur *et al.*, 2014; Gurung *et al.*, 2015). Whatever technique is adopted for the security purposes, the degree and level of security always remains top concern. In information hiding field cryptography, steganography and digital watermarking techniques are used separately or together in combination (Zhou *et al.*, 2016; Razaq *et al.*, 2017) to provide greater security and overcome the threats of deciphering. Information security employs mathematical techniques and related aspects to provide confidentiality, data security, entity authentication and data origin authentication.

The most common information hiding technique is cryptography which is used directly or indirectly by everyday computer users. Internet websites are usually routed through secure protocols, or the device storage is encrypted, and only the user with the correct password or certificate can access their content. Cryptography is defined as the system by which ‘normal’ records can be turned to the unreadable form by using computationally intensive mathematical algorithms (Mishra *et al.*, 2015; Ling *et al.*, 2011) so that the unlawful individuals or entities could not access the plain or ‘overt’ records. The record is usually a text or digital data which is nothing else than an array of symbols. However, traditional cryptography suffers from such drawbacks as the key distribution (Maqsood *et al.*, 2017), the visibility of the cipher text to an eavesdropper, passive attacks which are commonly observed in the traditional system (Moizuddin *et al.*, 2017, Mishra *et al.*, 2015). Besides, cryptography is a computationally intensive technique which only works if a computer is present. Quantum computing, quantum cryptography and quantum key distribution, when available to the broad public, could solve the listed drawbacks (Moizuddin *et al.*, 2017). Meanwhile, with the availability of increasing computation power, it is only a matter of time before decrypting information becomes simple. An

information hiding mechanism which not only ensures confidentiality and authentication but is also cost effective is required (Gurung *et al.*, 2015; Sundari *et al.*, 2015).

Apart from complex mathematical models, there are several schemes which provide information security ensuring high capacity, the ease of use and secrecy. Visual Cryptography (VC) is a technique which allows visual information to be encrypted in such a way that its decryption can be performed by the Human Visual System (HVS) without any complex cryptographic algorithms (Gurung *et al.*, 2015). In 1994, Naor and Shamir suggested a secret sharing scheme which takes a secret binary image and divides it into many pieces known as shares. The decoding can be done visually by overlaying a defined number of shares (Naor *et al.*, 1994). Instead of the static superposition of shares, the concept of Dynamic Visual Cryptography (DVC) was introduced by (Ragulskis *et al.*, 2009a). DVC is based on time-average geometric moiré applied for a single encoded image. The secret image is embedded into the stochastic moiré grating in such a way that a naked eye cannot interpret the secret from the stationary cover image. The secret is leaked in the form of a pattern of time-averaged moiré fringes only when the encrypted cover image is oscillated according to a predefined law of motion. Special algorithms are required to encode the image, but the decoding is still completely visual. Visual cryptography is applied in a variety of areas: biometric security, remote electronic voting, user identification, online payments, etc., and is also used in conjunction with other techniques: watermarking and steganography (Pandey *et al.*, 2016; Rura *et al.*, 2016).

Steganography is another information hiding technique in which the very existence of secret information is hidden into cover objects. It has been widely used in the area of secret communication. Whereas steganography and watermarking jointly belong to the science branch of information hiding, they are definitely different. Specifically, steganography is the art of writing a message or information in such a way that no one apart from the sender and the recipient knows its meaning. Modern steganography offers a level of service that includes privacy, authenticity, integrity, availability, and confidentiality of the transmitted data (Sheshasaayee *et al.*, 2017). The reasons impacting the growth of interest in steganography are the interest in techniques for hiding encrypted copyright marks and serial numbers in the digital content as well as the need to communicate in some countries where the freedom of speech is restricted. Thus the methods by which private messages can be embedded in seemingly innocuous cover messages are widely studied. The ultimate objectives of steganography – which are undetectability, robustness (resistance to various image processing methods and compression) and capacity of the hidden data – are the main factors that distinguish it from the related techniques, such as watermarking and cryptography (Cheddad *et al.*, 2010).

Each steganography technique based on its embedding mechanism puts a special pattern on the stego-images. The most widely known spatial domain technique of steganography is the *Least Significant Bit* (LSB) substitution technique. A variety of extensions of the ‘common’ LSB can be mentioned: LSB with a shift (Joshi *et al.*, 2015), modified LSB (Odat *et al.*, 2016), MNEB (Maximum Number of Embedded Bits), ISB (Intermediate significant bits) (Parah *et al.*, 2012), etc. The

implementation of LSB is straightforward, but the embedded information is usually highly vulnerable and could be easily destroyed (Joshi *et al.*, 2015). For more secure data transfer, additional techniques such as cryptography (Joshi *et al.*, 2015; Zhou *et al.*, 2016), visual cryptography (Nandakumar *et al.*, 2011), or a pattern emerged from physical processes (Saunoriene *et al.*, 2011; Ishimura *et al.*, 2014) are used together with steganography. The latter attracts prominent interest because of the employment of mathematical models representing natural processes and due to its potential speed advantage over standard cryptographic techniques.

Spatial pattern formation is a key feature of many natural systems in physics, chemistry, and biology. The essential theoretical issue in understanding pattern formation is the explanation how a spatially homogeneous initial state can undergo spontaneous symmetry breaking leading to a stable spatial pattern (Killingback *et al.*, 2013). This problem is most commonly studied by using partial differential equations to model a reaction-diffusion system of the type introduced by Turing (Saunoriene *et al.*, 2011; Ishimura *et al.*, 2014; Barkley *et al.*, 1990). Self-organizing patterns can also be induced by complex interactions between competing individuals (Li *et al.*, 2012; Ziaukas *et al.*, 2014), nonlinear competitively coupled maps (Killingback *et al.*, 2013) or arise in the context of coupled-map lattices (Xu *et al.*, 2016). However, not every pattern and, especially, not every pattern formation mechanism is suitable for embedding secret visual information because of the inability to resist simple statistical analysis or even worse – human inspection. Thus it is important to ensure that the selected pattern formation method as well as the stego-image is secure (Roy *et al.*, 2016). The strengths and weaknesses are evaluated, for instance, by using pattern analysis of the image pixels or the palette, by visual inspection of the image, automated detection of steganographic characteristics (Johnson *et al.*, 2012), relative entropy between the cover and the stego-image, fidelity or imperceptibility (Roy *et al.*, 2016), by examining the textural features of the pattern (Yang *et al.*, 2014), or by using other alternative methods.

1.1. Information Hiding Techniques

Various data hiding techniques have been developed for different purposes and applications which are collectively known as the ‘information hiding’ techniques (Feng *et al.*, 2017; Muhammad *et al.*, 2017; Altaay *et al.*, 2012) and are broadly classified as cryptography, steganography and watermarking. A basic categorization of the outlined techniques as listed by (Gupta *et al.*, 2015; Weir *et al.*, 2012; Sundari *et al.*, 2015; Altaay *et al.*, 2012) are shown in Fig. 1.1, and a comparison (Cheddad *et al.*, 2010; Zielinska *et al.*, 2014; Mishra *et al.*, 2015; Chandra *et al.*, 2014) is presented in Table 1.1. Considering the topic of this thesis and the difference between the encoding and decoding processes, three main techniques could be complemented by an extension of cryptography – *Visual Cryptography* (VC) (Sahare *et al.*, 2015; Weir *et al.*, 2012). Despite the classification, these techniques are interlinked in practice: visual cryptography is used in watermarking (Weir *et al.*, 2012); the message is encrypted before hiding it inside the image by using watermarking techniques (Sundari *et al.*, 2015); steganography and cryptography are

complementary and orthogonal to each other, and both can be used in a combined form to provide a higher level of security (Kaur *et al.*, 2014; Razzaq *et al.*, 2017).

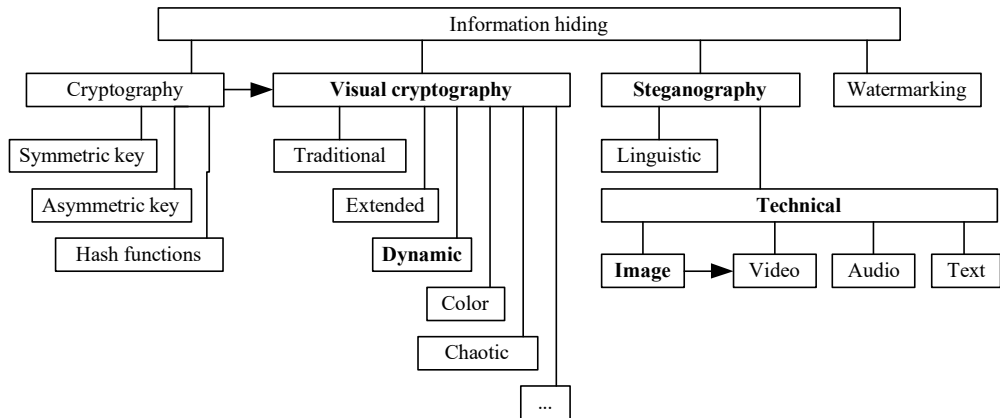


Fig. 1.1. Information hiding techniques. The arrows indicate an extension whereas the bold font indicates the focus of this thesis.

Table 1.1. Comparison of cryptography, steganography and watermarking.

Criterion	Cryptography	Steganography	Watermarking
Carrier	Usually text-based, with some extensions to image files	Any digital media	Mostly image/video/audio files
Secret data	Plain text	Payload	Watermark
Key	Necessary	Optional	
Input files	One	At least two unless in self-embedding	
Visibility	Always	Never	Sometimes
Detection	Blind	Blind	Usually informative
Authentication	Full retrieval of data	Full retrieval of data	Usually achieved by cross correlation
Objective	Data protection	Secret communication	Copyright preserving
Security of communication	Relies on the confidentiality of the key	Relies on the confidentiality of the method of embedding	
Result	Cipher-text	Stego-file	Watermarked file
Concern	Robustness	Detectability/capacity	Robustness
Type of attacks	Cryptanalysis	Steganalysis	Image processing
Fails when	Deciphered	Detected	Removed/replaced
Flexibility		Free to choose any suitable cover	Cover choice is restricted
Technology	Most algorithms are already known	Still being developed	

1.1.1. Cryptography

The exponential growth in the networking technology leads to the development of dramatic changes in the common culture for data interchanging. Therefore, the sensitive information, such as credit cards, banking transactions and social security numbers, need to be protected while in transmission. Cryptography

offers the means for ensuring communication security by scrambling the data to prevent the attacker from understanding the content. Cryptography also ensures that the message should be sent without any alteration and only the authorized person can be able to open and read the message (Niveditha, 2014). Thus the algorithms should ensure data privacy, confidentiality, integrity, authenticity, access control and non-repudiation (Sheshasaayee *et al.*, 2017; Chandra *et al.*, 2014; Niveditha, 2014; Mitali *et al.*, 2014).

The concept of cryptography is based on two main terms – the *plain text* and the *cipher text*. The original message is called the plain text whereas the encrypted version of the message is referred to as the cipher text. The method of encoding plain text is called *encryption*, and the process of reversing a ciphered text to its original plain text is called *decryption* (Maqsood *et al.*, 2017). The conceptual communication scheme based on cryptography is shown in Fig. 1.2.

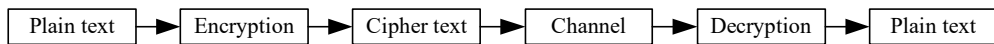


Fig. 1.2. Conceptual cryptography based communication scheme.

An important aspect of performing encryption and decryption is the key which makes the process of cryptography secure. Based on the key distribution, cryptography is further classified into three major types – *symmetric* key cryptography, *asymmetric* key cryptography and *hash functions* (Maqsood *et al.*, 2017; Chandra *et al.*, 2014; Niveditha, 2014; Ubale *et al.*, 2017; Mukundan *et al.*, 2016):

- In the type of symmetric encryption, the sender and the receiver share the same key for encryption as well as decryption. This type of cryptographic techniques has several benefits determining its relatively high performance (Chandra *et al.*, 2014), and, since this algorithm depends on its key entirely, it can be directly implemented on hardware (Niveditha, 2014). The weakness of a symmetric algorithm lies in the sharing of the symmetric key between the sender and the receiver; in those cases when sharing is compromised, the encrypted communication can be easily decrypted by the attacker. Various algorithms have been developed so far to describe symmetric key cryptography: AES, DES, 3DES, Blowfish (Ubale *et al.*, 2017).

- Users of asymmetric encryption use different keys for encryption and decryption: the sender uses a public key of the receiver for encryption whereas the receiver uses his/her private key to decrypt the message. Thus anyone can encrypt the message but only the legitimate person can decrypt the message. The problem of asymmetric encryption is that it works slower if compared to symmetric encryption. Most asymmetric algorithms depend on the properties of hard problems in mathematics such as factoring the product of two large prime numbers. There are various algorithms to implement this encryption mechanism: RSA, Diffie-Hellman, ECC, and Digital Signature Algorithm (Ubale *et al.*, 2017; Chandra *et al.*, 2014; Niveditha, 2014).

- Hash functions, also called *message digests* and *one-way encryption*, are algorithms that, in essence, use no key (Wang *et al.*, 2017; Mukundan *et al.*, 2016).

Instead, a fixed-length hash value is computed based upon the plain text that makes it impossible for either the content or the length of the plain text to be recovered. Hash algorithms are typically used to provide a digital fingerprint of a file's content; they are often used to ensure that the file has not been altered by an intruder or a virus. Hash functions are also commonly employed by many operating systems to encrypt passwords (Marcella *et al.*, 2007).

As mentioned above, cryptography is usually applied and works best on the plain text, but there also exist extensions of image encryption which are different from the text encryption technique (Das *et al.*, 2014). There are several security problems associated with digital image processing and transmissions; moreover, digital images are comparatively less sensitive than data because any single change in the pixels does not change the entire image. In other words, a small modification of a digital image is acceptable compared to data – yet it is more prone to attacking. This leads to a group of visual cryptography techniques working only on graphical data.

1.1.2. Visual and Dynamic Visual Cryptography

The basic idea of cryptography is that the computation process should be complex enough to guarantee that nobody (i.e., no intruder) will be able to break the system (Sahare *et al.*, 2015). In 1994, Naor and Shamir introduced the *Visual Cryptography* (VC) method of securing data without cryptographic computation (Naor *et al.*, 1994). It encrypts visual information in such a way that the decryption is completely visual and computers are not required to interpret the secret image. The secret image is broken up into several shares which are printed on separate transparencies. Decryption is performed by overlaying the shares (Fig. 1.3). Many advances have been achieved in visual cryptography since 1994 (Vaidelys *et al.*, 2015b). Visual cryptography schemes enabling cheating prevention were presented by (Chen *et al.*, 2012); a multi-secret visual cryptography scheme based on random grids was introduced by (Han *et al.*, 2015); a secret sharing based visual cryptography scheme using CMY color space (Dahat *et al.*, 2016) and quality improvement in color extended visual cryptography has also been proposed (Mohan *et al.*, 2016).

The concept of dynamic visual cryptography was introduced by (Ragulskis *et al.*, 2009a). This technique is based not on static superposition of shares, but rather on time-average geometric moiré applied for a single encoded image. The secret image is embedded into the stochastic moiré grating; the secret is leaked only when the amplitude of the harmonic oscillations is set to a preselected value (Fig. 1.4). A naked eye cannot interpret the secret image from the stationary cover image (Fig. 1.4a). Therefore, dynamic visual cryptography is similar to classical visual cryptography – special algorithms are required to encode the image, but decoding is completely visual. Additional image security measures are suggested in (Vaidelys *et al.*, 2015b, Ragulskis *et al.*, 2009c) where the secret image is leaked in the form of a pattern of time-averaged moiré fringes only when the encrypted cover image is oscillated according to a predefined law of motion (Vaidelys *et al.*, 2015a).

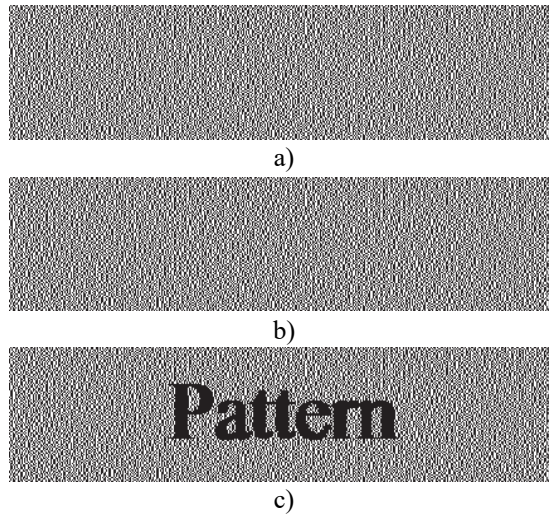


Fig. 1.3. An example of a visual cryptography scheme where the secret text (c) appears when two same-sized images (shares, shown in (a) and (b)) of apparently random black-and-white pixels are superimposed.

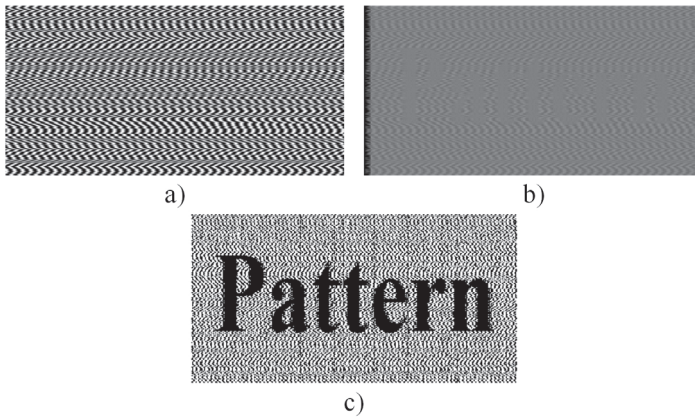


Fig. 1.4. Visual decryption of the secret data: a) the secret image encoded into a cover moiré image; b) the secret message is leaked when the cover image is oscillated according to a preselected law of motion; c) the secret message is highlighted by using a contrast enhancement algorithm (Ragulskis *et al.*, 2009b).

Visual cryptography schemes are one of the special and most interesting encryption techniques. One of the advantages of VC and DVC schemes is the property that decoding relies purely on the human visual system. It allows this technique to use in a lot of interesting applications in private and public sectors. VC is used with short messages thus giving cryptanalysis little to work with. It can be used together with other data hiding techniques to provide a higher security level. As far as short messages are considered, this method can be a part of another technique, e.g., for public keys encryption. VC has proved that security can even be attained with simplest encryption schemes.

1.1.3. Steganography

Steganography can be defined as the study of invisible communication that usually deals with the ways of hiding the existence of the communicated message (Sheshasaayee *et al.*, 2017, Taouil *et al.*, 2017). Unlike cryptography whose goal is to secure the transferred information from an eavesdropper, a steganographic system hides the content by embedding it in a cover media so that not to arouse an eavesdropper's suspicion while being transmitted through an open channel (Zhang *et al.*, 2017). There are many kinds of covers, such as texts (Sheshasaayee *et al.*, 2017; Zhang *et al.*, 2017), images (Huang *et al.*, 2012; Xia *et al.*, 2016b), videos (Sadek *et al.*, 2017), biological media, such as human skin or DNR, etc. The present work focuses on steganography in digital images which is the most popular form of steganography – thus other kinds of covers are not discussed further in the paper.

Steganography provides the ultimate guarantee of authentication that no other security tool can ensure and has a number of applications in distinct fields, such as defense and intelligence, medical, on-line banking, on-line transaction, intellectual property protection, enhancing robustness of an image in search engines, as well as many other financial and commercial purposes (Kaur *et al.*, 2014; Zhang *et al.*, 2017, Wang *et al.*, 2017, Sheshasaayee *et al.*, 2017). For example (Xia *et al.*, 2016a; Zhou *et al.*, 2017), methods of detecting illegal copies of copyrighted images have been introduced. In the field of medical sciences, it is necessary to ensure the confidentiality between the patients' image data or DNA sequences and their captions, however, a link must be maintained between the two. Thus embedding the patient's information in the image as stated by (Taher *et al.*, 2016; Liu *et al.*, 2013; Wang *et al.*, 2017) could be a useful safety measure which helps in solving such problems. Inspired by QR codes and the notion that steganography can be embedded as part of the normal printing process, a method for embedding data into a ready-to-print halftone image which provides an alternative for embedding data in visually meaningful images has been presented (Chen *et al.*, 2017). A printed picture can contain encoded data that is invisible but still decodable with a mobile phone camera.

There are some terms commonly used by steganography communities. The term *cover-image* is used to describe the image designated to carry the embedded bits. An image with embedded data is called the *payload* or the *stego-image*. Analogously to cryptanalysis, *steganalysis* (or *attack*) refers to visual image processing and statistical analysis approaches aiming to detect hidden information inside a cover without the knowledge of the embedding algorithm and the key (Rafat *et al.*, 2016). Embedding is usually parametrized by a key that makes it difficult even to detect the presence of data and further find a key to access the data (Kaur *et al.*, 2014).

The process of transmitting (embedding and extraction) secret message M can be defined as follows (Cheddad *et al.*, 2010): Let C denote the cover carrier, i.e., the cover-image, and C' the stego-image. An optional key used to encrypt the message or to generate a pseudorandom noise is denoted as K . Em is an acronym for embedding and Ex stands for extraction. Therefore:

$$Em: C \oplus K \oplus M \rightarrow C',$$

$$Ex(Em(c, k, m)) \approx m, \quad \forall c \in C, \quad k \in K, \quad m \in M. \quad (1)$$

There are three ways to hide a digital message in a digital cover (Kaur *et al.*, 2014): first of all, *data injection* – a secret message is embedded directly in the cover carrier, which results in larger files. Secondly, *replacement* or *substitution* – selected pixels of the cover are interchanged with the secret data. However, depending on the amount of secret data, the quality of the original cover can noticeably decrease. Finally, *generation of the cover* should be mentioned – a cover is generated for the sole purpose of concealing a secret message.

Image steganography techniques are divided into *spatial domain* (plane co-ordinate system) and *transform* (frequency) *domain* categories (Kaur *et al.*, 2014; Niveditha, 2014; Rafat *et al.*, 2016):

- Spatial domain techniques include bitwise manipulation of the intensity of pixels and noise manipulation. The most common and the simplest approaches to embed data in the spatial domain are the *Least Significant Bit* (LSB) methods. The concept of LSB substitution includes the embedding of the secret data at the bits having minimum weighting. If the last 2 bits of a color are manipulated, the value of the color changes at most +/-3 value places, and such change is indistinguishable by the human visual system (HVS) (Fig. 1.5). However, LSB insertion is very easy to implement, yet, on the other hand, it is also easily attacked (Niveditha, 2014). Firstly, hidden information can be easily overwritten by changing the original secret message. Secondly, the statistical properties of the media are modified – thus statistical methods can be used in order to detect and subsequently extract the secret. This technique works best when the message is considerably smaller than the cover image file, and when the color map over the image varies significantly. Other spatial domain methods are the *Optimal Pixel Adjustment Procedure* (OPAP), the *Pixel Indicator Technique* (PIT), and the *Pixel Value Differencing* (Roy *et al.*, 2016).




Color (Gray)	Base 10	Binary	Change
	128	10000000	base
	130	10000010	+2
	131	10000011	+3

Fig. 1.5. Information may be concealed by manipulating the LSB of an image. The change of the last 2 bits of a color value results in the change of color value by +/-3 places.

- Transform domain techniques initially convert an image from the spatial domain to the frequency domain, and then the secret message is embedded. The secret data is embedded by modifying the transform coefficient of the image, which makes this technique more robust to attacks like compression, filtering, etc. The techniques in use are *Discrete Cosine Transformation*, *Discrete Wavelet Transform*, *Discrete Fourier Transform*, (Cheddad *et al.*, 2010), or *Singular Value Decomposition* (SVD) *transform* based method (RHISSVD) (Roy *et al.*, 2016).

The primary objectives of steganography are its undetectability (resistance against steganalysis techniques), robustness (resistance against various image processing methods and compression), security (an algorithm is considered secure if

the embedded information cannot be removed after detection) and the embedding rate of the hidden data (Kaur *et al.*, 2014; Niveditha, 2014). Breaking a steganography system normally consists of detecting, extracting and disabling or destroying the embedded information. A system is already insecure if an attacker is able to prove the existence of a secret message (Garzia, 2013). The security requirement in steganography ultimately means that neither a human nor a computer detection method should be able to confirm the presence of a secret message within a cover with a significant reliability (Garzia, 2013). When developing a formal security model, it is important to assume that an attacker has unlimited computation power and is able and willing to perform a variety of attacks. Thus no matter how sophisticated and complex the information hiding scheme may be, the security of the system primarily lies in keeping the cover-image secret (Rafat *et al.*, 2016) and the information hiding algorithm private (Zhang *et al.*, 2017).

The theoretical and formal definition of a steganographic security system was formulated by (Cachin, 2004). The main idea is to refer to a selection of the cover as random variable C with probability distribution P_C (Garzia, 2013). The embedding of a secret message can be seen as a function defined in C ; let P_S be the probability distribution of $Em(c, k, m)$ – that is the set of all the stego-images generated by the steganographic system. If a cover is never used as a stego-image, then $P_S(c) = 0$. In order to calculate P_S , probability distributions on K and M must be imposed. By using the definition of the relative entropy $D(P_1||P_2)$ between two distributions P_1 and P_2 defined on the set Q , the impact of the embedding process on distribution P_C can be measured.

$$D(P_1||P_2) = \sum_{q \in Q} P_1(q) \log_2 \frac{P_1(q)}{P_2(q)}. \quad (2)$$

This formula measures the inefficiency of assuming that the distribution is P_2 , where the true distribution is P_1 .

Specifically, the security of a steganography system is defined in terms of $D(P_C||P_S)$ as: S is a steganographic system, P_S is the distribution probability of the stego-image sent over the channel, and P_C the distribution probability of C . S is thus ε -secure against a passive attack if $D(P_C||P_S) \leq \varepsilon$ and is called perfectly secure if $\varepsilon = 0$.

1.1.4. Watermarking

Digital watermarking or fingerprinting is the process of embedding a watermark signal into multimedia data to generate a watermarked object to protect the authenticity of the owner on that digital object and mainly focuses on the robustness of the embedded message rather than the capacity or concealment (Kaur *et al.*, 2014). A digital watermark can be any signal or pattern embedded into any multimedia file which can be used for copyright protection and authentication as it cannot be altered or modified (Sundari *et al.*, 2015).

1.2. Self-Organizing Patterns

The study of self-organizing patterns started in the 1950's with a Belousov-Zhabotinsky (BZ) reaction which serves as a classical example of non-equilibrium thermodynamics resulting in the establishment of a nonlinear chemical oscillator. It was observed that a reaction of a mixture of specific chemicals does not reach an end point but rather keeps oscillating by changing colors. However, the finding cannot be backed up theoretically because of a contradiction to the second law of thermodynamics (Prigogine *et al.*, 1977). It was not before the late 1960's when Belousov's findings were confirmed by Zhabotinsky, and it was also noticed that the reaction exhibits a pattern formation mechanism with similarities to the mechanism that Turing had proposed. However, an unusual and interesting feature of the reaction is that as it progresses on a two-dimensional plate, self-organized spirals are formed (Fig. 1.6).

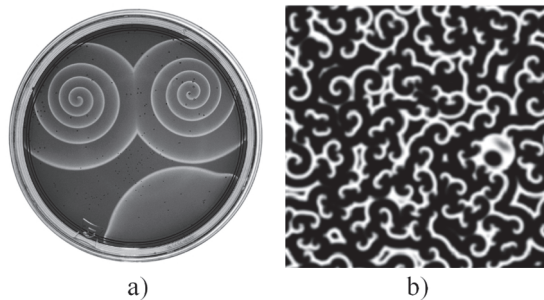


Fig. 1.6. The Belousov-Zhabotinsky reaction can form spiral waves in a petri-dish (a) and during computer simulation (b). The white color corresponds to high concentrations of a particular acid used in the reaction (Averill *et al.*, 2012; Ball, 1994).

The basic mechanism of the BZ reaction consists of cerium-catalyzed oxidation of malonic acid in an acid medium by bromate ions, and the simplest realistic model devised by (Field *et al.*, 1974) is the three-component Oregonator model given by:

$$\begin{aligned}\frac{\partial x}{\partial t} &= qy - xy + x(1 - x) + D_x \nabla^2 x, \\ \frac{\partial y}{\partial t} &= -qy - xy + fz + D_y \nabla^2 y, \\ \frac{\partial z}{\partial t} &= x - z + D_z \nabla^2 z,\end{aligned}\tag{3}$$

where x , y and z correspond to the scaled concentrations $[\text{HBrO}_2]$, $[\text{Br}^-]$ and $[\text{Ce}^{4+}]$, respectively. q and f parameters adjust the dynamics of the model whereas D_x , D_y and D_z are the diffusion coefficients. The Oregonator model produces concentric waves or spiral waves.

Such mathematical models mimicking the evolution of nature are important not only to theoretical chemistry or biochemical and biological systems but also produce interesting visual effects on the 2D plane. Thus the formation of

self-organizing patterns (SOP) in biology (Yamasaki *et al.*, 2011, Wang *et al.*, 2011; Zheng *et al.*, 2015, Klein *et al.*, 2017) (animal markings, growth of colonies, vegetation patterns, cancer dynamics), chemistry (Grindrod, 1996, Rogora *et al.*, 2016) (reaction-diffusion systems, Turing, precipitation patterns), physics (Weiss *et al.*, 2007) (liquid crystals, granular material, optical resonators), computer graphics (Sahin *et al.*, 2015) (cellular automata, texture analysis) has been attracting the attention of researchers since the middle of the twentieth century.

Self-organizing patterns emerging from nature should not be mixed up with the self-organizing map (SOM) which defines a type of artificial neural network (ANN) and certain self-organized patterns (SOP) that develop automatically and unexpectedly during the training of a typical self-organizing map (SOM) network. These highly structured patterns emerge and evolve gradually from the random initial state as the training progresses (Wang, 2015). However, ANNs are not within the scope of this thesis.

It is well known that self-organizing patterns can also be used for hiding and communicating secret visual images. A secure steganographic communication algorithm has been developed (Saunoriene *et al.*, 2011; Ishimura *et al.*, 2014) where patterns are produced by using a Beddington-DeAngelis type predator-prey model with self- and cross-diffusion. Self-organizing patterns induced by prisoner-dilemma-type interactions between competing individuals and described by evolutionary spatial 2×2 games are exploited for hiding and transmitting secret visual information (Ziaukas *et al.*, 2014). Since they have some drawbacks, new models of self-organizing patterns are presented in this section and used in this thesis.

1.2.1. Chaotic logistic map

The generation of the initial population matrix is an important step in the evolution of many self-organizing patterns or systems (Ziaukas *et al.*, 2014; Saunoriene *et al.*, 2011; Bolliger *et al.*, 2013; Moore *et al.*, 2014). A simple dichotomous random number generator could be used to initialize the initial matrix; however, it does not ensure repeatability of the evolution. This is specifically important during secure communication when the Sender and the Receiver must be able to generate an identical copy of the initial matrix. The transmission of the whole initial matrix is not considered due to the bandwidth costs and the ease of tampering.

The chaotic Logistic map (Yu *et al.*, 2017) could be used for the efficient generation of the initial population. Iterated values of the logistic map are as follows:

$$a_{i+1} = ra_i(1 - a_i). \quad (4)$$

They can be used for the efficient generation of pseudo-random numbers. Here a_i is a number between zero and one that represents the ratio of the existing population to the maximum possible population; parameter r is within the interval $[0,4]$. In this thesis, parameter r is fixed to $r = 4$ because only at $r = 4$ the resulting chaotic sequence at almost all initial conditions a_0 falls into the interval $[0; 1]$ (Yu *et al.*, 2017).

By using the logistic map, the communicating parties can share only the initial condition of the logistic map instead of sharing the initial population of all the elements in the domain. Although every pseudo-random number generator has its drawbacks – the chaotic Logistic map has a limited uniformity of generated values, stable windows and a relatively small space of valid seeds. The Logistic map can be enhanced and extended – alternative versions of the map, such as an intertwined Logistic map (Wang *et al.*, 2013), can eliminate some of these drawbacks. However, the standard Logistic map is also successfully used in various image encryption techniques and protocols (Yu *et al.*, 2017; Ye *et al.*, 2017).

1.2.2. Nonlinear Competitively Coupled Maps¹

Let us consider a one-dimensional unimodal mapping in the form $f(x) = x \cdot F(x)$ where $F: \mathbb{R} \rightarrow \mathbb{R}$ is a smooth mapping. We shall use a mapping named after Maynard Smith (Killingback *et al.*, 2013):

$$F(x) = \eta(1 + x^b) \quad (5)$$

where parameters η and b are positive constants.

A two-dimensional generalization of this mapping with the introduction of the competitive aspect to the model gives the time evolution of a particular state $x(t)$ at time t on a rectangular domain $[1; L_x] \times [1; L_y]$:

$$x_{i,j}(t+1) = x_{i,j}(t) \cdot F[x_{i,j}(t) + \alpha \cdot \Sigma_{i,j}(t)] \quad (6)$$

where

$$\Sigma_{i,j}(t) = \sum_{p,q \in \{-1,0,1\} \setminus \{0,0\}} x_{k,l}(t), \quad (7)$$

$$k = \text{mod}(i + p - 1, L_x) + 1; l = \text{mod}(j + q - 1, L_y) + 1$$

is the sum of adjacent elements in the 8-element Moore neighborhood of the element $x_{i,j}(t)$; α is a non-negative parameter that represents the strength of the competitive interaction between neighboring elements. We should note that the local site dynamics are coupled through a competitive – rather than diffusive – interaction. 2D periodic boundary conditions are assumed; L_x and L_y define the number of elements in the rectangular domain. We should also note that every element $x_{i,j}$ represents a single pixel of a digital image.

Competitively coupled maps are based on interactions between discrete neighboring nodes. These interactions are usually interpreted as the competition from the physical (or biological) point of view. In terms of steganography, it is

¹ Some passages have been quoted verbatim from the following source:

Competitively Coupled Maps for Hiding Secret Visual Information.
Vaidelys M., Ziaukas P., Ragulskis M.
Copyright © 2015 Elsevier B.V.

always important to take into account algorithmic aspects of the evolutionary model – such as feasibility, computational efficiency and complexity, memory and time requirements. A wide variety of different evolutionary models exhibiting interesting behavioral aspects does exist. However, competitively coupled maps are relatively simple yet robust and computationally effective models capable of producing stationary patterns from homogeneous initial configurations – and therefore they are well suited for the considered steganographic application. Moreover, presented competitively coupled maps (Killingback *et al.*, 2013) do produce complex spatial patterns even when the dynamics at each node is trivial (the local dynamics of an isolated node does exhibit a stable fixed point). This is in stark contrast to conventional diffusively coupled map lattices where trivial dynamics of a node can only result in a spatially homogeneous state (Waller *et al.*, 1984; Jansen *et al.*, 2000; Rohani *et al.*, 1996).

Other nonlinear competitively coupled maps could be considered instead of the Maynard Smith map. A possible example could be the Ricker and Hassell maps discussed in (Killingback *et al.*, 2013) or even some other more complex nonlinear competitively coupled maps. However, the ability of a coupled map to generate self-organizing patterns is not a sufficient condition for the construction of the proposed image hiding scheme. It is important that the difference image between the patterns produced by the non-modified and modified initial conditions would be able to represent the dot-skeleton representation of the secret information. This requirement is far from being trivial and necessitates the appropriate tuning of the system's parameters.

1.2.3. Atrial Fibrillation Model²

The atrial muscle is comprised from myocytes which form the primal structure of the tissue. Observable patterns formed by myocytes are not regular and conform to complex self-organizing rules as proposed in (Luke *et al.*, 1991; Verheule *et al.*, 2003). Cells within this structure are coupled mainly by longitudinal (end-to-end) connections rather than latitudinal (side-by-side) connections thus resembling a cable-like signal transmission (Luke *et al.*, 1991; Nakamura *et al.*, 2011). Such conditions as fibrosis and scarring processes can weaken and damage the connections (Luke *et al.*, 1991) and adjust the network of functioning cells (Clayton *et al.*, 2011, Clayton *et al.*, 2001).

The whole interaction of cells within the network can be modeled as proposed in (Christensen *et al.*, 2015). Longitudinal (end-to-end) signals are always transmitted, whereas latitudinal (side-by-side) signals are transmitted only with a probability v . This non-symmetrical coupling corresponds to the physical organization of cable-like transmissions. As a simplification, the structure can be

² *Some passages have been quoted verbatim from the following source:*

Image hiding scheme based on the atrial fibrillation model
Vaidelys M., Ragulskiene J., Ziaukas P., Ragulskis M.
Applied Sciences, 2015

presented as a flat entity because the wall of the atrial muscle is relatively thin (Nakamura et al., 2011).

The general idea of cable-like transmissions (Christensen *et al.*, 2015) used to mimicking the branching network of heart muscle cells is implemented on a discrete grid as follows. Three states of cells are considered: the resting state, the excited state, and the refractory state. Resting cells and excited cells interact in two directions with different probabilities – probability l for the longitudinal direction and probability ν for the latitudinal (transversal) direction. Just after a cell has been excited, it enters the refractory state where it remains for the time period equal to τ (as illustrated in Fig. 1.7).

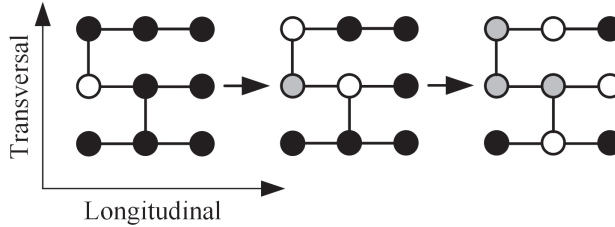


Fig. 1.7. The diagram of interaction between cells within a network. The resting cells (black) and the excited cells (white) interact in two directions with different probabilities. A resting cell becomes excited if it interacts with another excited cell. An excited cell (white) enters a refractory state (gray) for time period τ .

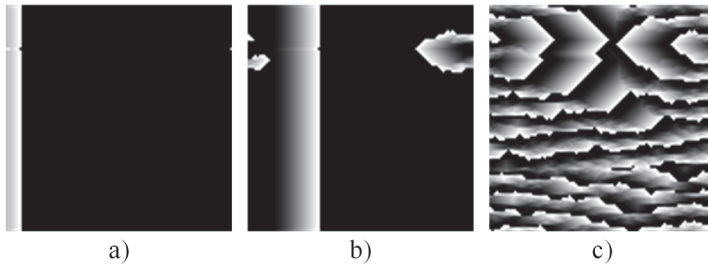


Fig. 1.8. Initial plane vertical wave is induced at the left side by pacemaker cells (a). However, one cell is dysfunctional and blocks the propagation of the wave front (b). Due to the vertical connections between longitudinal cables, the resulting process forms a pattern (c).

In order to recreate some basic topological features of the atrial muscle, periodic boundary conditions in the transversal direction can be combined with open boundary conditions in the longitudinal direction. This corresponds to the topology of a cylinder which is useful in order to investigate the effects of spontaneous heterogeneity that takes place on the front of the propagating wave. In general, once the initial grid has been fixed, all the interactions that can be numerically simulated depend only on system parameters ν (the probability of interactions along the transversal direction) and τ (the time spent in the refractory state). However, the interactions between cells can be seriously complicated by dysfunctional cells. That can be illustrated by a simple computational experiment presented in Fig. 1.8. Pacemaker cells are placed at the left boundary of the digital image and initiate the

wave front which propagates to the right in all longitudinal cables (Fig. 1.8(a)). However, because of dysfunctional cells, this is not always the only wave direction. A dysfunctional cell may block the propagation wave front (Fig. 1.8(b)). The interplay between the wave fronts can form different patterns as shown in Fig. 1.8(c). We should note that the boundary conditions are periodic.

The reader should keep in mind that the presented atrial fibrillation (AF) model is a rough approximation of complex biological processes taking place in the tissue of the heart. The complex distribution of cardiac action potentials, spiral waves, arrhythmias, sinoatrial nodes and many other phenomena taking place in the heart cannot be modeled by using this AF model. More sophisticated models that facilitate understanding of the behavior of the waves in the context of the heart should be used: a visualization of spiral and scroll waves in simulated and experimental cardiac tissue was presented by (Cherry *et al.*, 2008); a spiral wave drift and complex-oscillatory spiral waves caused by heterogeneities in two-dimensional *in vitro* cardiac tissues were presented by (Woo *et al.*, 2008).

1.2.4. The Spiral Wave Model³

Spiral waves are observed in various nonequilibrium systems having a two-dimensional plane. Various examples are known to exist, for instance, the previously mentioned Belousov-Zhabotinsky reaction-diffusion system (Field *et al.*, 1974), FitzHugh-Nagumo model (Sherwood, 2014), Ball's model (Ball, 1994), the chloride-iodide-malonic acid or ferrocyanide-iodate-sulfite reaction-diffusion systems (Szalai *et al.*, 2008), and others. In all the cases, the spiral wave activity either underlies an important biological function or is denoted by physiological significance. For example, it was noted that waves of contraction (electrochemical BZ waves) propagate in the heart tissue with the switch from concentric ring patterns to spiral waves being associated with the onset of ventricular fibrillation (Winfree, 1994). Waves of contraction are initiated and propagate out to the muscle tissue in the ventricles. After contraction, the tissues go into a temporary refractory state, thus the waves propagate away from the centers of initiation, and the heart beats normally. However, if inhomogeneity is observed in the heart tissue (i.e., if some tissues are damaged or unresponsive to stimulation), even a small infarct can act as sites for the initiation of spiral waves of contraction and send the ventricles into a state of fibrillation.

The paradigmatic Barkley model (Barkley *et al.*, 1990; Dowle *et al.*, 1997) for modeling spiral waves in excitable and oscillatory media is presented here. This model is often used as a qualitative model in pattern forming systems, such as the Belousov-Zhabotinsky reaction and other systems that have been well described by the interaction of an activator and an inhibitor component.

³ Some passages have been quoted verbatim from the following source:

Digital Image Communication Scheme Based on the Breakup of Spiral Waves.
Vaidelys M., Lu C., Cheng Y., Ragulskis M.
Copyright © 2016 Elsevier B.V.

The considered model comprises a system of reaction-diffusion equations describing the interaction of activator u and inhibitor v :

$$\begin{aligned}\frac{\delta u}{\delta t} &= f(u, v) + \nabla^2 u, \\ \frac{\delta v}{\delta t} &= g(u, v) + D\nabla^2 v,\end{aligned}\tag{8}$$

where $f(u, v)$ and $g(u, v)$ are local reaction kinetics functions whereas parameter D is consequently the ratio of diffusion coefficients. Reaction term $f(u, v)$ is given by:

$$f(u, v) = \frac{h(x)}{\varepsilon} u(1 - u)(u - u_{th}(v))\tag{9}$$

where parameter ε sets the timescale separation between the fast u -equation and the slow v -equation (therefore ε is typically small); functions $h(x)$ and $u_{th}(v)$ define the evolution of the slow variable. In the simplest case (Barkley *et al.*, 1990), we obtain the following:

$$h(x) = 1, \quad u_{th}(v) = \frac{v - b}{a}\tag{10}$$

where a and b are system parameters – thus a larger a gives a longer excitation duration, and a higher ratio b/a gives a larger excitability threshold. The other reaction term reads:

$$g(u, v) = u - v\tag{11}$$

The nullclines in the Barkley model for the nonlinear u reaction kinetics are straight lines. The u -nullclines are given by $f(u, v) = 0$ so that the three branches are:

$$u = \begin{cases} 0, \\ u_{th}(v), \\ 1. \end{cases}\tag{12}$$

The middle branch sets the excitation threshold. In practice, for spiral wave solutions, the system does not pass through the corners where the branches of the nullclines intersect.

This reaction is simulated with a simple Euler forward scheme; the Laplacian operator is simulated numerically by using a finite differences method on a regular square grid with a five-point formula (Dowle *et al.*, 1997):

$$\frac{\nabla^2 u}{4} = \frac{1}{4}(u_{i+1,j} + u_{i-1,j} + u_{i,j+1} + u_{i,j-1}) - u_{i,j}\tag{13}$$

By combining the five-point formula with large time steps, the reaction terms can be time-stepped with relatively minor computational efforts.

The domain is represented as a 2D square of size L with zero-flux boundary conditions. We set the initial conditions as dichotomous patches (vertical for the u -field and horizontal for the v -field) where the black color corresponds to 0 and the

white color corresponds to 1 (Fig. 1.9). In such a model, the spiral wave forms with no sign of breakup (Barkley *et al.*, 1990). Time step dt is set to 0.05; the time period used for the computation is marked as T . The evolving spiral wave is illustrated at $T = 5, 10, 15, 20$ and 30 in Fig. 1.9.

A regular spiral wave may evolve into a non-regular spiral wave with breakups when reaction term g is a nonlinear function (as suggested by Bär *et al.*, 1993):

$$g(u, v) = u^3 - v \quad (14)$$

As discussed in (Barkley, 2008), there are sets of parameters a, b and ε , when the spirals may undergo period rotations or various types of meander/break-ups. The evolution of the pattern into a complete breakage is illustrated in Fig. 1.10.

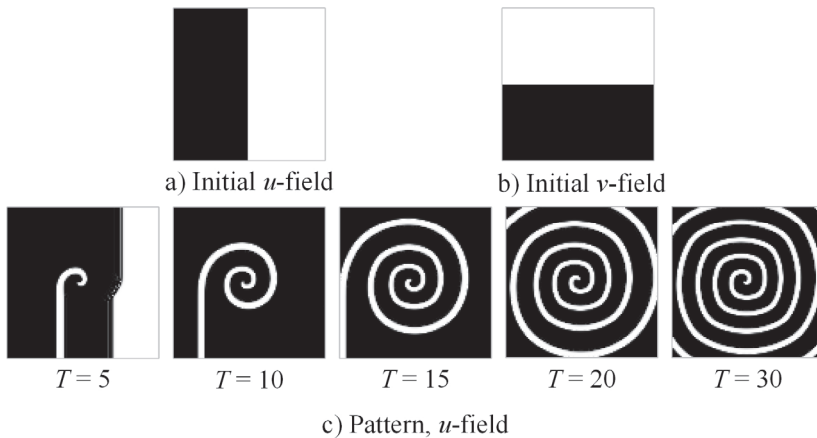


Fig. 1.9. The evolution of a regular spiral wave. The parameters of the model are set to: $L = 100, \varepsilon = 0.1, a = 0.7, b = 0.06, g = u - v; dt = 0.05$. The initial conditions are shown in (a) and (b); the evolution of the u -field is shown in (c).

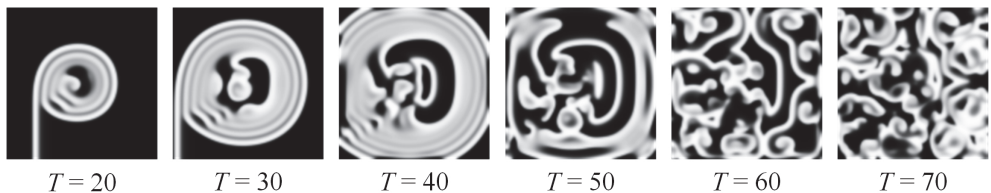


Fig. 1.10. The evolution of a spiral wave with breakups (u -field only) with reaction term g set to: $g = u^3 - v$ (other parameters are the same as in Fig. 1.9).

1.3. Image Processing Techniques

Image enhancement techniques have been widely used in many applications of image processing in order to bring out details in an image that are obscured or to highlight certain features of interest in an image for human viewers. Enhancement techniques include contrast adjustment, filtering, morphological filtering, and deblurring (Umbugh, 2010). Image enhancement operations typically return a modified version of the original image and are frequently used as a preprocessing step to improve the results of image analysis techniques. There is no general theory

for determining what is a ‘good’ image enhancement when it comes to human perception. The general idea is that if something looks good, it is good. The few image enhancement techniques and morphological operations employed in this thesis are presented in this Section.

1.3.1. Thresholding

Thresholding is the simplest and fastest pixel-based technique to segment an image. The standard thresholding approach creates binary images from grey-level ones by turning all the pixels below some threshold to zero, and all the pixels above that threshold to one. If $g(x, y)$ is a thresholded version of $f(x, y)$ at some global threshold T , then (Umbaugh, 2010):

$$g(x, y) = \begin{cases} 1, & f(x, y) \geq T, \\ 0, & \text{otherwise.} \end{cases} \quad (15)$$

The major problem with thresholding is that only the intensity is considered, and the relationships between the pixels are ignored. There is no guarantee that the pixels identified by the thresholding process are contiguous, and, if the illumination across the scene changes, additional adaptation is required. There are a number of different ways to perform thresholding: for global thresholding, Otsu’s method is aimed to find the optimal value T ; automatic, variable and multiple thresholding tries to adapt to the changing illumination conditions across the image. However, when using a thresholding technique, it is typical to experiment with its parameter T in order to get a satisfying result.

Since thresholding produces a binary image, this feature can be advantageous in certain applications when subsequent morphological operations (Rad *et al.*, 2014) or level set methods (Nobi *et al.*, 2001, Xu *et al.*, 2010) are used (it can be easier to manipulate with only black and white pixels).

Instead of converting the image to a binary, a threshold value could also be defined to replace all the values under the threshold to the 0 value, and the other values are made to take the values of the original image (Nobi *et al.*, 2001). This helps to keep the original value fixed and to ignore the unnecessary part of the image that is not required for the task. In such a case, the thresholding function reads as:

$$g(x, y) = \begin{cases} f(x, y), & f(x, y) > T, \\ 0, & \text{otherwise.} \end{cases} \quad (16)$$

1.3.2. Mapping Functions

Patterns of time-averaged moiré fringes usually require classical contrast enhancement techniques to make them friendlier to the human eye. A digital image should be filtered by using grayscale level adjustment transformation where levels around 0.5 are mapped to 0 (middle gray levels are mapped to the black color); all the other grayscale levels are mapped to 1 (grayscale levels except for middle gray are mapped to the white color). One of the mapping functions $F(I(x, y))$ used for contrast enhancement could be the step mapping function (Ragulskis *et al.*, 2009b):

$$F(I(x, y)) = \begin{cases} 0, & m - \varepsilon \leq I(x, y) \leq m + \varepsilon, \\ 1, & \text{otherwise.} \end{cases} \quad (17)$$

where F is the intensity of the image after filtering; $I(x, y)$ is the intensity at point (x, y) in the original image; m is a grayscale level at moiré fringe centerlines, and ε represents the bandwidth around m . A characteristic feature of the step mapping function is that the continuous grayscale interval is mapped into pure black and white colors.

1.3.3. Hyperbolic Tangent Contrast Enhancement

Hyperbolic tangent is a mathematical sigmoid function having a characteristic ‘S’-shaped curve or a sigmoid curve. The hyperbolic tangent contrast enhancement method uses the function of the hyperbolic tangent to produce a nonlinear translation of image values in order to improve its contrast. As a result, the midrange portion of the display histogram is stretched at the expense of both high and low values, thus increasing the image contrast for midrange values without greatly shifting the average brightness. It is proposed to use the following square of hyperbolic tangent representation (Ragulskis *et al.*, 2009b):

$$F(I(x, y)) = \tanh^2(k(I(x, y) - m)), \quad (18)$$

or a simplified hyperbolic tangent version:

$$F(I(x, y)) = \tanh(kI(x, y)), \quad (19)$$

where F is the intensity of the image after filtering; $I(x, y)$ is the intensity at point (x, y) in the original image; \tanh is a hyperbolic tangent (the classical sigmoidal function), and k is the parameter defining the depth of darkening of the digital image around $I = m$. At $k < 1$, the whole image is darkened, but at higher values of k this filter highlights the midrange values (Ragulskis *et al.*, 2006).

1.3.4. The Difference Image

The construction of a digital image communication scheme based on self-organizing patterns requires the formation of two patterns. The nonlinear model of the system governs the evolution of one pattern from a predetermined set of initial conditions – while the evolution of the second one starts from the perturbed initial conditions (Saunoriene *et al.*, 2011; Ishimura *et al.*, 2014; Ziaukas *et al.*, 2014). The secret image leaks in a form of a difference image between these two patterns. The morphological operation describing the difference pattern reads as (Vaidelys *et al.*, 2017):

$$D(x, y) = \text{abs} \left(P(x, y) - \tilde{P}(x, y) \right) \quad (20)$$

where $P(x, y)$ and $\tilde{P}(x, y)$ are the grayscale levels of the pixel (x, y) in the first and the second patterns; $D(x, y)$ denotes the difference pattern. Thus the difference image is black if two patterns are identical.

1.4. Linear Recurrent Sequences⁴

Recurrent sequences play a central role in a large variety of mathematical algorithms and applications (Telksnys *et al.*, 2016). Some of the best-known examples of recurrent sequences are used in computational biology. The logistic map was used to model the population growth (Section 1.2.1). The logistic map is often used to illustrate how complex behavior can arise from very simple equations (Strogatz, 2014), and how it is possible to model (Diaz-Mendez *et al.*, 2009), to predict (Nagatani, 2008) and to encrypt (Patidar *et al.*, 2009) different physical systems and processes.

The optimal estimation of recurrence structures in neurophysiological time series obtained from anaesthetized animals is used to classify the subject's state of consciousness (Beim *et al.*, 2016). Recurrences are widely applied in the theory of recurrence plots, which is a powerful technique for the visualization of the behavior of dynamical systems in the phase space (Marwan *et al.*, 2007). It was shown by (Villette *et al.*, 2015) that a population code integrating distance naturally emerges in the hippocampus in the form of recurring sequences.

Models incorporating linear recurrent sequences (LRS) are used in digital signal processing for system identification (Juang *et al.*, 1985); in the analysis of algorithms, the running time of an algorithm can be described in a recurrence relation if it can be broken into smaller subroutines (Sedgewick *et al.*, 2013). LRS are also used in economics where the functionality of financial sectors depends on lagged variables (Sargent, 2009). LRSs are successfully exploited for time series analysis (Ragulskis *et al.*, 2011a) and the construction of solutions to nonlinear ordinary differential equations (Navickas *et al.*, 2013).

The classical one-dimensional (1D) LRS (x_0, x_1, x_2, \dots) is defined by the linear relation (Everest *et al.*, 2003):

$$x_n = \alpha_1 x_{n-1} + \alpha_2 x_{n-2} + \dots + \alpha_n x_0, \quad (21)$$

where $\alpha_k \in \mathbb{R}$, $k = 1, \dots, n$. Given the initial values x_0, \dots, x_{n-1} , each subsequent term is determined according to (21).

There is a number of generalizations of 1D recurrent sequences to two or more dimensions. Prunescu considers recurrent two-dimensional (2D) sequences over the finite field \mathcal{A} (Prunescu, 2011b): given vectors $\lambda \in \mathcal{A}^n$, $\mu \in \mathcal{A}^m$; $n, m \in \mathbb{N}$, a recurrent 2D sequence is defined as the mapping $a: \mathbb{N} \times \mathbb{N} \rightarrow \mathcal{A}$, where:

- 1) $\forall i \geq 0: a(i, 0) = \lambda_{i \bmod n}$;
- 2) $\forall j \geq 0: a(0, j) = \mu_{j \bmod m}$;
- 3) $\forall i, j \geq 1: a(i, j) = f(a(i-1, j), a(i-1, j-1), a(i, j-1))$, where $f: \mathcal{A}^3 \rightarrow \mathcal{A}$.

⁴ Some passages have been quoted verbatim from the following source:

The Order of a 2-Sequence and the Complexity of Digital Images.
 Telksnys T., Navickas Z., Vaidelys M., Ragulskis M.
 Copyright © 2016 World Scientific Publishing Company.

It has been demonstrated that such 2D recurrent sequences can be produced by context-free substitutions and can generate realizations of well-known fractals (Prunescu, 2010). It is shown that in the case $\mathcal{A} = \mathbb{K}$, where \mathbb{K} is Klein's four-element group (the smallest noncyclic group) and f is a linear function:

$$f(x, y, z) = Ax + By + Cz, \quad A, B, C = \text{const}, \quad (22)$$

the resulting recurrent 2D sequences can be classified into 90 groups in terms of their geometric content (Prunescu, 2011a).

Multidimensional LRS and linear recurrent arrays over quasi-Frobenius rings and modules are discussed by (Lu *et al.*, 2004, Mikhalev *et al.*, 1996), respectively. It has also been demonstrated that n -dimensional LRSs over a module can be expressed in the canonical form by using eigenvalues of Hankel matrices that have been constructed from the sequence (Kurakin *et al.*, 1995).

The main objective of this section is to present an alternative definition of 2D LRS (referred to as 2-LRS) over the field of complex numbers \mathbb{C} by utilizing only 1D LRS.

1.4.1. General LRS

Let R be a commutative ring. Any function $P: \mathbb{Z}_0 \rightarrow R$ is called a sequence over ring R , and the set of all sequences is denoted as $R^{(1)}$. The elements of the sequence are denoted as p_j , $j \in \mathbb{Z}_0$, and the sequence itself is denoted as $P = (p_j, j \in \mathbb{Z}_0)$. The product of a polynomial $f(\lambda) = \sum_{s=0}^K f_s \lambda^s \in R[\lambda]$ and a sequence $P \in R^{(1)}$ is defined as:

$$f(\lambda)P = v, \quad v \in R^{(1)}, \quad v_k = \sum_{s \geq 0} f_s p_{k+s}. \quad (23)$$

Sequence $P \in R^{(1)}$ is called order m LRS (1-LRS) over R if there exists a monic polynomial $f(\lambda) \in R[\lambda]$ of order m such that $f(\lambda)P = 0$. The polynomial $f(\lambda)$ is called the characteristic polynomial of P , and the first m values of the sequence $(p_0, p_1, \dots, p_{m-1})$ are called the initial vector of P (Kurakin *et al.*, 1995).

Function $X: \mathbb{Z}_0^2 \rightarrow R$ is called a 2D sequence, and the set of all 2D sequences over R is denoted as $R^{(2)}$. In the context of this thesis, a 2D sequence can be considered as an infinite matrix or a data array, with elements denoted as x_{kl} ; $k, l \in \mathbb{Z}_0$, and the 2D sequence itself is denoted as $X = [x_{jr}]_{j,r=0}^{+\infty}$.

Let us consider a bivariate polynomial $f(\lambda, \mu) = \sum_{s=0}^K \sum_{t=0}^L f_{s,t} \lambda^s \mu^t \in R[\lambda, \mu]$. The product of a polynomial and a 2D sequence is defined as:

$$f(\lambda, \mu)X = v, \quad v \in R^{(2)}, \quad v_{k,l} = \sum_{s,t \geq 0} f_{s,t} x_{k+s, l+t}. \quad (24)$$

1.4.2. 1-LRS over \mathbb{C}

Now we expand the linear recurrent sequences over the complex field, thus $R = \mathbb{C}$. For 1-LRS over \mathbb{C} , there is a convenient criterion based on the Hankel matrix

which simplifies the determination of the order of the sequence.

Let us consider a complex-valued sequence P . By using P , a sequence of Hankel matrices ($H_n; n \in \mathbb{N}$) can be formed:

$$H_n := \begin{bmatrix} p_0 & p_1 & \cdots & p_{n-1} \\ p_1 & p_2 & \cdots & p_n \\ \cdots & \cdots & \cdots & \cdots \\ p_{n-1} & p_n & \cdots & p_{2n-2} \end{bmatrix}. \quad (25)$$

The Hankel mapping ($d_n; n \in \mathbb{N}$) reads:

$$d_n := \det(H_n). \quad (26)$$

Sequence $P = (p_j; j \in \mathbb{Z}_0)$ is of order $m \in \mathbb{Z}_0; (m < +\infty)$ 1-LRS over \mathbb{C} if the Hankel mapping of that sequence has the following structure:

$$(d_1, \dots, d_m, 0, 0, \dots), \quad (27)$$

where $d_m \neq 0$ and $d_{m+k} = 0, k = 1, 2, \dots$

1.4.3. 2D Sequences

This section is dedicated to the definition of Complex 2D sequences $X := [x_{jr}]_{j,r=0}^{+\infty}$, where $x_{jr} \in \mathbb{C}$ are considered.

Any 2D sequence features two elementary families of 1D sequences:

$$R_k(X) := (x_{kr}; r \in \mathbb{Z}_0), \quad (28)$$

for fixed $k \in \mathbb{Z}_0$ it is called the k th row sequence of X . Likewise,

$$C_l(X) := (x_{jl}; j \in \mathbb{Z}_0), \quad (29)$$

for fixed $l \in \mathbb{Z}_0$ it is called the l th column sequence of X .

1.4.4. The Order of a 2D Sequence

In this section, the order of a 2D sequence based on the concept of 1-LRS is introduced.

Let us take $X := [x_{jr}]_{j,r=0}^{+\infty}$. Let us suppose that each row sequence $R_k(X)$, $k = 0, 1, \dots$ is a 1-LRS, and Γ is the finite set of characteristic roots in row sequences $R_k(X)$, $k = 0, 1, \dots$ (omitting repetitions of roots). Thus $\Gamma = \{\gamma_1, \gamma_2, \dots, \gamma_n\}$, $n < +\infty$. The multiplicity of $\gamma_k \in \Gamma$ is defined as $n_k = \max_{j \geq 0} n_k^{(j)} < +\infty$, where $n_k^{(j)}$ is the multiplicity of γ_k in sequence $R_j(X)$ (if γ_k is not a root of the characteristic polynomial corresponding to R_j then $n_k^{(j)} := 0$). If these conditions are met, X has a row order equal to $N = \sum_{k=1}^n n_k$.

Elements of set Γ are called the row characteristic roots of X .

Let us suppose that each column sequence $C_l(X)$, $l = 0, 1, \dots$ is a 1-LRS, and that \mathcal{M} is the finite set of characteristic roots in column sequences $C_l(X)$, $l = 0, 1, \dots$ (omitting repetitions of roots). Thus $\mathcal{M} = \{\mu_1, \mu_2, \dots, \mu_m\}$, $m < +\infty$ and the

multiplicity of each $\mu_l \in \mathcal{M}$ is defined as $m_l = \max_{r \geq 0} m_l^{(r)} < +\infty$, where $m_l^{(r)}$ is the multiplicity of μ_l in sequence $C_r(X)$ (if μ_l is not a root of the characteristic polynomial corresponding to C_r then $m_l^{(r)} := 0$). If these conditions are met, X has a column order equal to $M = \sum_{l=1}^m m_l$.

Elements of set \mathcal{M} are called the column characteristic roots of X .

A 2D sequence X has a 2D order ord_2 if it has both a row order and a column order. It is denoted as:

$$\text{ord}_2 X = (N, M), \quad (30)$$

where N is the row order and M is the column order of X . If X only has a finite row or a column order, it is denoted as:

$$\text{ord}_2 X = (N, +\infty), \quad \text{ord}_2 X = (+\infty, M), \quad (31)$$

respectively. If X has neither a finite row nor a column order, the notation is:

$$\text{ord}_2 X = (+\infty, +\infty). \quad (32)$$

It can be proved that a 2D sequence has a finite order if and only if it can be written in the canonical form (Telksnys *et al.*, 2016).

Let us suppose that $X = [x_{jr}]_{j,r=0}^{+\infty}$ is a 2D sequence with $\text{ord}_2 X = (N, M)$. Then, any element of X can be expressed as:

$$x_{jr} = \sum_{k=1}^n \sum_{s=0}^{n_k-1} \sum_{l=1}^m \sum_{t=0}^{m_l-1} c_{kl}^{(st)} \binom{r}{s} \binom{j}{t} \lambda_k^{r-s} \mu_l^{j-t}, \quad (33)$$

where $\lambda_k, k = 1, \dots, n; \mu_l, l = 1, \dots, m$ are the row and column characteristic roots, respectively, with multiplicities $n_k, k = 1, \dots, n$ and $m_l, l = 1, \dots, m; c_{kl}^{(st)} \in \mathbb{C}$ are constants which do not depend on j and r .

The reversed statement is also true. Let us suppose that any element of a 2D sequence X can be written as in (33). Then, $\text{ord}_2 X = (N, M)$.

1.5. Concluding Remarks

Our literature review shows that secure transfer of digital information is of utmost importance; although a lot of approaches exist and are implemented in everyday life, risks to data security are still significant. One of the best concepts of data protection is to conceal it in such a way that no one even knows it exists. Thus visual information hiding methods based on the formation of a self-organizing pattern and dynamic visual cryptography in conjunction with a secure visual communication scheme are investigated in this thesis. Computational tools for the pattern formation based on physical processes and harmonic oscillations of the deformable harmonic moiré grating shall be developed. A tool to evaluate the pattern suitability for secure information hiding shall be introduced.

2. VISUAL INFORMATION HIDING. THE USE OF SELF-ORGANIZING PATTERNS⁵

This Section presents several approaches to the generation of self-organizing patterns and demonstrates the hiding and transmission of secret visual information between two communicating parties.

Pattern formation algorithms developed and presented in previous researches do exhibit a number of drawbacks in secret image communication applications. The self-organized pattern produced in a model of reaction-diffusion cellular automata clearly resembles the initial fingerprint image and cannot be considered as an image hiding algorithm. Despite this fact, it was adapted for steganographic communication algorithm by (Ishimura *et al.*, 2014). Self-organizing patterns induced by the Turing instability and produced by the Beddington-DeAngelis-type predator-prey model have been successfully used in a secure steganographic communication algorithm (Saunoriene *et al.*, 2011; Ishimura *et al.*, 2014). However, the reaction-diffusion models have the main computational speed drawback which is influenced by the computational solution of PDE where at least 10000-time forward iterations are required for the formation of an interpretable pattern. The speed issue is solved in the evolutionary spatial 2×2 game (ESG) model (Ziaukas *et al.*, 2014); yet, another question arises concerning the system insensitivity to small local perturbations. This fact is based on the property of ESG where the strategy of a single individual does not determine the resulting strategy of the whole population.

Thus an effective application of a communication algorithm based on self-organizing patterns needs to satisfy several important requirements. First of all, this algorithm should be steganographically secure. Image steganography is the science of concealing secret images within other digital cover images (Nakamura *et al.*, 2011). The advantage of steganography, over cryptography alone is that steganography can be said to protect not only messages but also communicating parties, whereas cryptography protects only the content of a message (Clayton *et al.*, 2011). Secondly, the secret visual information should be encoded in the random image of the initial conditions by using slight modifications of only several individual pixels; all the modifications should be lower than the noise level of the

⁵ Some passages have been quoted verbatim from the following sources:

Competitively Coupled Maps for Hiding Secret Visual Information.

Vaidelys M., Ziaukas P., Ragulskis M.

Copyright © 2015 Elsevier B.V.

Image Hiding Scheme Based on the Atrial Fibrillation Model.

Vaidelys M., Ragulskiene J., Ziaukas P., Ragulskis M.

Applied Sciences, 2015.

Digital Image Communication Scheme Based on the Breakup of Spiral Waves.

Vaidelys M., Lu C., Cheng Y., Ragulskis M.

Copyright © 2016 Elsevier B.V.

initial conditions. Finally, the communication algorithm should be computationally effective – the number of time forward steps used for the development of self-organizing patterns should be small. An important objective of this section is to develop a computationally effective visual communication scheme based on self-organizing patterns which could preserve the security of the communication but minimize drawbacks mentioned in the previously suggested communication schemes.

This Section is organized as follows. Communication algorithm based on competitively coupled maps using the Maynard Smith model are presented in Subsection 2.1 (Vaidelys *et al.*, 2016); the image hiding scheme based on the atrial fibrillation model is presented in Subsection 2.2 (Vaidelys *et al.*, 2015c); Digital image communication scheme based on the breakup of spiral waves is presented in Subsection 2.3 (Vaidelys *et al.*, 2017); concluding remarks are outlined in the final subsection.

2.1. Competitively Coupled Maps for Hiding Secret Visual Information⁶

A novel digital image hiding scheme based on competitively coupled maps model described in Subsection 1.2.2 is presented in this Subsection. Self-organizing patterns produced by an array of non-diffusively coupled nonlinear maps are employed to conceal the secret. The secret image is represented in the form of a dot-skeleton representation and is embedded into a spatially homogeneous initial state far below the noise level. Self-organizing patterns leak the secret image at a predefined set of system parameters. Computational experiments are used to demonstrate the effectiveness and the security of the proposed image hiding scheme.

2.1.1. Self-Organizing Patterns

The chaotic logistic map (see Subsection 1.2.1) is used for the efficient generation of the initial states of all elements of 200×200 domain over the interval $[0,1]$. The initial digital image is illustrated in Fig. 2.1.

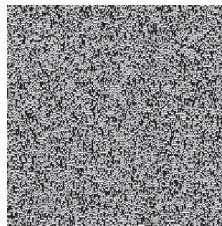


Fig. 2.1. Pseudorandom initial conditions generated sequentially by the logistic map; the initial value is $a_0 = 0.05$; the dimensions are $L_x = L_y = 200$.

⁶ *The results presented in this section have been published as:*

Competitively Coupled Maps for Hiding Secret Visual Information.
Vaidelys M., Ziaukas P., Ragulskis M.
Copyright © 2015 Elsevier B.V.

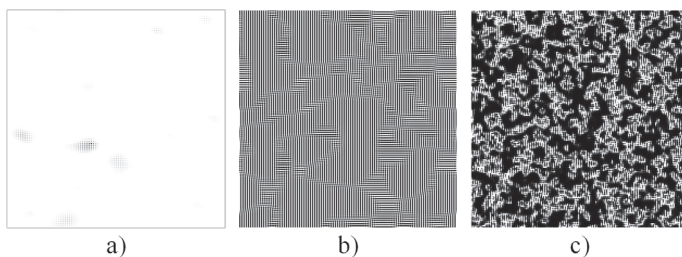


Fig. 2.2. Patterns produced by the Maynard Smith map (5) depend on the system's parameters. The set of parameters $\eta = 5$, $\alpha = 0.25$, $b = 1$ does not produce an interpretable pattern even after 300 iterations (a). $\eta = 4$, $\alpha = 0.26$, $b = 2$ produces an interpretable pattern after 300 iterations (b). $\eta = 7$, $\alpha = 0.3$, $b = 4$ also results in a developed pattern after only 6 iterations (c). All the three patterns have been generated from the same initial conditions in Fig. 2.1.

It is clear that the η and b parameters of the Maynard Smith function (5), as well as the strength of the competitive interaction between the neighboring elements α and the number of iterations n have a strong effect on the formation of self-organizing patterns given a spatially homogeneous initial state. Different combinations of these parameter values result in the formation of different patterns (or even the absence of interpretable patterns at all) – some typical situations are illustrated in Fig. 2.2. The set of parameters $\eta = 5$, $\alpha = 0.25$, $b = 1$ does not produce an interpretable pattern even after 300 iterations from the initial conditions shown in Fig. 2.1 (Fig. 2.2(a)). Parameters $\eta = 4$, $\alpha = 0.26$, $b = 2$ yield an interpretable pattern after 300 iterations (Fig. 2.2(b)) from the same initial conditions. Finally, $\eta = 7$, $\alpha = 0.3$ and $b = 4$ also result in a developed pattern but after only as few as 6 iterations (Fig. 2.2(c)) from the same initial conditions. The size of all the digital images in Fig. 2.2 is $L_x = L_y = 200$; the periodic boundary conditions are set along the borders of the image.

2.1.2. A Communication Scheme Based on Self-Organizing Patterns

Self-organizing patterns (SOP) can be efficiently exploited as cover images for the transmission of secret visual information. The communication scenario between the Sender and the Receiver can be described by the scheme below (see Steps 1–6).

The Sender and the Receiver can use an asymmetric (arbitrary) protocol in order to determine initial value a_0 , and the number of time-forward iterations n for SOP generation (parameters of SOP η , α , b , L_x , L_y must be determined beforehand):

1. The Sender generates the pseudo-random matrix of initial conditions (as introduced in Subsection 2.1.1) by using the Logistic map and value a_0 ; the size of the matrix is $L_x \times L_y$.

2. The Sender modifies the pseudo-random matrix of the initial conditions by adding or subtracting a small number δ to/from some pixels. Usually, δ is much lower than the range (the difference between the highest and the lowest values) of the initial conditions.

3. The Sender executes the SOP n forward iteration algorithm (as introduced in subsection 2.1.1) starting from the modified initial conditions and sends the SOP

image to the Receiver.

4. The Receiver generates the pseudo-random matrix of the initial conditions by using the Logistic map and value a_0 ; the size of the matrix is $L_x \times L_y$ (this is an identical image to the one generated by the Sender in Step 1).

5. The Receiver executes the SOP n forward iteration algorithm starting from the non-modified initial conditions.

6. Finally, the difference (Section 1.3.4) between the SOP image produced by the non-modified and the modified initial conditions reveals the secret.

It can be noted that instead of the whole dichotomic silhouette of the secret image one may use skeleton dots corresponding to the contour instead (the dot-skeleton representation of the secret image).

It is clear that not all values used as SOP parameters (η , α , b) would be applicable for such a communication scheme (even if the values of parameters do ensure the evolution of a well-developed SOP). Let us assume that a dot-skeleton representation of the secret image is a regular array of dots (Fig. 2.3(a)). We set $\delta = 0.01$ and modify the image of pseudorandom initial conditions in Fig. 2.1 by randomly adding or subtracting 0.01 to/from the grayscale level of the corresponding pixels. We should note that the values of pixels generated by the chaotic Logistic map are distributed in the interval $[0,1]$ – thus all the perturbations we make are much weaker than the noise level of the initial conditions.

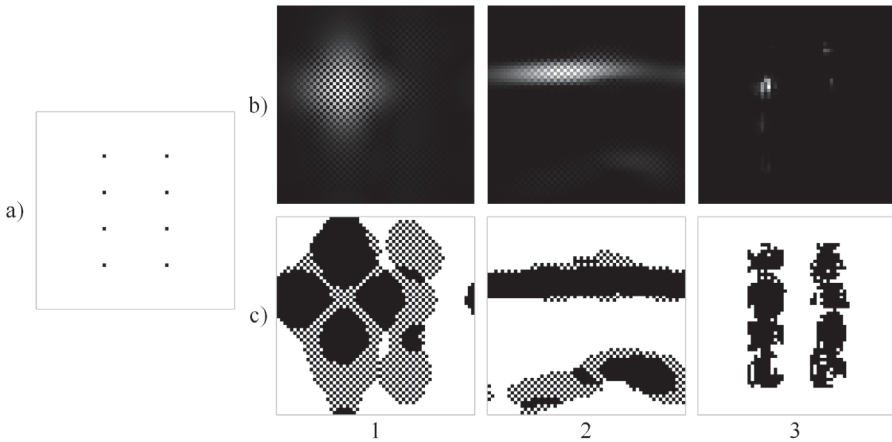


Fig. 2.3. The difference image between the patterns produced by random initial conditions and modified initial conditions by the dot-skeleton representation as shown in part (a). Column 1 represents the set of parameters $\eta = 5$, $\alpha = 0.25$, $b = 1$; column 2 represents the set of parameters $\eta = 4$, $\alpha = 0.26$, $b = 2$; column 3 represents the set of parameters $\eta = 7$, $\alpha = 0.3$, $b = 4$. The difference images are presented in row (b); the difference images with an enhanced contrast are presented in row (c). Parameter sets in columns (1) and (2) do fail to recreate the hidden information, while the parameter set in column (3) produces a satisfactory result.

It is natural to expect that the first parameter set used in Fig. 2.2 would not produce any interpretable pattern in the difference image – the perturbation in the initial conditions causes some uninterpretable fluctuations in the difference image

(Fig. 2.3(b), column 1). The contrast of the difference image can be sharpened by using digital morphological operations like the one presented in Section 1.3.1 (Fig. 2.3(c), column 1) – but the difference image is still uninterpretable.

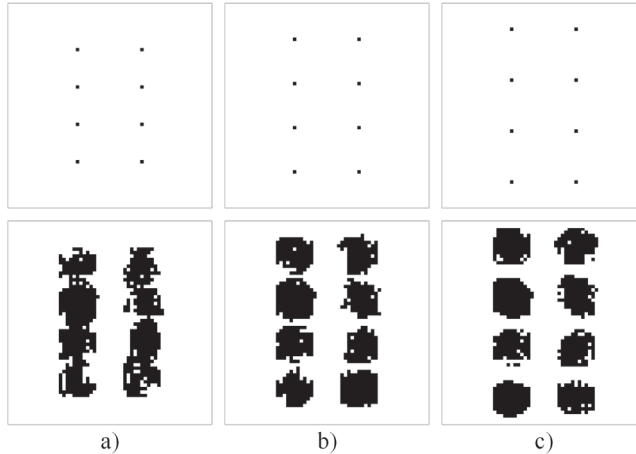


Fig. 2.4. The optimal density of dot-skeleton points in the case of parameters $n = 6$, $L_x = L_y = 50$, $\eta = 8$, $\alpha = 0.3$, $b = 4$. Figures in the upper row show the dot-skeletons; figures in the lower row illustrate the highlighted difference images. Distances between skeleton dots in cases (a), (b) and (c) are 10, 12 and 14, respectively.

However, surprisingly, the second parameter set used in Fig. 2.2 does not produce any meaningful information, either (Fig. 2.3(b) and 2.3(c), column 2). However, the third set of parameters does produce an interpretable pattern in the difference image (Fig. 2.3(b) and 2.3(c), column 3).

Figure 2.4 illustrates the formation of two parallel lines in the difference image from the dot-skeleton representation of these lines in the random image of the initial conditions. It is clear that different distances between dot-skeleton points may not result in the formation of continuous lines in the difference image. Thus the optimal density of dot-skeleton points for the formation of continuous line-type objects in the difference image is 10 pixels; we should note that the width of the resulting lines is about 13 pixels (Figure 2.4(a)).

Finally, the communication scheme based on SOP generated by competitively coupled maps can be illustrated by the following flow chart diagram in Figure 2.5. The original secret image is shown in part (a); the dot-skeleton representation of the secret image is shown in part (b). The sender retrieves parameter a_0 and generates the random image of initial conditions by using the Logistic map (part (c)). The dot-skeleton representation of the secret image is embedded into the random image of initial conditions by randomly adding or subtracting 0.01 to/from the corresponding pixels of the random image (part (d)). We should note that all the deformations of the image of the initial conditions are far below the noise level.

Next, the sender executes the pattern formation algorithm and produces the SOP image (part (f)) from the modified initial conditions (part (d)). In order to conceal the transmission of a suspicious image of SOP, the sender uses a standard cover image (part (e)) and a standard least significant bit based stenographic

algorithm (Section 1.1.3) for hiding the SOP image (part (f)) in the cover image. The resulting image (part (g)) is transmitted to the receiver.

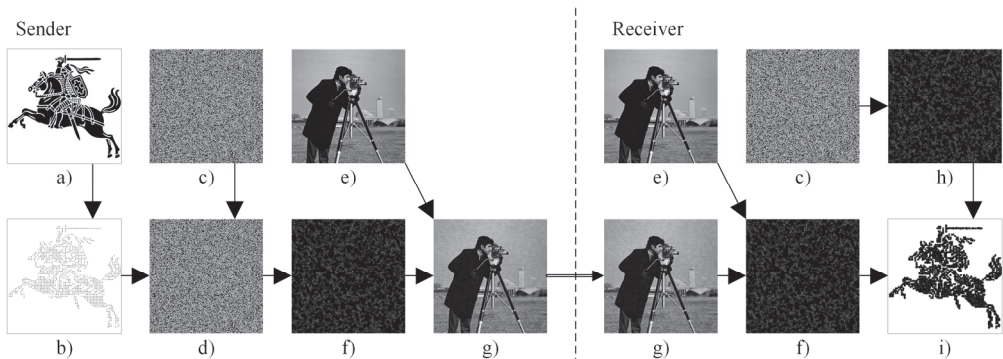


Fig. 2.5. Flow chart diagram of the communication algorithm. The original image (a); the dot-skeleton representation (b); the initial conditions (c); the perturbed initial conditions (d); the cover image (e); the perturbed self-organizing pattern (f); the perturbed cover image (g); the self-organizing pattern (h); the difference image (i).

The receiver uses the same cover image (part (e)) and the received image (part (g)) to reproduce the SOP image (part (f)). We should note that the SOP image (part (f)) has been produced from the initial conditions with the embedded dot skeleton representation of the secret image.

Then, the receiver retrieves parameter a_0 and generates the random image of the initial conditions by using the Logistic map (part (c)). The receiver uses the identical pattern formation algorithm as used by the sender and produces his copy of the SOP image (part (h)). The difference image between two SOP images reveals the secret (part (i)).

2.1.3. Sensitivity of the Communication Scheme to the Perturbation of Parameters

As mentioned previously, the presented communication scheme does function at preset values of the system parameters. Slight changes of these parameters (when the Sender and the Receiver use different parameters) may compromise the communication system.

Figure 2.6 illustrates the sensitivity of the communication system to slight perturbations; all the illustrations represent difference images in the enhanced contrast mode (similarly as used in Fig. 2.3, 2.4, 2.5). Initially, we perturb the random initial conditions. The Sender uses all the system parameters as preset in the computational experiment illustrated in Fig. 2.5 ($a_0 = 0.05$, $\eta = 7$, $\alpha = 0.3$, $b = 4$) – but the Receiver uses $a_0 = 0.0501$ instead of $a_0 = 0.05$. The chaotic Logistic map is sensitive to small perturbations – thus it is natural to expect that the evolving patterns from different initial conditions would result in a completely different SOP image which is not applicable for the reconstruction of the embedded secret. As expected, the resulting difference image (Fig. 2.6 (a)) is completely uninterpretable.

The next computational experiment simulates an attack of parameter η . The receiver mistreats parameter η by using $\eta = 7.01$ instead of $\eta = 7$. The change is

crucial enough to make the difference image (Fig. 2.6 (b)) uninterpretable. Analogously, competitive parameter $\alpha = 0.301$ is used instead of $\alpha = 0.3$. The resulting difference image (Fig. 2.6 (c)) is meaningless. Finally, $b = 4.01$ is taken instead of $b = 4$ by the receiver. Once again, this results in a failure to obtain a meaningful difference image (Fig. 2.6 (d)).

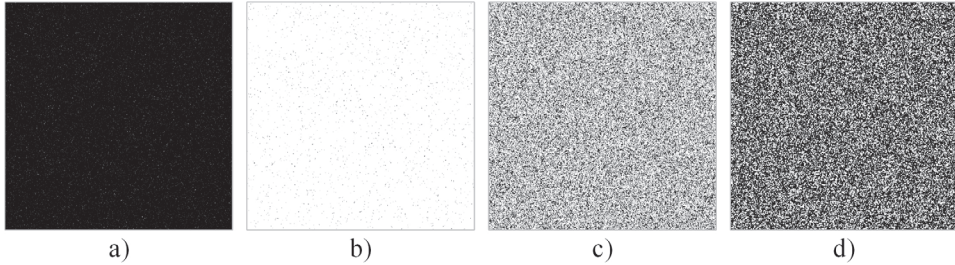


Fig. 2.6. Initial parameters used by the Sender are: $a_0 = 0.05$, $\eta = 7$, $\alpha = 0.3$, $b = 4$. The perturbation of one parameter by the Receiver results in an uninterpretable difference image (a single perturbation of one parameter is used in every part respectively):
 (a) $a_0 = 0.0501$; (b) $\eta = 7.01$; (c) $\alpha = 0.301$; (d) $b = 4.01$.

2.2. Image Hiding Scheme Based on the Atrial Fibrillation Model⁷

An image communication scheme based on the atrial fibrillation (AF) model described in Subsection 1.2.3 is presented in the present Subsection. Self-organizing patterns produced by the AF model are used to hide and transmit secret visual information. A secret image is encoded into the random matrix of initial cell excitation states in the form of a dot-skeleton representation. Self-organized patterns produced by such initial cell states ensure a secure and efficient transmission of secret visual images. The mentioned feature was missing in self-organized patterns produced by competitively and non-diffusively coupled non-linear maps (Vaidelys *et al.*, 2016) in Subsection 2.1 where wave propagation in isotropic media predetermines a rather low complexity of the pattern structure.

It is well known that patterns produced by the atrial fibrillation (AF) model originate from complex rules of self-organization and wave propagation in anisotropic media. The ability to exploit this complex pattern formation phenomenon in a digital image communication scheme is the main goal of this subsection. Procedures for digital encoding and decoding of secret images, as well as the sensitivity of the communication scheme to the perturbation of the AF model's parameters are demonstrated in this Subsection.

⁷ The results presented in this section have been published as:

Image Hiding Scheme Based on the Atrial Fibrillation Model.
 Vaidelys M., Ragulskiene J., Ziaukas P., Ragulskis M.
 Applied Sciences, 2015

2.2.1. The Generation of Self-Organizing Patterns Based on Atrial Fibrillation Model

The initial computational setup of the AF model as illustrated in Figure 1.8 requires many time-forward interactions for the formation of well-developed patterns. The wave front must propagate over all the plane (and, preferably, more than once); it has to collide with all the dysfunctional cells.

Let us consider an alternative computational setup where pacemaker cells are randomly distributed across a 2D plane. Now, wave propagation continues in all directions, which makes waves collide with each other. The benefit of such AF model implementation is that it requires less than 1% cells to be initially excited in order to form self-organized patterns (Fig. 2.7).

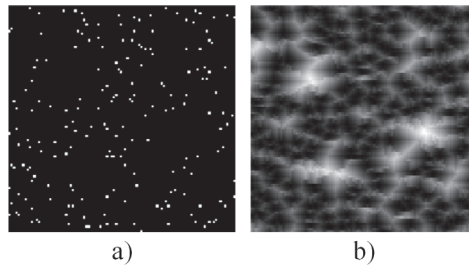


Fig. 2.7. Initial cell state conditions (a) and the resulting pattern after 20 iterations (b).
Parameter ν is set to 0.5; $\tau = 20$.

The computational efficiency of the numerical AF scheme can be enhanced even further by decreasing real pacing times τ of the cells. Optimal pacing time τ depends on the number of initially excited cells and on the length of simulation. If τ is excessively small, not all plane cells become excited, thus the pattern does not fully form. Otherwise, a too long refractory period results in a relatively static pattern since the process cannot evolve freely.

2.2.2. Initial Conditions

The initial states of all the cells are set as randomly uniformly distributed numbers over the real interval $[0; 1]$. Connections between cells in the transversal direction are distributed randomly as well. A pseudo-random number generator can be used for the reduction of the amount of information needed to define a unique configuration of the AF model. The benefit of such an approach is that a single seed of the random number generator defines all the states and connections between cells.

Let us consider a regular grid with periodic boundary conditions. The chaotic logistic map (Eq. (4)) with the initial value $a_0 = 0.02$ is used to generate a chaotic sequence; the generated discrete values of the sequence are sequentially assigned to every node on the grid (row by row). The resulting digital image is illustrated in Figure 2.8 (here, 0 corresponds to the black color; 1 denotes the white color; all the intermediate values are depicted by the appropriate grayscale levels).

The initial cell dichotomous states are now defined by a simple binary rule. A cell is set to be in the excited state if the value of the grid node is lower than δ ; $0 < \delta \ll 1$. Thus only $\delta \cdot 100\%$ cells would be excited in the initial state.

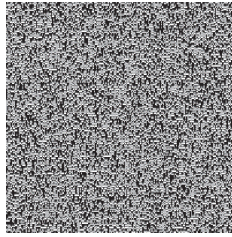


Fig. 2.8. Pseudorandom initial conditions generated sequentially by the Logistic map; the initial value of the Logistic map a_0 is set to 0.02.

The same rule is used to generate the connection map; yet, the transversal connection probability ν is used instead of δ to describe transversal connections. In addition, a different a_0 could be used in this Logistic map.

2.2.3. Parameters of the AF Model

The resulting SOP governed by the AF model depends on a few parameters:

1. The cell excitation probability δ (in random initial conditions);
2. The connection map with the corresponding probability of transversal connections ν ;
3. Refractory period τ ;
4. The number of time-forward iterations n .

Some of the typical patterns are illustrated in Figure 2.9. It is clear that different connection maps result in the apparent effect of stretching – smaller values of ν result in a rather rhombus-like form of patterns; the larger values of ν result in more horizontally stretched shapes (Figs. 2.9 (a, b)).

Another important parameter is the number of time-forward iterations n . It appears that the richest pattern is formed when n is close to the refractory period τ (Fig. 2.9 (d)). Only some of the cells are excited in a small number of time-forward iterations (Fig. 2.9 (c)). Relatively large regions of cells remain unexcited. The boundaries of these black regions seem to be discontinuous due to the complexity of interactions between cells. All cells start converging to the resting state when the number of time-forward steps considerably exceeds the refractory index (Fig. 2.9 (e)).

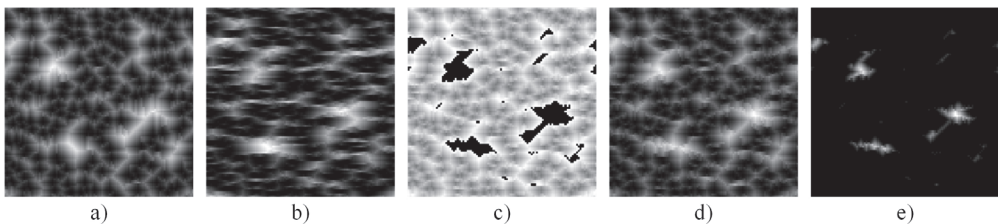


Fig. 2.9. Comparison of self-organizing patterns (SOP) for different values of parameters. (a) $\nu = 0.1$, $\tau = 20$, $n = 20$, $\delta = 0.001$; (b) $\nu = 0.9$, $\tau = 20$, $n = 20$, $\delta = 0.001$; (c) $\nu = 0.5$, $\tau = 20$, $n = 10$, $\delta = 0.001$; (d) $\nu = 0.5$, $\tau = 20$, $n = 20$, $\delta = 0.001$; (e) $\nu = 0.5$, $\tau = 20$, $n = 30$, $\delta = 0.001$.

Refractory period τ cannot be too short – a sufficient number of cells must be

excited for the formation of an interpretable self-organized pattern. On the other hand, the number of initially excited cells is too high, and the developed patterns are too scrambled if probability δ is too high (Fig. 2.10 (a)). The formation of such a pattern does not require a long refractory period; however, the pattern becomes static after a few iterations, and then it fades out altogether (Fig. 2.10). We should note that all the patterns illustrated in Figure 2.10 are normalized to the full grayscale range – therefore some patterns appear brighter whereas some others seem to be darker.

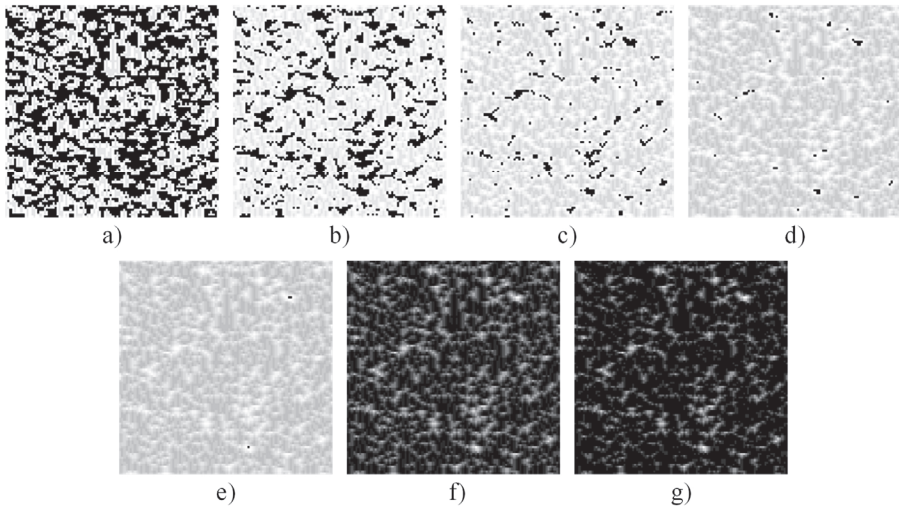


Fig. 2.10. Iterative processes at $\nu = 0.5$, $\tau = 10$, $\delta = 0.1$. (a) $n = 1$; (b) $n = 2$; (c) $n = 3$; (d) $n = 4$; (e) $n = 5$; (f) $n = 8$; (g) $n = 11$.

Cell excitation probability δ is closely related to the number of iterations n (in terms of the richness of the pattern). In general, it is better to fix the number of iterations so that the formation of static images can be prevented. In this particular case, the best results are produced at $\tau = n$.

2.2.4. A Communication Scheme Based on Self-Organizing Patterns

As mentioned above, SOPs can be successfully employed to transmit secret visual information between the communicating parties. A typical communication scenario is presented in a scheme that consists of the following steps.

Initially, the Sender and the Receiver must use an asymmetric (arbitrary) protocol in order to determine the initial value a_0 and the number of time-forward iterations n (parameters ν , τ , δ , L_x , L_y must be determined beforehand).

1. The Sender generates pseudo-random matrices of the initial cell excitation states and the connection map by using the Logistic map with the initial value a_0 ; the size of the matrix is set to $L_x \times L_y$; the parameters of the AF model are ν and δ . The initial random matrix is dichotomous (its cells contain binary values 0 or 1); the connections between cells are random.

2. The Sender modifies the pseudo-random matrix of the initial cell excitation states by inverting pixels corresponding to the dot-skeleton representation of the

secret image.

3. The Sender executes n time-forward iterations starting from the modified matrix of the initial conditions and sends the image of the self-organized pattern to the Receiver.

4. The Receiver generates the identical copy of pseudo-random matrices of the initial cell excitation states and the connection map by using the chaotic Logistic map with the initial value a_0 and the parameters of the AF model (specifically, ν and δ); the size of the matrix is $L_x \times L_y$ (this is an identical copy of the matrix generated by the Sender in Step 1).

5. The Receiver executes n time-forward iterations starting from the non-modified initial conditions.

6. Finally, the difference (see Section 1.3.4) between the digital images of the patterns produced by the non-modified and modified initial conditions reveals the secret.

Unfortunately, a straightforward inversion of the pixel values in the areas occupied by the secret image (in the digital image of the initial conditions) does not work well in general (Fig. 2.11). The ‘secret’ image is shown in Figure 2.11 (a); the digital image representing the initial conditions (with inverted pixels in the zones occupied by the secret information) is shown in Figure 2.11 (b). The self-organized pattern is illustrated in Figure 2.11 (c). It is clear that such a pattern is not safe – even a naked eye can detect the contours of the secret original image. The difference image is shown in Figure 2.11 (d); the binarized difference image (Section 1.3.1) is shown in Figure 2.11 (e). Thus the image hiding scheme proposed by (Ziaukas *et al.*, 2014) cannot be used with the AF model. However, single dot (1×1 pixel) inversions in the initial conditions are not interpretable in self-organized patterns (Fig. 2.11) – thus the further image communication scheme is based on the single pixel inversion strategy.

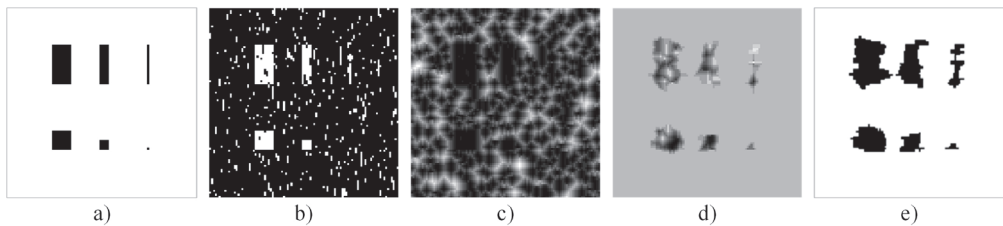


Fig. 2.11. Big clusters of initially excited cells result in interpretable self-organized patterns ($\nu = 0.5$, $n = \tau = 20$, $\delta = 0.01$). (a) The secret image; (b) initially excited cells (shown in white); (c) the self-organized pattern; (d) the difference image; (e) the binarized initially excited cells.

A huge difference in the shape of the ‘secret’ images can be seen in Figure 2.11 (a, e). It is clear that not all of the parameters considered in the SOP model (a_0 , ν , δ) are equally applicable for the proposed communication scheme (even if an adequate formation of the self-organizing pattern is ensured). Firstly, the initial random background used for the initial excitation should be close to uniform (or homogeneous) in order to avoid empty spaces and larger initial cell clusters.

Secondly, δ directly affects the clearness of the resulting image (Fig. 2.11 (c)) as well as the easier interpretation of the difference image (Fig. 2.11 (d)). Meanwhile, probability ν does not have a major effect except for stretching; however, it is recommended to keep it within the range (0,1) and not to use the trivial cases (0 or 1).

Let us consider four groups of dots presented in a regular array (Fig. 2.12 (a)). The dots in four groups are respectively 15, 10, 5, 3 pixels away from each other. Figure 2.12 illustrates the difference images at different values of parameter δ . It can be seen that, depending on the cell probability to be excited (parameter δ), the required minimum distance from the dots (in the secret image) varies. A better information visibility of the decoded image is ensured by higher values of δ . However, the denser initially excited cells lead to a lower number of resting cells – and this results in a lower number of iterations required for a fully developed pattern. On the other hand, a smaller number of iterations results in smaller changes in the initial image.

The secret visual communication scheme based on SOP in the AF model can be illustrated in Figure 2.13 ($\nu = 0.2$, $\tau = n = 20$, $\delta = 0.08$). Before the transmission takes place, the original secret image is transformed into a dot-skeleton equivalent. System parameters ν , τ , δ , L_x , L_y must be determined beforehand. Finally, the pseudo-random number seed a_0 and the number of iterations n are transmitted by using secure communications channels.

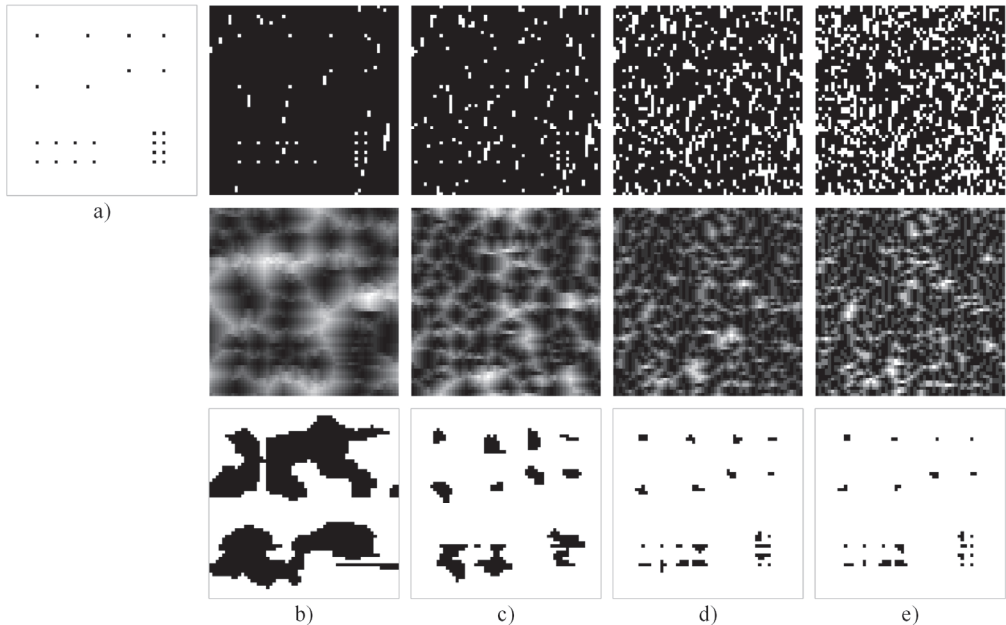


Fig. 2.12. The initial dot-skeleton image (a) and SOP at different δ : the first row represents the initial conditions; the second row shows patterns; the third row contains binarized difference images. (a) $\delta = 0.001$ (b) $\delta = 0.01$ (c) $\delta = 0.1$ (d) $\delta = 0.2$.

The original secret image is shown in Figure 2.13 (a). Its dot-skeleton

equivalent is illustrated in Figure 2.13 (b). By using parameter a_0 (as well as parameter δ), the Sender generates initially excited cells (Fig. 2.13 (c)). The initial states of the cells are inverted according to the dot-skeleton representation (Fig. 2.13 (d)). The resulting self-organizing pattern is shown in Figure 2.13 (f). This pattern can be placed on top of the standard cover image (Fig. 2.13 (e)) by using the least significant bit (LSB) steganographic technique (Fridrich *et al.*, 2001). This is a standard spatial domain steganographic technique which manipulates the LSB of pixels in order to embed the secret information in the cover image (Section 1.1.3). The final cover image ready to be sent over to the Receiver via an open communication channel is shown in Figure 2.13 (g).

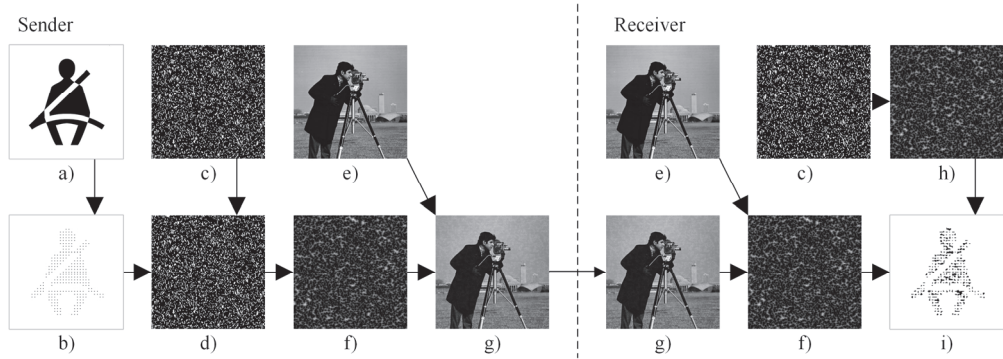


Fig. 2.13. The flow chart diagram of the communication algorithm. Original image (a); dot-skeleton representation (b); initial conditions (c); perturbed initial conditions (d); cover image (e); perturbed self-organizing pattern (f); perturbed cover image (g); self-organizing pattern (h); binarized difference image (i).

The Receiver obtains the cover image (Fig. 2.13 (g)) and reproduces the pattern (Fig. 2.13(f)) by using a clean copy of the cover image (Fig. 2.13 (e)).

The remaining procedure for the Receiver is to simply re-generate the initial array of pseudo-randomly excited cells (as shown in Figure 2.13 (c)) and to generate the pattern (the parameters of the AF model are privately known in advance) – the alternative pattern is illustrated in Figure 2.13 (h). Finally, the difference image between the two (Fig. 2.13 (f) and Fig. 2.13 (h)) reveals the secret message as shown in Figure 2.13 (i).

2.2.5. The Sensitivity of the Communication Scheme to Perturbations of System Parameters

The proposed communication scheme does actually work well with a preselected set of system parameters. Slight changes in the parameter values (when the Sender and the Receiver use different parameters) would compromise the communication system. Figure 2.14 illustrates the sensitivity of the communication system to perturbations; all the illustrations represent difference images in the enhanced contrast mode. We set initial parameters to: $n = 20$, $\tau = 20$, $\nu = 0.2$, $\delta = 0.08$, $a_0^{ex} = 0.02$, $a_0^{con} = 0.02$, where a_0^{ex} is the initial value of the chaotic logistic map used to select the initially excited cells, and a_0^{con} is the initial value of the

transversal connection map.

The Sender uses all the system parameters as preset in the computational experiment illustrated in Figure 2.13 – but the Receiver uses $a_0^{ex} = 0.021$ instead of $a_0^{ex} = 0.02$ (Fig. 2.14 (a)). The chaotic Logistic map is sensitive to small perturbations – thus it is natural to expect that the evolving patterns from different initial conditions would result in a different SOP image. The correct initial cell excitation map is essential in order to show the embedded secret (Fig. 2.13 (a)). However, the AF model construction allows some perturbations in the connection map (Fig. 2.14 (b)); thus a different map does not completely break down the results, and visual interpretation of the embedded secret is still possible.

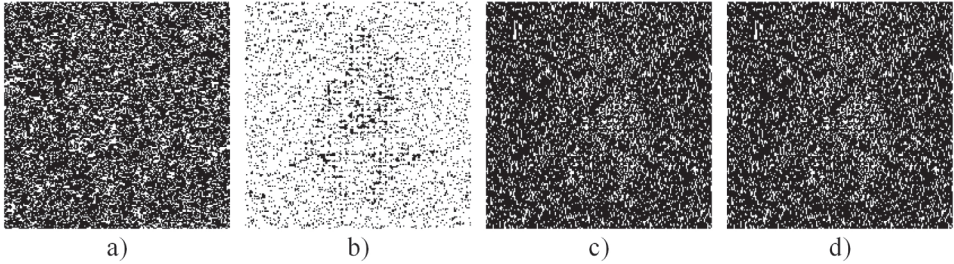


Fig. 2.14. The sensitivity of the communication scheme to the perturbation of the system parameters. The difference images are shown when: (a) $a_0^{ex} = 0.021$ is used instead of 0.02; (b) $a_0^{con} = 0.021$ is used instead of 0.02; (c) $n = 21$ is used instead of 20; (d) $\tau = 19$ is used instead of 20.

Perturbations can be introduced in the number of iterations n and in the refractory period of the cells τ . It can be noted that differences are only visible when $\tau < n$. Otherwise, the model does not reach the breaking point when cells finish their relaxation period. As it can be seen in Figure 2.14 (c, d), changes by one time-step do hide most of the embedded image, but if the change is even higher, the difference image does not reveal any secret.

2.3. Digital Image Communication Scheme Based on the Breakup of Spiral Waves⁸

All the previously discussed digital image communication schemes are based on some sort of modification of the initial conditions in a self-organizing pattern formation. The secret image is represented in the form of a dot-skeleton representation and is embedded into a spatially homogeneous random initial state far below the noise level (Saunoriene *et al.*, 2011; Ishimura *et al.*, 2014; Subsections 2.1 and 2.2). Dichotomous pixels in the initial conditions are inverted in the regions

⁸ The results presented in this section have been published as:

Digital Image Communication Scheme Based on the Breakup of Spiral Waves.
Vaidelys M., Lu C., Cheng Y., Ragulskis M.
Copyright © 2016 Elsevier B.V.

corresponding to the secret image (Ziaukas *et al.*, 2014). These self-organized patterns in digital image communication schemes are induced by spatially homogeneous random initial conditions. The generation of initial conditions is an integral part of all these communication schemes. For example, Subsection 2.2 shows that a slight variation in the random initial conditions completely compromises the communication algorithm.

In other words, the generation of random initial conditions and an appropriate modification of these initial conditions lies in the backbone of the discussed communication algorithms. Therefore, the parameters determining the generation of random initial conditions are an integral part of the set of private and public keys of the communication algorithm. The ability to avoid the necessity of using random initial conditions for the generation of a self-organizing pattern would be a serious enhancement in terms of the security of the communication scheme. On the other hand, it would be advantageous if the communication scheme could avoid the use of the perturbation of initial conditions. That would prevent the cheating attack against the communication scheme – and also an eavesdropper would not be able to embed fake secret images – even if all the keys of the communication scheme had been compromised (i.e., known to the eavesdropper).

The main objective of this Subsection is to develop such a digital image communication scheme based on self-organizing patterns that would neither use random initial conditions nor require any perturbations of the initial conditions. Clearly, a new approach is required for the physical model governing the formation of self-organizing patterns as well as for the concept of the communication scheme itself.

2.3.1. The Formation of the Difference Image

Several different perturbation models in the initial conditions are used to illustrate the formation of difference images D (see Section 1.3.4) in the spiral wave with the breakups model presented in Subsection 1.2.4. The parameters of the system are kept the same as described in Fig. 1.10; the time interval used for the evolution of the pattern is set to $T = 70$. The initial values of the v -field are kept the same as in Fig. 1.10; the initial values of the u -field are modified by changing the numerical value in the right part of the field from 1 to 0.99. Such perturbation of the initial conditions is similar to the perturbation used in (Ziaukas *et al.*, 2014) where an inversion of a single pixel does not change the self-organizing pattern, and manipulation with blocks of pixels is required for generating any changes in the difference image.

The left image in row (a) in Fig. 2.15 shows unmodified pattern P (this is the same image as the rightmost pattern in Fig. 1.10). The middle image in row (a) in Fig. 2.15 is pattern \tilde{P} evolved from the modified initial conditions. The right image in row (a) in Fig. 2.15 is the difference pattern between P and \tilde{P} . It can be seen that the perturbation in the initial conditions spread across the whole domain. Moreover, this perturbation is clearly visible in the difference image – no contrast enhancement techniques are required to visualize the pattern in the difference image. This is a serious improvement compared to the previously proposed digital image

communication schemes where contrast enhancement of the difference image is an integral part of these schemes (Saunoriene *et al.*, 2011; Ishimura *et al.*, 2014; Ziaukas *et al.*, 2014; Subsections 2.1 and 2.2).

However, it appears that the evolution of spiral waves to breakups is sensitive to perturbations even at one single pixel of the initial conditions. The middle image in row (b) in Fig. 2.15 shows the pattern that evolved from the initial values identical to the ones used in Fig. 1.10 except for one pixel at the center of the image – its value was perturbed from 1 to 0.99. Remarkably, the complexity of the difference image is comparable to the one in the previous computational experiment (Fig. 2.15 row (a)).

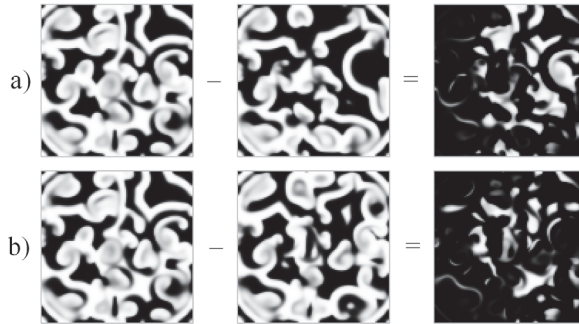


Fig. 2.15. The formation of patterns is sensitive to a perturbation of even one pixel in the initial conditions. Part (a) shows the pattern which forms from the initial u -field when the whole right part of the u -field is perturbed from 1 to 0.99. Part (b) shows the pattern which forms when a single pixel of the u -field is inverted. Remarkably, the complexity of the resulting difference images is not significantly different.

A simple perturbation of the initial conditions would not be applicable for the construction of the digital image communication scheme based on the breakup of spiral waves – a slight perturbation of a single pixel results in the alternation of the complete pattern. That can be explained by a long time required for the evolution of the pattern and the unpredictable avalanche-type formation of the breakups. However, shorter time intervals cannot be used either – the pattern is simply undeveloped then (Fig. 1.10). Another type of algorithm should be designed in order to replicate the communication scheme presented in (Saunoriene *et al.*, 2011; Ishimura *et al.*, 2014; Ziaukas *et al.*, 2014; Subsections 2.1 and 2.2).

2.3.2. The Experimental Scheme

The straightforward approach of the presented hiding scheme could be created of multiple patterns (as presented in Fig. 1.9) concatenated into one. By using this approach, the hiding of a more complex secret image could be accomplished easily with one spiral representing one bit of information. Obviously, the information capacity is very low, and the resulting pattern should be large enough to hide valuable visual information.

In the subsequent examples, the same initial conditions as described in Subsection 1.2.4 will be used. Multiple experiments showed that the initial configuration of u and v -field presented in (Barkley, 2008) is the best option.

Neither the angle nor the color intensity or random initial conditions as used in the models described earlier results in a spiral wave with breakups. One of the reasons is the way how the formation of a single spiral wave starts. The single spiral wave always initiates between the intersection of u and v -field ‘edges’; what regards the overlapping order of the fields, the spiral starts spinning clockwise or counter-clockwise (Fig. 2.16). Other parts of the initial conditions as well as random noise applied on the initial fields are unable to induce any significant formation. The experiment demonstrated in Fig. 2.16 uncovers the capacity properties of the possible concatenated pattern, and consequently one intersection of two u and v -fields stripes results in 4 autonomous spirals.

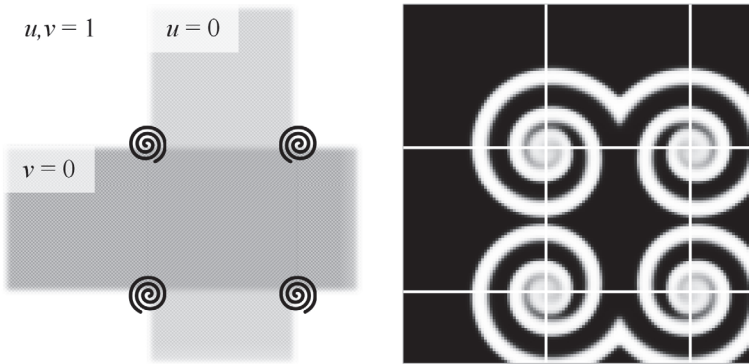


Fig. 2.16. Four intersection points of u and v -field borders result in autonomous spiral waves: spinning clockwise or counter-clockwise.

This idea can be extended with multiple stripes used as the initial conditions to generate larger patterns as shown in Fig. 2.17 (a, row 1). However, each field intersection is identical, and, as expected, such initial conditions result in a regular pattern (Fig. 2.17 (c, row 1)), which is not feasible considering information hiding applications. If any alternation in the initial conditions is introduced, the whole pattern becomes compromised as shown in Fig. 2.15. This drawback could be eliminated by adding uniform random noise all over the u -field as shown in Fig. 2.17 (a, row 2).

The resulting pattern seen in Fig. 2.17 ((c), row 2) is more convenient for information hiding than Fig. 2.17 ((c), row 1) because the whole area is chaotic, and small changes are invisible to a naked eye. As only small perturbation is required to change the whole evolution of the single spiral wave (Fig. 2.15), this pattern could be used to create the information hiding scheme in the same manner as previously presented models without diminishing the security.

The results of this hiding scheme are presented in Fig. 2.18. Different pattern formation periods are presented: at $T = 35$, the spirals only start to break, and each bit of information is clearly distinguished; at $T = 50$, patterns already start interacting but some mirroring is still visible; and, only at $T = 70$, the pattern becomes a continuous one. In all the three demonstrations, the secret information is visible in the difference images (part (c)) and could be exposed (part (d)) by using some enhancement method.

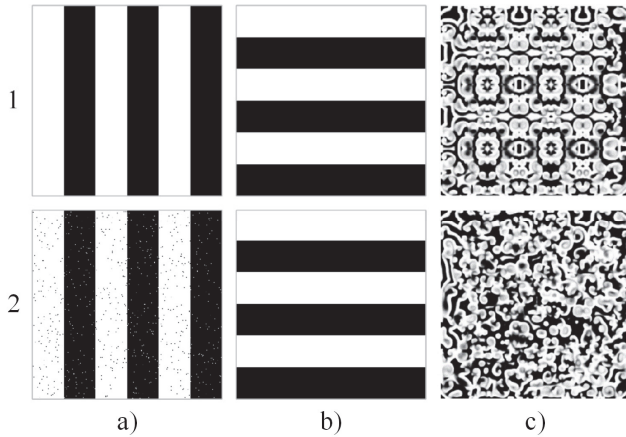


Fig. 2.17. Initial conditions (u -field (a) and v -field (b)) and the corresponding patterns (c). The full pattern consists of 3×3 concatenated patterns of size $L = 100$. Without noise (row 1), with uniform random noise covering 1% of the u -field (row 2).

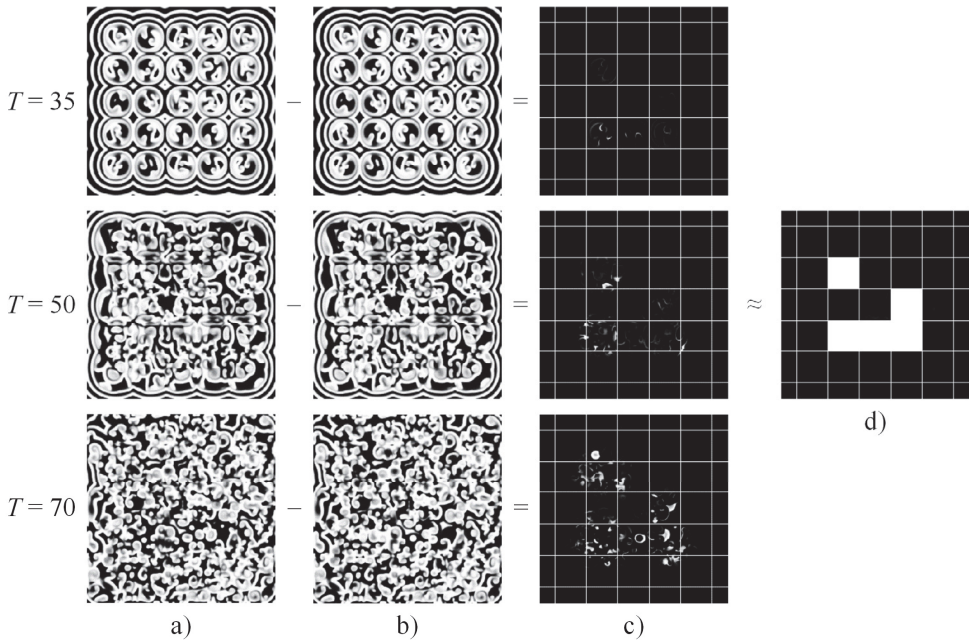


Fig. 2.18. A comparison of difference images (c) between two patterns (a) and (b) evolved from different initial conditions. Each row represents different evolution time while hiding the same secret (d). The grid in part c bounds the theoretical area of a single spiral wave.

However, this simple approach compared with the previously mentioned methods does not give any advantage regarding the steganographic security, speed or visual information quality. Despite the interesting features of spiral wave formation, a new idea of employing spiral waves is required.

2.3.3. The Proposed Scheme

As mentioned previously, a perturbation of the initial conditions cannot be employed for hiding a secret image in the self-organizing pattern produced by the breakup of spiral waves. And, while the evolution of the first pattern from the random initial conditions is not altered, the evolution of the second pattern should be perturbed in a different way compared to (Saunoriene *et al.*, 2011; Ishimura *et al.*, 2014; Ziaukas *et al.*, 2014; Subsections 2.1 and 2.2). A possible solution is to perturb the second pattern not at the beginning of its evolution but rather at some moment before the evolution of both patterns is terminated.

2.3.3.1. Delayed Perturbation at a Discrete Point

Let us repeat the computation experiment presented in Fig. 2.15 – except that the perturbation into the second pattern is introduced at time moment $T = 57.5$, and the evolution of both patterns is terminated at $T = 60$ (the initial conditions are the same as earlier; $L = 50$; $\varepsilon = 0.1$; $a = 0.7$; $b = 0.06$; $g = u^3 - v$; $dt = 0.05$). We do perturb one pixel at the center of the second pattern by adding 5% to its value at $T = 57.5$ (Fig. 2.19). The unperturbed pattern at $T = 57.5$ is shown in Fig. 2.19 (a); the perturbed image is presented in Fig. 2.19 (b) (the perturbation is so small that it is invisible to a naked eye). The perturbation point is clearly visible in the difference image at $T = 57.5$ in Fig. 2.19 (c) – the grayscale range is automatically adjusted to the max-min levels in the image.

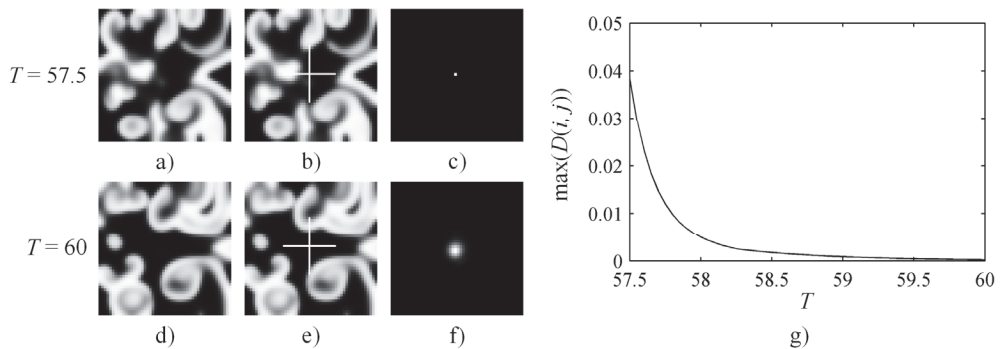


Fig. 2.19. Perturbation is introduced at time $T = 57.5$ by adding +5% to the u -field at the center point of the image. Part a) shows the unperturbed pattern at $T = 57.5$; b) demonstrates the perturbed pattern at $T = 57.5$ (the white cross denotes the perturbed pixel); c) visualizes the difference image between the perturbed and the unperturbed patterns at $T = 57.5$. The unperturbed view, the perturbed pattern, and the difference image at $T = 60$ are shown in parts d), e) and f). The decay of the maximum value of the u -field in the difference image over time is illustrated in part g).

The maximum value of the u -field in the difference image in Fig. 2.19 (c) is 0.0372 and is illustrated in Fig. 2.19 (g) at $T = 57.5$. Fig. 2.19 (d) shows the unperturbed pattern; Fig. 2.19 (e) demonstrates the perturbed pattern at $T = 60$. The initial perturbation at one pixel (Fig. 2.19 (c)) diffuses as the patterns continue to evolve (Fig. 2.19 (f)). However, the maximum value of the u -field in the difference image quickly decreases as the time goes on (Fig. 2.19 (g)). The only reason why the

diffused region is well visible in Fig. 2.19 (f) is due to the automatic adjustment to the max-min levels (it is the same procedure as used in Fig. 2.19 (c)).

However, it appears that the decay of the contrast of the perturbed pixel is not always monotonic, and it depends on the location of the pixel in respect to the breaking waves (Fig. 2.20). Two pixels are perturbed at $T = 57.5$ (Fig. 2.20 (b)). However, the evolution of the perturbations in the difference image is completely different (Fig. 2.20 (g)). This effect can be explained by the interaction between the perturbation and the propagating front of the breaking spiral wave. The top left point remains in the calm zone during the whole time interval of evolution $57.5 \leq T \leq 60$ (Fig. 2.20 (b and e)). On the contrary, the bottom right point is located in the region of the formation of the breakup wave. It appears that the interaction of the perturbation with the propagating wave front causes a temporary amplification of the perturbation effect and a complex pattern formation in the difference image around the perturbation point (Fig. 2.20 (f)). Moreover, the effects caused by the perturbation at the top left point are completely overwhelmed by the effects caused by the perturbation at the bottom right point (Fig. 2.20 (f)). Therefore, the evolution of the pattern in the difference image is sensitive to the geometrical location of the perturbation point in respect to the evolving front of the propagating breakup wave. It is clear that a strategy based on straightforward perturbations of the evolving pattern at a preselected set of points would not be applicable for hiding a secret in the difference image.

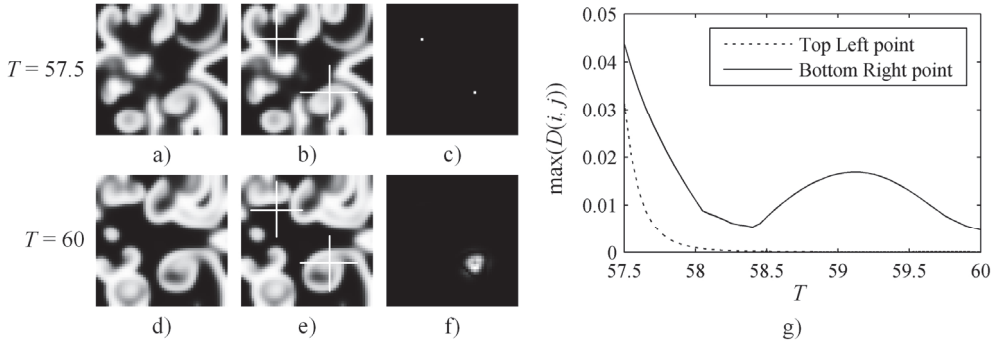


Fig. 2.20. The perturbation at the top left point is introduced in the area where no new breakup waves occur during the rest of the simulation; thus the maximum intensity of the spot in the difference image decreases monotonically. However, the bottom right perturbation point is located in the area where multiple breakup waves pass until the simulation is terminated. That results in the fluctuation of intensity of the spot in the difference image.

2.3.3.2. The Equalization of Maximum Intensities in the Difference Image

A possible solution to the problem associated to different decay rates of the perturbation intensities at different locations of the evolving pattern could be based on the variation of time moments of perturbations at different points. Such equalization of maximum intensities at the difference image in Fig. 2.20 (f) is illustrated in Fig. 2.21. We repeat the computational experiment but only the bottom right point is perturbed at $T = 58$ (the difference image is shown in Fig. 2.21 (a)).

The intensity of the perturbation at the bottom right point starts to decay – and we perturb the top left point at $T = 59.55$ (Fig. 2.21 (b)). The perturbation at the bottom right point starts interacting with the propagating front of the breakup wave – and the intensity of the difference image around this point starts increasing; the maximum intensities of perturbations around two points in the difference image become equal at $T = 60$ (Fig. 2.21 (c)).

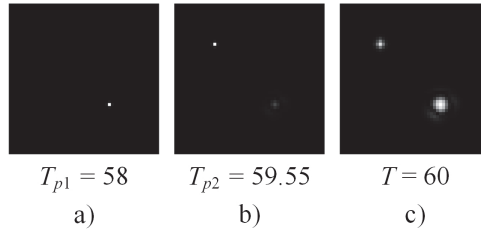


Fig. 2.21. The equalization of the maximum intensities of perturbations in the difference image. The perturbation at the bottom right point (p_1) is performed at $T = 58$ (a); the perturbation at the top left point (p_2) is performed at $T = 59.55$ (part b). The perturbations evolve differently due to different interaction with the propagating front of the breakup waves (c).

It is clear that the selection of proper time moments of the perturbation is a difficult problem – everything depends on the location of the perturbation points and on the particular dynamical distribution of the evolving pattern of breakup waves. The complexity of the problem is illustrated in Fig. 2.22. All the parameters of the system (including the geometrical locations of the two perturbation points) are kept the same. The only varying parameter is the time moment of the perturbation at the top left point (denoted as T_{p2} in Fig. 2.22). Point (p_1) is perturbed at $T = 58$ (Fig. 2.22 (a)). Then, five independent computational experiments are executed by perturbing the pattern at point (p_2) at $T = 58.5$ (Fig. 2.22 (b)); $T = 59$ (Fig. 2.22 (c)); $T = 59.25$ (Fig. 2.22 (d)); $T = 59.5$ (Fig. 2.22 (e)) and $T = 59.75$ (Fig. 2.22 (f)). Figures at the top row show the difference image at the moment of perturbation; figures at the bottom row demonstrate the difference image at $T = 60$. As mentioned previously, the evolution of a perturbation depends on the interaction with the propagating front of the breakup wave. Anyway, it is possible to find such T_{p2} where the maximum front intensities of the evolved perturbations in the difference image at $T = 60$ are almost the same (cf. Fig. 2.22 (e)) – even though the ‘deformations’ around points p_1 and p_2 are different.

However, on the larger scale, where more pattern points are perturbed, the contrast equalization becomes a complex task, and sometimes it is not possible to achieve. The following experiment considers a pattern of the size of 100×100 pixels and 100 points perturbed at $T \in [68, 69.5]$ time interval. Two strategies are studied: where points are perturbed as early as possible (Fig. 2.23 (b)) and as late as possible (Fig. 2.23 (c)) with the intention to achieve the closest equivalent contrast of each point’s surrounding.

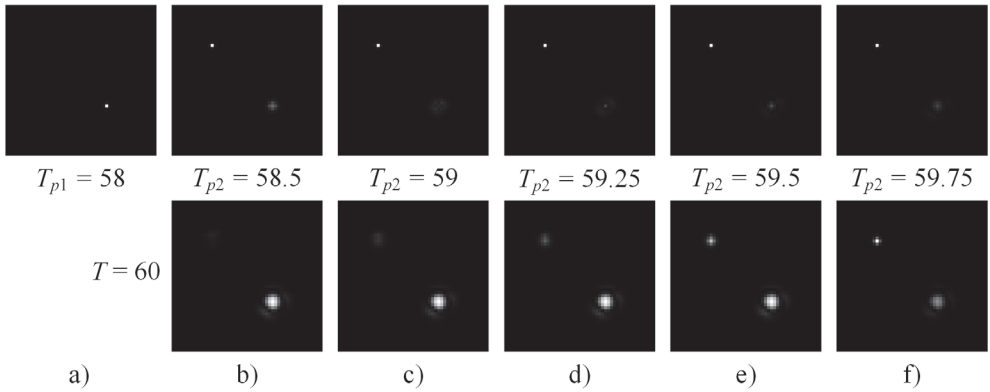


Fig. 2.22. A comparison of difference images when the bottom point (p_1) perturbation is fixed at time $T = 58$, and the top point (p_2) perturbation time varies. The corresponding difference image (at $T = 60$) is provided in the second row of images.

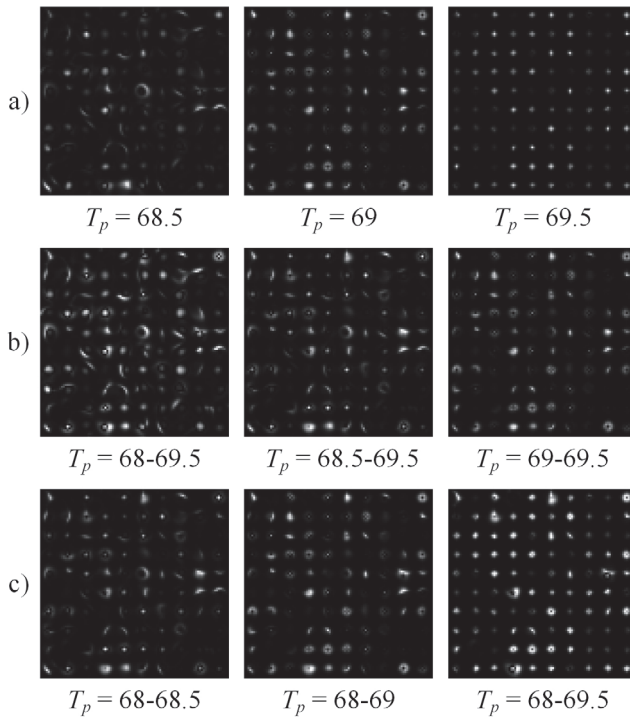


Fig. 2.23. Perturbation time selection of 100 points in a 100×100 pixel pattern.

a) All the points are perturbed at the same time T_p ; b) patterns are perturbed ‘as early as possible’ and c) ‘as late as possible’.

The difference images of the two patterns where all the selected points in the u -field are perturbed at the same time ($T = 68.5, 69, 69.5$) are shown in the top row of Fig. 2.23, i.e., Fig. 2.23 (a). The results of Fig. 2.23 represent previous remarks regarding the intensity and size where some points dominated over others, and earlier perturbation times resulted in bigger affected areas. Both strategies do have

their own advantages and disadvantages. The strategy ‘as early as possible’ (Fig. 2.23 (b)) uncovers more perturbed points if a longer window for perturbation is given, but, on the other hand, points also spread wider. The strategy ‘as late as possible’ (Fig. 2.23 (c)) works the opposite way, and it provides better results if the time window is shorter. In both cases, there are about 5% of points that disappear because of the same effect described in Subsection 2.3.3.1, thus a better point selection method should be considered.

2.3.3.3. The Equalization of both Intensities and Shapes

Such manipulation with time moments of the perturbation at different points of the evolving pattern can yield the same maximum intensity at all (or at least the majority of) points in the difference image. However, the size of the deformations around the perturbed points (in the difference image) is clearly different (Fig. 2.21 (c)). It would be almost impossible to use such a perturbation strategy for a meaningful hiding of the secret image. A new perturbation strategy should be used in order to overcome this limitation.

We continue the same computational experiment as described in Fig. 2.21 – however, we change the perturbation around point p_2 . Instead of perturbing the evolving pattern at a single pixel, we perturb 6 adjacent pixels around p_2 (Fig. 2.24 (b)). We should note that the intensity of perturbations is kept the same at all 6 pixels; the specific geometrical location of the perturbed pixels is adjusted experimentally in order to produce such a difference image that both intensities and geometric shapes of the deformations are almost identical in the difference image (Fig. 2.24 (c)).

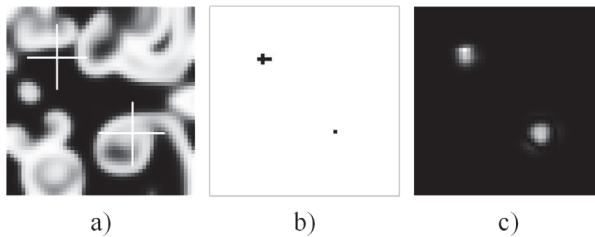


Fig. 2.24. The adaptive perturbation strategy helps to equalize both the intensities and shapes of spots in the difference image. The location of the perturbation points is the same as in Fig. 2.20. The perturbation at the bottom right point (p_1) and the top left point (p_2) is performed at $T = 58.7$. Six pixels around point p_2 are perturbed; the intensity of the perturbation at all the pixels is the same as before.

2.3.3.4. The Formation of Geometric Primitives in the Difference Image

The ability to control the shape and the intensity of the deformations in the difference image allows a possibility to construct different shapes and geometrical primitives. We continue the computational experiments with the same set of parameters – except that the dimensions of the area used for the pattern formation are now 500×500 pixels (Fig. 2.25). The intensity of perturbations is kept the same by adding +5% to the u -field – but instead of perturbing a single point we do perturb all the points on the circle (Fig. 2.25 (a)). The perturbation is performed at $T = 145$;

the system continues to evolve until $T = 150$. The final pattern produced after the perturbation is shown in Fig. 2.25 (b); the difference image is presented in Fig. 2.25(c).

It is natural to expect that the produced ring in the difference image is discontinuous – the formation of the difference image is sensitive to the geometrical locations of the propagating fronts of the breakup waves. One of the possibilities to make the geometric object more comprehensible in the difference image is to increase the area of perturbation (Fig. 2.25 (d)). However, even though the discontinuities become less prominent, the differences between the highest and the lowest intensities in the difference image are still large (Fig. 2.25 (d)).

2.3.3.5. Adaptive Perturbation Strategy

A strategy for the equalization of intensities and shapes is also required for geometric primitives in the difference image. A possible adaptive solution to the problem is schematically illustrated in Fig. 2.25. Let us assume that the perturbation (Fig. 2.25 (a)) results in the difference image as shown in Fig. 2.25 (b). The discontinuities in the difference image can be detected by using manual, semi-automatic or even completely automatic means. Then, the perturbation must be adaptively tuned in order to eliminate the discontinuities (Fig. 2.25 (c)). In general, the variation of the perturbation is sensitive to almost all the parameters of the system – including the moment of the perturbation and the final time moment when the evolution of patterns is terminated. In our computational setup, it is enough to enlarge the width of the perturbation line from a one-pixel line to a 5-pixel line (Fig. 2.25 (c)). That is sufficient to ensure that the discontinuities in the difference image disappear (Fig. 2.25 (d)).

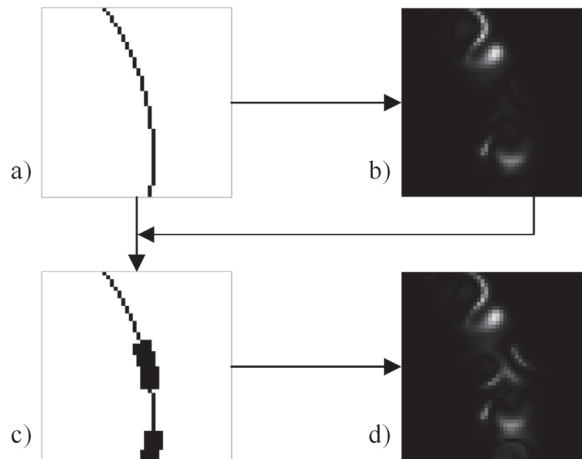


Fig. 2.25. An illustration of the iterative process of the formation of the perturbation. A thin line type perturbation (part (a)) yields the difference image with an undeveloped inner part (part (b)). The perturbation is strengthened in those parts where the difference image is not clear enough (part (c)), and the computational experiment is repeated again till the difference image is clear enough (part (d)).

The same adaptive strategy is now applied to the computational experiment

presented in Fig. 2.26. The discontinuities and zones of lower intensity are detected in Fig. 2.26 (c); the perturbation is adaptively corrected (Fig. 2.26 (d)). The resulting difference image now clearly represents a regular geometric shape (Fig. 2.26 (f)). The resulting image Fig. 2.26 (c and f) can be further enhanced by applying the image enhancement technique as described in Section 1.3.3. In the current implementation, the discontinuities are detected by human inspection, but special algorithms could be employed to automate the process.

We should note that the presented adaptive strategy of the perturbation does not exploit the variation of time delays used to perform the perturbation at different locations of the digital image. The application of such features could enhance the difference image even more – but we limit the functionality of the proposed communication algorithm by excluding these time-related aspects.

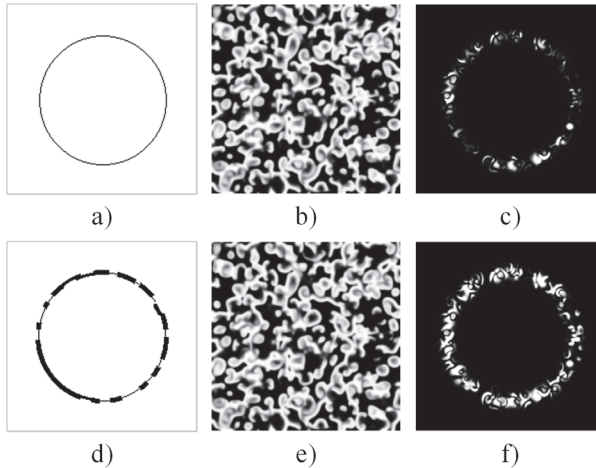


Fig. 2.26. The adaptive perturbation strategy for the formation of a ring in the difference image. A thin circle-type perturbation (part (a)) is applied to the pattern at $T = 145$. The resulting pattern at $T = 150$ is shown in part (b); the difference image (at $T = 150$) is demonstrated in part (c). The adaptive perturbation strategy is used to modify the perturbation (part (d)). The resulting pattern (at $T = 150$) is shown in part (e); the difference image is presented in part (f).

The set of the system parameters is as follows: $\varepsilon = 0.1$; $a = 0.7$; $b = 0.06$.

2.3.4. The Communication Algorithm

The proposed communication algorithm based on the breakup of spiral waves is illustrated by the following diagram (Fig. 2.27). Let us consider two communication parties – the Sender and the Receiver. The Sender transmits a secret digital image to the Receiver. The action steps to be taken by the Sender are bordered by a thick dashed line; the steps to be taken by the Receiver are enclosed into a gray-shaded area (Fig. 2.27).

2.3.4.1. Encoding of the Secret Image

Initially (at $T = 0$), the Sender selects the initial conditions of the u -field and the v -field (the initial parameters of reaction-diffusion equations (8)) as shown in

Fig. 2.27. We should note that generation of random initial conditions is not required for this communication scheme – which is a serious advantage compared to other communication algorithms based on the self-organizing patterns.

Then, the Sender stops the evolution of the spiral waves at $T = 145$ and perturbs it at the points corresponding to the secret image (by adding 5% to the appropriate pixels of the u -field). The Sender continues to evolve the perturbed pattern until $T = 150$ (100 time forward steps from the moment of perturbation). At the same time, the Sender evolves the pattern from the initial conditions without any perturbations until reaching the final time moment $T = 150$. That allows the Sender to check what the difference image between the perturbed and unperturbed patterns looks like (Fig. 2.27).

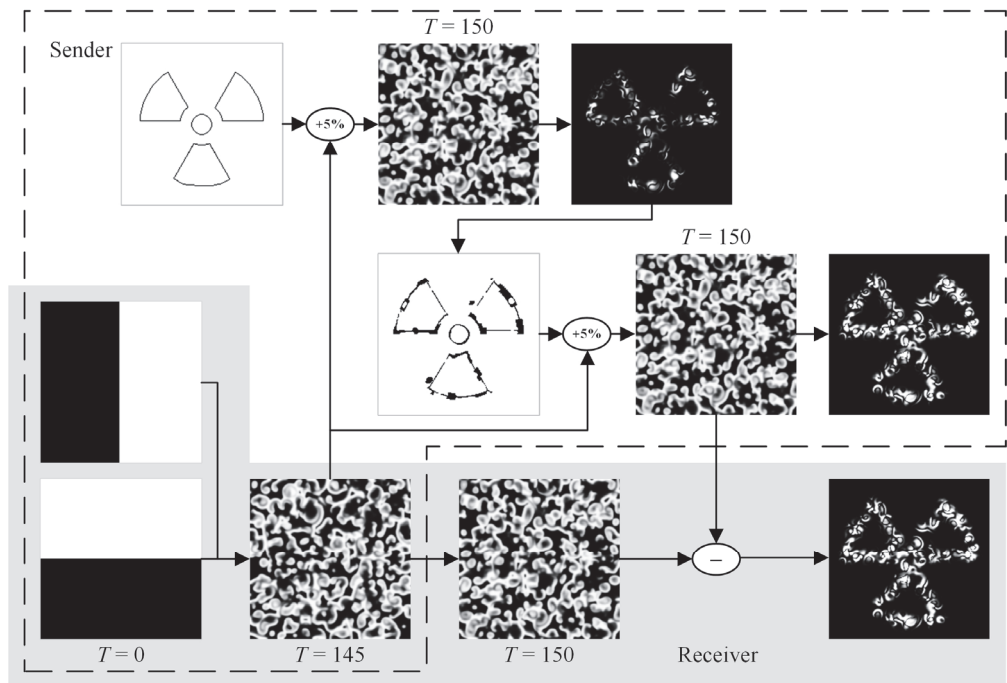


Fig. 2.27. The schematic diagram of the digital image communication scheme based on the breakup of spiral waves.

Now, the Sender uses the adaptive perturbation strategy and repeats the computational simulation of the perturbed and unperturbed patterns. The proper adjustment of the perturbation points ensures that the difference image is sufficiently clear and representative (Fig. 2.27). Then, the Sender transmits the perturbed pattern to the Receiver. We should note that the perturbation is performed at $T = 145$ and the transmitted pattern is fixed at $T = 150$. Moreover, 100 forward time steps do completely hide the perturbation in the pattern of spiral waves. No algorithms (statistical or deterministic) could detect any perturbation in this pattern. Also (even in the cases when all the system parameters are known to the eavesdropper), the time backward evolution of the model is still impossible due to the nonlinearity of the governing evolutionary equations. The secret digital information is securely

embedded into the pattern of spiral waves.

2.3.4.2. Decoding the Secret Image

The decoding process is straightforward. The Receiver uses the identical initial conditions and evolves the pattern until $T = 150$. Then, s/he simply computes the difference image between the evolved and the received patterns, and the resulting image reveals the secret (Fig. 2.27).

2.3.4.3. Sensitivity of the Communication Scheme to the Perturbation of Parameters

The presented decoding process does function only when all the system parameters are preset and available both to the Sender and the Receiver. Slight changes of these parameters (when the Sender and the Receiver use different parameters) may compromise the communication scheme.

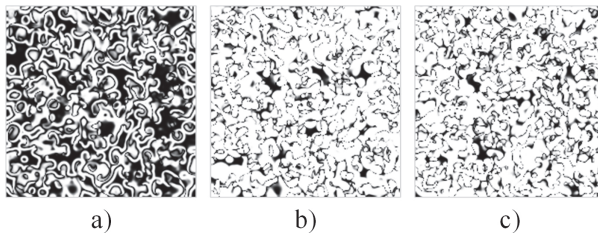


Fig. 2.28. Slight perturbations of the system parameters compromise the communication system. The set of parameters used by the Sender is: $T = 150$; $\varepsilon = 0.1$; $a = 0.7$; $b = 0.06$. A slight perturbation of any of these parameters by the Receiver results in an uninterpretable difference image (a separate perturbation of a single parameter is used in every part, respectively): a) $T = 149.95$; b) $a = 0.69$; c) $b = 0.061$.

The sensitivity of the communication scheme to the initial parameters is presented in Fig. 2.28; all the illustrations represent difference images only. Initially, we perturb the pattern evolution time by a single integration step. The Sender creates the pattern by using the previously set parameters ($T = 150$; $\varepsilon = 0.1$; $a = 0.7$; $b = 0.06$). However, the Receiver stops the evolution of this pattern evolution at $T = 149.95$ instead of $T = 150$. Spiral waves evolve in every iteration – thus the Sender’s and the Receiver’s patterns are different enough to become useless (Fig. 2.28 (a)).

The next computational experiment simulates the changes of parameters a and b . The Receiver mistreats parameter a by using $a = 0.69$ instead of $a = 0.7$. The change is crucial enough to make the difference image (Fig. 2.28 (b)) uninterpretable. Analogously, parameter $b = 0.061$ is used instead of $b = 0.06$. The resulting difference (Fig. 2.28 (c)) is meaningless.

2.4. Concluding Remarks

Self-organizing patterns can be used to conceal secret images; reaction-diffusion models and evolutionary spatial games which had been successfully exploited for these purposes previously. However, reaction-diffusion models do require long transients; evolutionary spatial games are not sensitive to

changes in the strategy of a single individual pixel in the initial state of the system.

It appears that competitively and non-diffusively coupled nonlinear maps help to overcome the drawbacks of the above mentioned communication schemes. The secret image can be embedded into the spatially homogenous initial state in a form of a dot-skeleton representation – and far below the noise level of the initial random image. The parameters of the array of competitively coupled maps can be used as private and public keys thus enabling an efficient and secure communication system based on self-organizing patterns.

It appears that the complex rules of self-organization and wave propagation in anisotropic atrial fibrillation media help to overcome such drawbacks of digital image communication schemes as long transients, relatively large primitives, or the relative simplicity of the cover pattern. The secret image can be embedded into the spatially homogeneous dichotomous initial state by inverting the dot-skeleton representation of the secret and thus enabling an efficient and secure communication scheme based on SOP.

The proposed digital image communication scheme based on breaking spiral waves does not use random initial conditions for the pattern formation – nor does it use any perturbations of the initial conditions in order to conceal and transmit the secret digital image. Such a computational setup does have a number of serious advantages if compared to all alternative communication systems based on self-organizing patterns which had been introduced so far. The sender and the receiver of the image do not need to worry about keeping any keys (private or public) which would determine the generation of the initial random conditions. Moreover, the communication algorithm does not use any perturbations of the initial conditions (any dot-skeleton representations or inversions of the dichotomous pixels). Such an approach could be considered as a serious step forward in respect of the security of the communication algorithm.

The evolving pattern is perturbed – just not at the beginning but rather in the middle of the pattern formation process. It appears that this perturbation is sensitive to the geometrical locations of the travelling fronts of the breakup waves. Therefore, a special adaptive perturbation technique is required for the proper embedding of the secret image into the evolving pattern. However, this adaptive perturbation procedure does not impact the decoding of the secret image. The decoding process remains simple and straightforward – the receiver of the secret image needs just to reproduce the unperturbed pattern of breakup waves.

So far, the adaptiveness of the perturbation has been employed only in the sense of the area of the perturbation in the zones where the difference image appears not to be clear enough. However, the perturbation could be adapted not only in space but also in time (as demonstrated in Fig. 2.24). The development of a fully automatic adaptive perturbation technique in space and in time remains a definite objective for the future research.

The SOP communication scheme can be used without LSB steganography. However, a transmitted SOP image may draw attention from eavesdroppers. LSB steganography could eliminate this threat. However, LSB steganography alone is prone to steganalysis algorithms. The SOP communication scheme ensures the

security of the secret image even if LSB steganography had been compromised. Thus the synergy of the SOP communication scheme and LSB steganography offers the added security to the transmitted image.

It is worth noting that the information hidden by using the LSB algorithm only could be easily detected with standard steganography detection tools, and secret information could be revealed by using statistical methods. Meanwhile, SOP creates an additional layer of security guaranteeing that even if the existence of secret information is detected, the information still remains secure.

The three schemes outlined above provide specific advantages over each other. However, they should not be directly compared because of the differences in the models, the required initial conditions, the information embedding peculiarities and the decoding quality. The preference towards any of the schemes depends on the Sender's/Receiver's needs and are presented as almost equal alternatives.

3. DYNAMIC VISUAL CRYPTOGRAPHY SCHEME BASED ON FINITE ELEMENT GRIDS⁹

Digital image communication schemes presented in Section 2 were based on the evaluation of SOP and on the decoding process requiring a comparative pattern to find the difference in order to uncover the secret. For example, the Sender produces one pattern, the Receiver generates the second one, and the secret information is only revealed when the difference between two patterns is calculated. The situation is similar to a classical VC introduced by Naor and Shamir (Naor *et al.*, 1994) where one image is divided into 2 shares, and the secret is unveiled by overlaying the shares. Although in SOP each share is produced separately (which increases the security of the scheme), but the communication scheme still requires 2 shares for the decryption of the secret. This restriction can be eliminated by DVC where is no need for 2 shares to reconstruct the secret. The DVC communication scheme (similarly to SOP) employs a physical process to form the patterns, but the process used is different, and in the DVC case, the physical deformations are required for the time-averaged moiré fringes to form. Thus, in this Section, the information hiding scheme is expanded to employ only one share by applying the concepts of DVC.

The idea of information hiding in deformable moiré gratings is not new (Palivonaitė *et al.*, 2014). The secret image is leaked from the cover image when it is deformed and averaged in time along the longitudinal coordinate of the stochastic moiré grating. Different image hiding schemes have also been studied (Subsection 1.1.2), however, deformable moiré gratings in physical processes have not been studied yet. The main objective of this Section is to hide the secret information in a stochastic deformable moiré grating in such a way that only one share is required for the communication and that the physical process describing the oscillations of the system could be used as a decoding key. Such image hiding schemes would open up new possibilities for the optical control of MOEMS (micro-opto-electro-mechanical systems) where a stochastic cover moiré image could be formed on the surface of the cantilever or the diaphragm. The secret image would be leaked when the micro-structure would oscillate at a predetermined law of motion. This property can be exploited for mechanical vibration testing, parameter monitoring and visual monitoring of micro-components and MEMS devices.

An image hiding scheme based on time-averaged moiré fringes on finite

⁹ Some passages have been quoted verbatim from the following sources:

Image Hiding in Time-Averaged Moiré Gratings on Finite Element Grids.
Vaidelys M., Ragulskienė J., Aleksienė S., Ragulskis M.
Copyright © 2015 Elsevier Inc.

Dynamic Visual Cryptography Scheme on the Surface of a Vibrating Structure.
Vaidelys M., Aleksienė S., Ragulskienė J.
Copyright © 2015 JVE International Ltd.

element grids is proposed in this Section. The visual communication scheme is based on the formation of time-averaged moiré fringes in the digital dichotomous cover image when it is deformed according to a predefined Eigen-shape. The proposed scheme is practical because the decryption of the secret can be performed by the human visual system only. This section is organized as follows: a cryptography scheme based on harmonic oscillations of the deformable harmonic moiré grating is presented in Section 3.1 (Vaidelys *et al.*, 2015b), a scheme based on time-averaged fringes generated by the Ronchi-type geometric moiré grating is presented in Section 3.2 (Vaidelys *et al.*, 2015a), and conclusions are outlined in Section 3.3.

3.1. Image Hiding in Time-Averaged Moiré Gratings on Finite Element Grids¹⁰

The image hiding technique based on harmonic oscillations of the deformable moiré grating according to a pre-selected Eigen-shape of an elastic structure is presented in this Section. The initial phase scrambling and phase normalization algorithms are used to encode the secret in the cover image. The theoretical relationships between the amplitude of the Eigen-shape, the order of the time-averaged moiré fringe and the pitch of the deformable one-dimensional moiré grating are derived. Computational experiments are used to illustrate the efficiency and applicability of this image hiding scheme in practical applications (Vaidelys *et al.*, 2015b).

3.1.1. Preliminaries

Let us consider a one-dimensional harmonic moiré grating (Kobayashi, 1993):

$$F(x) = \frac{1}{2} + \frac{1}{2} \cos\left(\frac{2\pi}{\lambda} x\right), \quad (34)$$

where x is the longitudinal coordinate; λ is the pitch of the grating; the numerical value 0 corresponds to the black color, 1 represents the white color, and all the intermediate values correspond to the appropriate grayscale level. Let the moiré grating be formed on the surface of a one-dimensional deformable body. Let the deformation from the state of equilibrium at point x at time moment t be equal to $u(x, t)$. Then, the deformed moiré grating can be expressed in the explicit form:

$$F(x, t) = \frac{1}{2} + \frac{1}{2} \cos\left(\frac{2\pi}{\lambda} \mu(x, t)\right) \quad (35)$$

if only independent variable x can be explicitly expressed from the relationship:

$$x + u(x, t) = z \quad (36)$$

¹⁰ The results presented in this section have been published as:

Image Hiding in Time-Averaged Moiré Gratings on Finite Element Grids.
Vaidelys M., Ragulskienė J., Aleksienė S., Ragulskis M.
Copyright © 2015 Elsevier Inc.

and converted into the form:

$$x = \mu(z, t). \quad (37)$$

Let us assume that function $u(x, t)$ does describe harmonic oscillation around the state of equilibrium (Ragulskis *et al.*, 2009a):

$$u(x, t) = a(x)\sin(\omega t + \varphi), \quad (38)$$

where $a(x)$ is the Eigenshape of in-plane oscillations; ω and φ are the circular frequency and the phase of harmonic oscillations.

Let us linearize the function $a(x)$ around point x_0 :

$$a(x) = a_0 + \dot{a}_0(x - x_0) + O(x - x_0)^2, \quad (39)$$

where $a_0 = a(x_0)$; $\dot{a}_0 = \left. \frac{da(x)}{dx} \right|_{x=x_0}$. Without losing the generality we assume that $\omega = 1$ and $\varphi = 0$. Then, Eq. (37) yields:

$$x \approx \frac{z - (a_0 - \dot{a}_0 x_0) \sin t}{1 + \dot{a}_0 \sin t}. \quad (40)$$

Thus the grayscale level of the deformed moiré grating at coordinate x at time moment t reads:

$$F(x, t) = \frac{1}{2} + \frac{1}{2} \cos\left(\frac{2\pi}{\lambda} \cdot \frac{x - (a_0 - \dot{a}_0 x_0) \sin t}{1 + \dot{a}_0 \sin t}\right). \quad (41)$$

3.1.1.1. Non-Deformable Moiré Grating

Different cases of $a(x)$ are examined in this and in the following sections. Firstly, let us assume that $a(x) = A$ (A is a constant). In other words, the deflection:

$$u(x, t) = A \sin(\omega t + \varphi) \quad (42)$$

describes the oscillation of a non-deformable body around the state of equilibrium (Ragulskis *et al.*, 2009a). Then the instantaneous grayscale level of the moiré grating reads:

$$F(x, t) = \frac{1}{2} + \frac{1}{2} \cos\left(\frac{2\pi}{\lambda} \cdot (x - A \sin(\omega t + \varphi))\right). \quad (43)$$

Now, let us assume that time-averaging techniques are used to register the time-averaged image of the oscillating moiré grating (Ragulskis *et al.*, 2009a):

$$\bar{F}(x) = \lim_{T \rightarrow \infty} \frac{1}{T} \int_0^T F(x, t) dt = \frac{1}{2} + \frac{1}{2} \cos\left(\frac{2\pi}{\lambda} x\right) J_0\left(\frac{2\pi}{\lambda} A\right), \quad (44)$$

where J_0 is the zero order Bessel function of the first kind. We should note that the distribution of the grayscale level in the time-averaged image does not depend on the frequency or on the phase of harmonic oscillations.

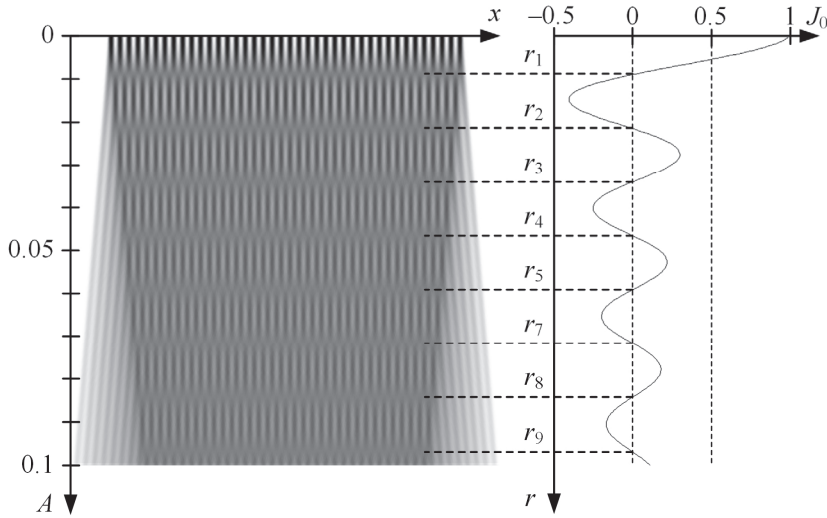


Fig. 3.1. Harmonic oscillation of the inelastic one-dimensional moiré grating ($\lambda = 0.025$) produces time-averaged fringes. A time-averaged image is shown on the left; the graph of J_0 is represented at the right part of the figure.

Time-averaged moiré fringes form when $J_0\left(\frac{2\pi}{\lambda}A\right) = 0$. This happens at amplitudes $\frac{2\pi}{\lambda}A_k = r_k$, where r_k are roots of J_0 ; $k = 1, 2, \dots$. The formation of time-averaged fringes is illustrated in Fig. 3.1. The x -axis in Fig. 3.1 stands for longitudinal coordinate x ; the y -axis denotes amplitude A . A sharp high-contrast harmonic moiré grating is visible at $A = 0$; gray time-averaged fringes are clearly visible at the amplitudes corresponding to roots r_k (Fig. 3.1). One-dimensional moiré grating is formed only in a finite interval in Fig. 3.1 – blurred zones around the ends of that interval do occupy a region proportional to the amplitude of harmonic oscillations.

3.1.1.2. Deformable Moiré Grating; Linear Deformation Field

Let us assume that $a(x) = Ax$. The deflection from the state of equilibrium is now proportional to coordinate x . In other words, a harmonic moiré grating can be formed on the surface of a one-dimensional body in the state of equilibrium – but the moiré grating will be deformed when the body performs oscillations in time. That is the principal difference from non-deformable moiré gratings (described in Subsection 3.1.1.1) where each point of the non-deformable one-dimensional body oscillates around the state of equilibrium at the same amplitude, and the moiré grating is not deformed.

Linearization around x_0 yields: $a(x) = Ax_0 + A(x - x_0)$; $a_0 = Ax_0$; $\dot{a}_0 = A$. Thus, Eq. (41) reads as:

$$\begin{aligned}
F(x, t) &= \frac{1}{2} + \frac{1}{2} \cos\left(\frac{2\pi}{\lambda} \frac{x}{1 + A \sin t}\right) \\
&= \frac{1}{2} + \frac{1}{2} \cos\left(\frac{2\pi x}{\lambda} (1 - A \sin t + (A \sin t)^2 - (A \sin t)^3 + \dots)\right) \\
&= \frac{1}{2} + \frac{1}{2} \cos\left(\frac{2\pi x}{\lambda} (1 - A \sin t + O(A^2))\right) \\
&\approx \frac{1}{2} + \frac{1}{2} \cos\left(\frac{2\pi}{\lambda} x - \frac{2\pi}{\lambda} Ax \sin t\right).
\end{aligned} \tag{45}$$

We should note that $0 < A \ll 1$ (a singularity occurs at $A = 1$ in Eq. (45)). Finally, the time-averaged image reads (Palivonaitė *et al.*, 2014):

$$\begin{aligned}
\bar{F}(x) &= \lim_{T \rightarrow \infty} \frac{1}{T} \int_0^T F(x, t) dt = \frac{1}{2} + \frac{1}{2} \cos\left(\frac{2\pi}{\lambda} x\right) \lim_{T \rightarrow \infty} \frac{1}{T} \int_0^T \cos\left(\frac{2\pi}{\lambda} Ax \sin t\right) dt \\
&= \frac{1}{2} + \frac{1}{2} \cos\left(\frac{2\pi}{\lambda} x\right) \lim_{T \rightarrow \infty} \frac{1}{T} \int_0^T e^{i \frac{2\pi}{\lambda} Ax \sin t} dt \\
&= \frac{1}{2} + \frac{1}{2} \cos\left(\frac{2\pi}{\lambda} x\right) J_0\left(\frac{2\pi}{\lambda} Ax\right).
\end{aligned} \tag{46}$$

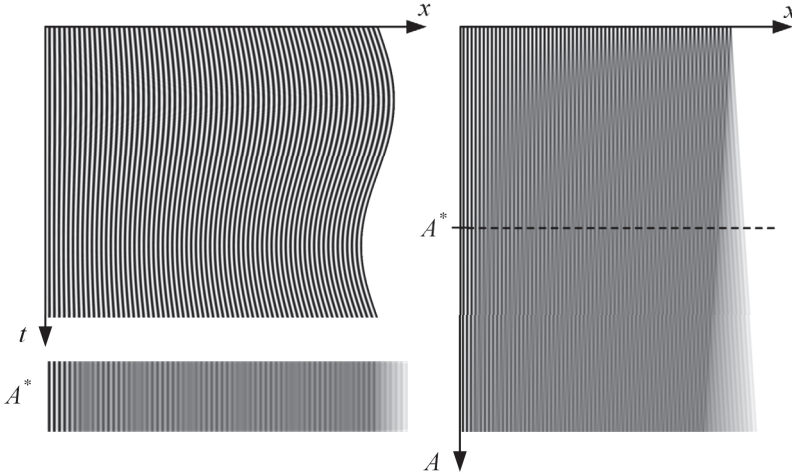


Fig. 3.2. Harmonic oscillation of the deformable one-dimensional moiré grating ($\lambda = 0.015$) produces time-averaged fringes. One period of harmonic oscillations with $A^* = 0.05$ is illustrated in the top left image; a one-dimensional time-averaged image at $A^* = 0.05$ is shown at the bottom on the left; the formation of time-averaged fringes at increasing amplitudes is illustrated on the right; $A = [0.001, 0.1]$.

Thus time-averaged moiré fringes form at $\frac{2\pi}{\lambda} Ax = r_k$; $k = 1, 2, \dots$ (Fig. 3.2). The oscillating moiré grating is shown in the left upper image. The left side of the one-dimensional moiré grating is motionlessly fixed; the right side of the deformed grating does oscillate at a preset amplitude $A^* = 0.05$, the pitch of the moiré grating at the state of equilibrium is $\lambda = 0.015$. The left bottom part of Fig. 3.2 represents the time-averaged image of the one-dimensional grating at $A^* = 0.05$;

time-averaged moiré fringes can be clearly seen in this image. The right part of Fig. 3.2 shows the time-averaged images of the one-dimensional moiré grating at increasing amplitudes A (the higher is the amplitude of harmonic oscillations, the larger number of moiré fringes is visible in the time-averaged image). The horizontal dashed line represents amplitude $A^* = 0.05$.

3.1.2. Deformable Moiré Grating; Nonlinear Deformation Field

The main objective of this Section is to develop an image hiding scheme based on deformable moiré gratings on finite element grids. In other words, deformation field $a(x)$ must be a nonlinear function. That requires the development of a complex inverse problem.

Let us construct this inverse problem for the general case described by Eq. (41). We may wonder what should be the distribution of the pitch of the one-dimensional moiré grating $\lambda(x)$ that the whole time-averaged image should be transformed into a time-averaged fringe regardless of the function $a(x)$. The argument of the cosine function in Eq. (41) can be arranged as follows:

$$\begin{aligned} \frac{x - (a_0 - \dot{a}_0 x_0) \sin t}{1 + \dot{a}_0 \sin t} &= (x - (a_0 - \dot{a}_0 x_0) \sin t) \cdot \frac{1}{1 + \dot{a}_0 \sin t} \\ &= (x - (a_0 - \dot{a}_0 x_0) \sin t) \left((1 - \dot{a}_0 \sin t) + O(\dot{a}_0^2) \right). \end{aligned} \quad (47)$$

Let us denote $\bar{a}(x) = a_0 + \dot{a}_0(x - x_0)$. Then, Eq. (41) reads:

$$\begin{aligned} F(x, t) &\approx \frac{1}{2} + \frac{1}{2} \cos \left(\frac{2\pi}{\lambda} \cdot (x - (a_0 - \dot{a}_0 x_0) \sin t - \dot{a}_0 x \sin t + (a_0 - \dot{a}_0 x_0) \dot{a}_0 \sin^2 t) \right) \\ &= \frac{1}{2} + \frac{1}{2} \cos \left(\frac{2\pi}{\lambda} \cdot (x + (a_0 - \dot{a}_0 x_0) \dot{a}_0 \sin^2 t - (a_0 + \dot{a}_0(x - x_0) \sin t)) \right) \\ &= \frac{1}{2} + \frac{1}{2} \cos \left(\frac{2\pi}{\lambda} (x + (a_0 - \dot{a}_0 x_0) \dot{a}_0 \sin^2 t) \right) \cos \left(\frac{2\pi}{\lambda} \bar{a}(x) \sin t \right) \\ &\quad + \frac{1}{2} \sin \left(\frac{2\pi}{\lambda} (x + (a_0 - \dot{a}_0 x_0) \dot{a}_0 \sin^2 t) \right) \sin \left(\frac{2\pi}{\lambda} \bar{a}(x) \sin t \right). \end{aligned} \quad (48)$$

We should note that $\lim_{T \rightarrow \infty} \frac{1}{T} \int_0^T \sin \left(\frac{2\pi}{\lambda} \bar{a}(x) \sin t \right) dt = 0$ due to the oddness of the sine function. Also, $\lim_{T \rightarrow \infty} \frac{1}{T} \int_0^T \sin^2 t dt = 0.5$. Then, the time-averaged image reads:

$$\begin{aligned} \bar{F}(x) &= \lim_{T \rightarrow \infty} \frac{1}{T} \int_0^T F(x, t) dt \\ &\approx \frac{1}{2} + \frac{1}{2} \cos \left(\frac{2\pi}{\lambda} \left(x + \frac{1}{2} (a_0 - \dot{a}_0 x_0) \dot{a}_0 \right) \right) \lim_{T \rightarrow \infty} \frac{1}{T} \int_0^T \cos \left(\frac{2\pi}{\lambda} \bar{a}(x) \sin t \right) dt \\ &= \frac{1}{2} + \frac{1}{2} \cos \left(\frac{2\pi}{\lambda} \left(x + \frac{1}{2} (a_0 - \dot{a}_0 x_0) \dot{a}_0 \right) \right) \lim_{T \rightarrow \infty} \frac{1}{T} \int_0^T e^{i \frac{2\pi}{\lambda} \bar{a}(x) \sin t} dt \\ &= \frac{1}{2} + \frac{1}{2} \cos \left(\frac{2\pi}{\lambda} \left(x + \frac{1}{2} (a_0 - \dot{a}_0 x_0) \dot{a}_0 \right) \right) J_0 \left(\frac{2\pi}{\lambda} \bar{a}(x) \right). \end{aligned} \quad (49)$$

Thus time averaged moiré fringes form at $\frac{2\pi}{\lambda}\bar{a}(x) = r_k; k = 1, 2, \dots$. This equality corresponds well to the results produced in Subsections 3.1.1.1 and 3.1.1.2 – but the equality is far from being trivial, and it does not follow directly from the formulation of the problem. We should note that the linearization is now performed at a preselected coordinate x – while the whole field of amplitudes was linear by the definition outlined in Subsection 3.1.1.2. A successful implementation of a DVC scheme requires that a preselected area of the cover image should be transformed into a uniform time-averaged moiré fringe. The only controlled parameter of the cover image is pitch $\lambda(x)$. Eq. (49) suggests that the distribution of the pitch should read:

$$\lambda(x) = \frac{2\pi}{r_k}\bar{a}(x), \quad k = 1, 2, \dots \quad (50)$$

Relationship (50) comprises the linearized field of amplitudes $\bar{a}(x)$. We shall use computational tools to test the conjecture that $\bar{a}(x)$ can be replaced by $a(x)$ in Eq. (50).

Let us assume that a one-dimensional elastic structure oscillates according to the law:

$$u(x, t) = 0.1 \sin(\pi x) \sin(\omega t + \varphi), \quad 0 < x < 1. \quad (51)$$

The above stated conjecture implies that a time-averaged moiré fringe must form in the whole domain of x when the stationary moiré grating with the pitch

$$\lambda(x) = 0.1 \frac{2\pi}{r_1} \sin(\pi x) \quad (52)$$

is oscillated according to the law described by Eq. (51). Parameter k is fixed to 1 because the contrast around the first time-averaged moiré fringe (the first root of J_0) is the highest.

We should note that the construction of a stationary moiré grating according to relationship (52) is a not very complex computational exercise – except for the regions around the boundaries where the pitch of the grating quickly converges to zero, and the size of the pixel is not small enough to represent the grayscale oscillation of the grating (as illustrated on the left side of Fig. 3.3). Now, instead of applying the oscillations of the moiré grating according to Eq. (51), we set the oscillation law to:

$$u(x, t) = b \sin(\pi x) \sin(\omega t + \varphi), \quad 0 < x < 1, \quad (53)$$

where parameter b varies from 0 to 0.2 (Fig. 3.3). It can be clearly seen that the time-averaged moiré fringe forms at $b = 0.1$. Thus the conjecture stating that linearized field $\bar{a}(x)$ can be replaced by $a(x)$ in Eq. (50) still holds even for such a complex non-linearized law of motion described by Eq. (51).

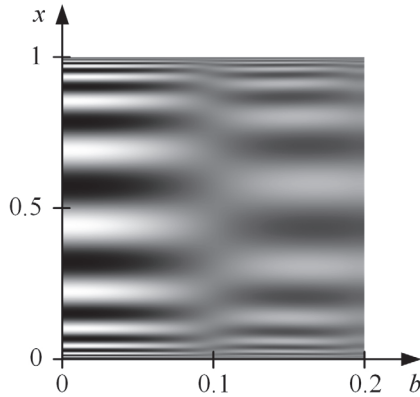


Fig. 3.3. Time-averaged image of the one-dimensional grating (the variation of the pitch is determined according to Eq. (52)); the variation of amplitude b is determined by Eq. (53).

3.1.3. Dynamic Visual Cryptography Based on Deformable Moiré Gratings on Finite Element Grids

In order to determine the 2D deformation fields used for the construction of time-averaged moiré fringes, the numerical model based on the finite element method is built. A thin structural steel plate (density $\rho = 7,850 \text{ kg/m}^3$, Young's modulus $E = 200 \text{ MPa}$) is considered as the structure; its length, width and thickness are $50 \times 20 \times 1 \text{ }\mu\text{m}$, respectively. The volume is meshed by 1976 tetrahedral volume elements resulting in 12237 degrees of freedom. The behavior law of the elements is the classical linear elasticity. Free boundary conditions are chosen for the finite element model. The obtained 5–20 natural eigenfrequencies of a rectangular plate are given in Table 3.1. Figure 3.4 shows the model and a 3D deflection shape of the plate for modes 10 and 12 as an example.

Table 3.1. Numerical eigenfrequencies of 5–20 natural modes for a rectangular plate (length $50 \text{ }\mu\text{m}$, width $20 \text{ }\mu\text{m}$, thickness $1 \text{ }\mu\text{m}$, Young's modulus: 200 MPa)

Mode No.	Num. freq. (kHz)	Mode No.	Num. freq. (kHz)
5	0.074	13	13699
6	0.141	14	14747
7	2086	15	17191
8	3139	16	18846
9	5793	17	19196
10	6749	18	24589
11	11275	19	24681
12	11297	20	28485

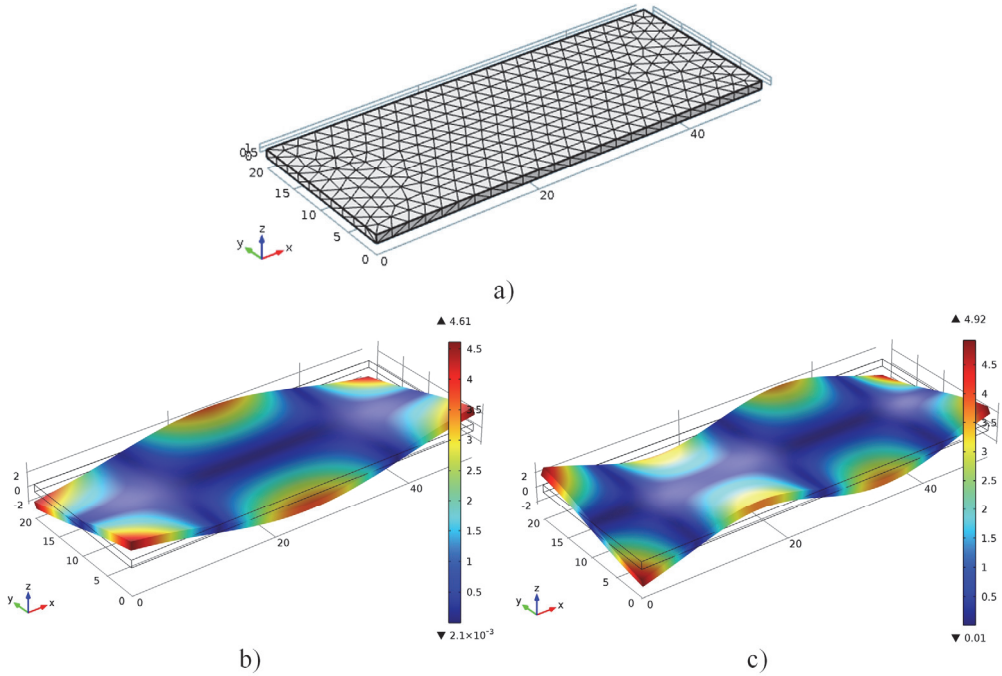


Fig. 3.4. A model of the plate and an example of the Eigen-shapes of the plate. The rectangular plate and the main geometrical parameters used in FEM simulation are shown in part (a). Example deformation shapes for 10 and 12 natural vibration modes (3D model) are presented in (b) and (c), respectively. The black edges indicate the non-deformed beam geometry; the color edges delineate the deformed geometry.

Since one-dimensional moiré gratings have been used so far, a 2D field of deformations $a(x, y)$ determined by FEM computations is sliced horizontally, whereas one-dimensional pitch distributions are computed in adjacent moiré gratings. Therefore, every row of pixels in the digital image of 2D deformations is interpreted as a separate one-dimensional variation of amplitudes $a(x)$. This process is illustrated in Fig. 3.5.

Fig. 3.5 (a) shows the twelfth Eigen-shape of a plate: the white zones stand for the maximum deformations from the state of equilibrium whereas the dark zones stand for the regions which do not oscillate at this resonance frequency. First of all, the maximum amplitude of oscillation must be set at the point of maximal deformations – the Eigen-shape is multiplied by a pre-determined constant. The next step is the formation of an array of one-dimensional moiré gratings. The resolution of Fig. 3.5 (a) is 500×500 pixels. Thus 500 horizontal one-dimensional moiré gratings are formed in Fig. 3.5 (b), and the variation of the pitch in the domain of the grating is constructed according to Eq. (50). The only exception is that the linearized deformation field $\bar{a}(x)$ is replaced by $ka(x) + b$ where $a(x)$ represents the numerical values of the Eigen-shapes in the current grating while k, b are positive constants greater than 0. Constant b is required in order to avoid singularities at the points where amplitudes $a(x)$ become equal to 0; k is required for the control of the range of numerical values of amplitudes. We set $k = 0.0025$ and $b = 0.0075$ in all

further computations – thus the initial range of the Eigen-mode $[-1,1]$ is transformed into the working range of amplitudes $[0.005,0.01]$.

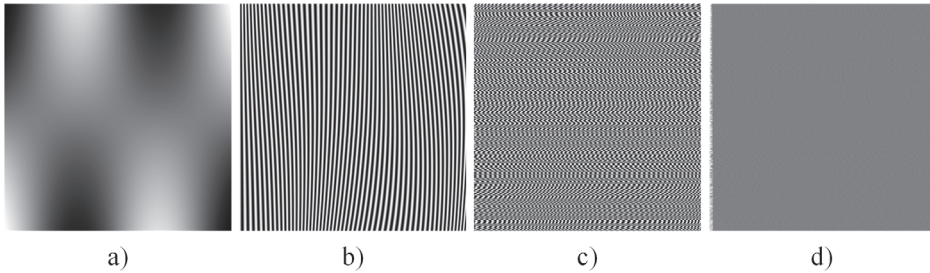


Fig. 3.5. Harmonic oscillations according to the 12-th Eigen-mode of a free rectangular plate produce a gray two-dimensional image; part (a) shows the Eigen-shape; part (b) illustrates the stationary moiré grating (the pitch of the grating varies within interval $\lambda = [0.013,0.026]$; $\lambda(x) = \frac{2\pi}{r_1} a(x)$; part (c) shows the cover image produced from the moiré grating; part (d) illustrates the time-averaged image when the cover image is oscillated according the 12-th Eigen-mode.

We should note that the initial phase of all 500 one-dimensional gratings is set to 0 – thus the image in Fig. 3.5 (b) represents an interpretable array of lines which can reveal the Eigen-shape itself. The stochastic initial phase deflection algorithm (Ragulskis *et al.*, 2009a) is used to confuse the image – the resulting image is shown in Fig. 3.5 (c). We should note that the variation of the pitch in every single one-dimensional grating is not altered in the process.

Now, in-plane unidirectional oscillations according to the x -axis produce time-averaged moiré fringes in the domain of every one-dimensional grating – the resulting image in Fig. 3.5 (d) is completely gray. The exception is the right and left boundaries where the image becomes slightly uneven due to the white background color averaging with the default value.

The secret image is embedded into the cover image by modifying the phase regularization algorithm introduced in (Ragulskis *et al.*, 2009a). The functionality of this algorithm is illustrated in Fig. 3.6. Let us assume that the variation of amplitude $a(x)$ is described in Fig. 3.6 (a). The corresponding grayscale level of the one-dimensional moiré grating is illustrated in Fig. 3.6 (b). Let us assume that the ‘secret’ information must be placed in the middle part of the grating. In other words, a time-averaged moiré fringe should form everywhere except for the region occupied by the middle interval. The field of amplitude governing the harmonic oscillation of the moiré grating is altered by multiplying it by constant C which is little lower (or higher) than 1. The variation of amplitude $a(x)$ in Fig. 3.6 (c) is exactly the same as in Fig. 3.6 (a) – except that it is multiplied by $C = 0.8$; the corresponding moiré grating is shown in Fig. 3.6 (d).

Such an image hiding scheme can be effectively used for embedding dichotomous images into the cover image. It is important to note that the Eigen-shape of the structure serves as the secret key for the visual decoding of the secret. In other words, the secret image leaks from the cover image only if it is oscillated according to the Eigen-mode which was used to encode the image.

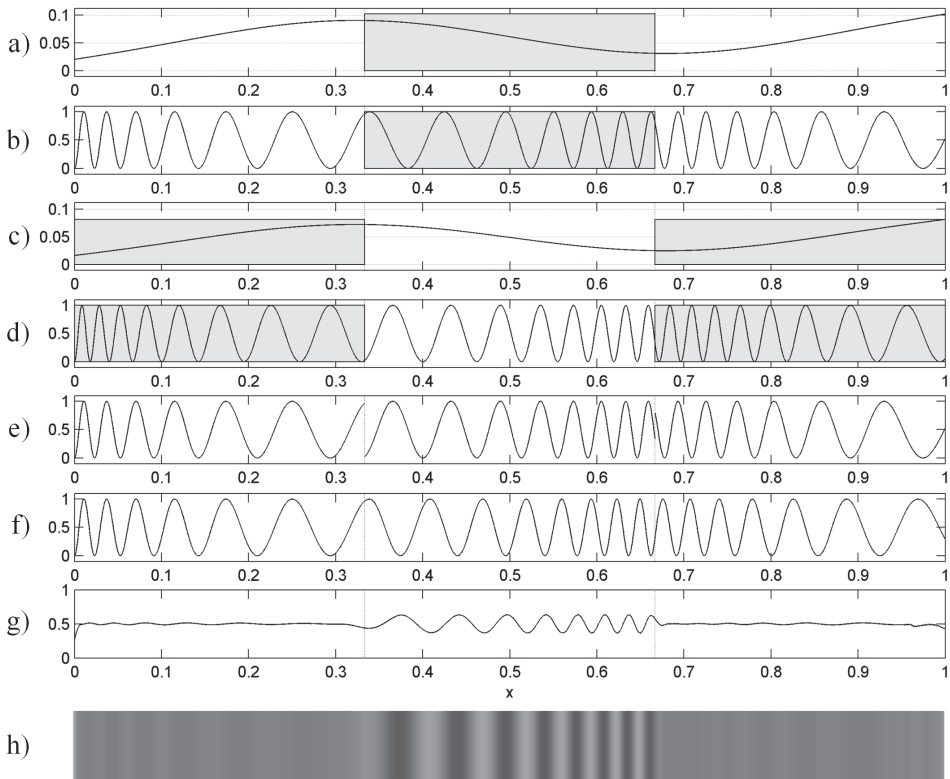


Fig. 3.6. A schematic diagram illustrating the encoding of the secret in a one-dimensional moiré grating. Part (a) shows the field of amplitudes $a(x)$ (according to a predefined Eigen-mode); part (b) illustrates the corresponding moiré grating. Part (c) shows the field of amplitudes used in the regions occupied by the secret; part (d) illustrates the corresponding moiré grating. The composite moiré grating uses the left and the right thirds from part (b) and the middle third from part (d). All the discontinuities in part (e) are eliminated by the phase regularization algorithm (part (f)). The time-averaged image of (f) is shown in parts (g), (h).

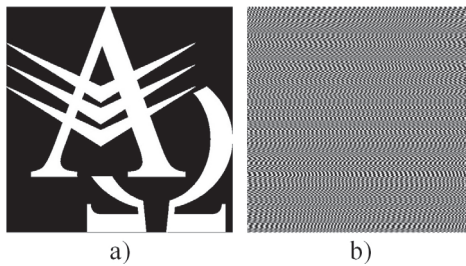


Fig. 3.7. The secret image is shown in part (a); the static cover image with the embedded secret (in such a way that the secret image would leak when the cover image is oscillated according to the 12-th Eigen-mode) is shown in part (b) (the range of the pitch is from 0.013 up to 0.026).

The following computation experiment is used to demonstrate the functionality of such an image hiding scheme based on dynamic visual cryptography. The secret

dichotomous image (shown in Fig. 3.7 (a)) is embedded into the cover image (Fig. 3.7 (b)) according to the twelfth Eigen-shape of the rectangular plate, and the stochastic initial phase and phase regularization algorithms are used to hide the secret. A naked eye could not identify the secret image from the cover image – moreover, the secret can be leaked only when the deformable cover image is oscillated according to the Eigen-mode which was used to encode the secret.

In other words, the Eigen-mode itself can be considered as a key for the visual decoding procedure. Fig. 3.8 shows the results of visual decoding when the cover image is oscillated according to different Eigen-modes; contrast enhancement procedures (Section 1.3.2) are used to highlight moiré fringes in time-averaged images.

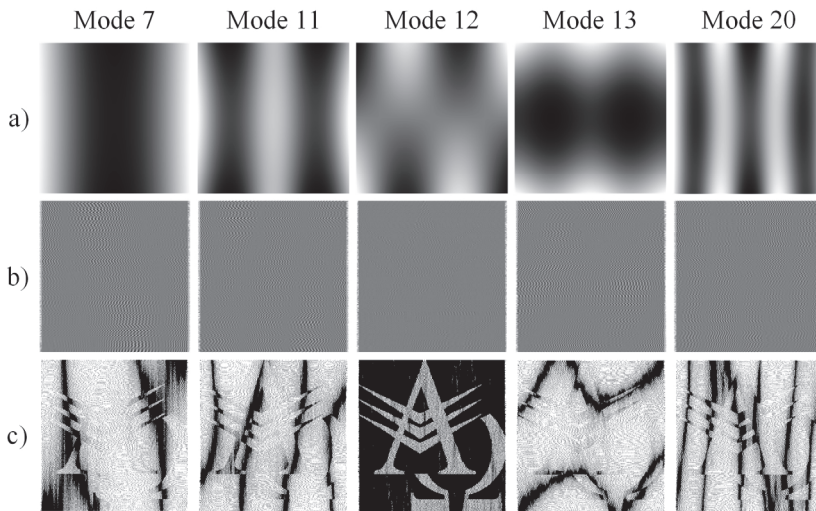


Fig. 3.8. The Eigen-mode serves as the key for the visual decryption of the cover image. The first row shows different Eigen-shapes; the second row demonstrates time-averaged images; the third row features contrast enhanced time-averaged images.

3.2. Dynamic Visual Cryptography Scheme on the Surface of a Vibrating Structure¹¹

The formation of a moiré grating with a harmonic variation of grayscale levels on a surface of a deformable structure (Section 3.1) becomes a challenging technological problem, especially if micro-electro-mechanical systems (MEMS) are considered. Thus the main objective of this Section is to construct the algorithms for the formation of cover images based on the Ronchi-type moiré grating (Petrauskiene *et al.*, 2014). The envelope functions determining the motion induced blur of the Ronchi-type moiré grating depend on the characteristic features of the motion. Even

¹¹ *The results presented in this section have been published as:*

Dynamic Visual Cryptography Scheme on the Surface of a Vibrating Structure.
 Vaidelys M., Aleksienė S., Ragulskienė J.
 Copyright © 2015 JVE International Ltd.

though harmonic oscillations do not result in a completely uniform time-averaged image of the Ronchi-moiré grating, the initial phase scrambling and phase normalization algorithms are used to encode the secret in the cover image. Theoretical relationships between the amplitude of the Eigen-shape, the order of the not completely developed time-averaged fringe, and the pitch of the deformable one-dimensional Ronchi-type moiré grating is derived (Vaidelys *et al.*, 2015a).

3.2.1. Optical Relationships

Let us consider a different one-dimensional geometric moiré grating from a previously presented harmonic moiré grating as shown in Eq. (34) in Section 3.1; a Ronchi-type moiré grating (Petrauskiene *et al.*, 2014):

$$F(x) = \frac{1}{2} + \frac{1}{2} \text{sign} \cos\left(\frac{2\pi}{\lambda} x\right) \quad (54)$$

where x is the longitudinal coordinate; λ is the pitch of the grating; numerical value 0 corresponds to the black color; 1 represents the white color.

Firstly, let us assume that these gratings are formed on the surface of a non-deformable structure which oscillates around the state of equilibrium according to the harmonic law of motion as described in Subsection 3.1.1.1. It was shown that harmonic moiré gratings are blurred due to these oscillations, and time-averaged moiré fringes are formed at the amplitudes corresponding to the roots of J_0 :

$$a_k = \frac{\lambda}{2\pi} r_k, k = 1, 2, \dots, \quad (55)$$

where r_k is the k -th root of J_0 .

However, relationship (44) does not hold for the Ronchi-type moiré grating – time-averaged fringes do not form at any amplitude of harmonic oscillations (Ragulskis *et al.*, 2009c) (Fig. 3.9). Ronchi-type moiré gratings generate time-averaged fringes only if the waveform of the oscillation is triangular (Ragulskis *et al.*, 2009c) – this phenomenon could be exploited as an additional factor serving for encoding security in DVC applications.

The proof and the adaptation of this phenomenon on dynamic visual cryptography is split into two parts. Firstly, the provided idea is simplified by using a harmonic moiré grating instead of a Ronchi-type moiré grating which is oscillated according to the triangular wave-form function. Secondly, if amplitudes resulting in the formation of the fringes could be verified on the simplified version, the hypothesis that time-averaged fringes form under the same amplitude conditions in the case of the Ronchi-type moiré grating could be proved experimentally.

The triangular wave-form function is defined as:

$$u(t) = \frac{2}{\pi} \left(t - \pi \left\lfloor \frac{t}{\pi} + \frac{1}{2} \right\rfloor \right) (-1)^{\lfloor \frac{t}{\pi} + \frac{1}{2} \rfloor}, \quad (56)$$

where the oscillation period is 2π , and value ranges from -1 to 1 .

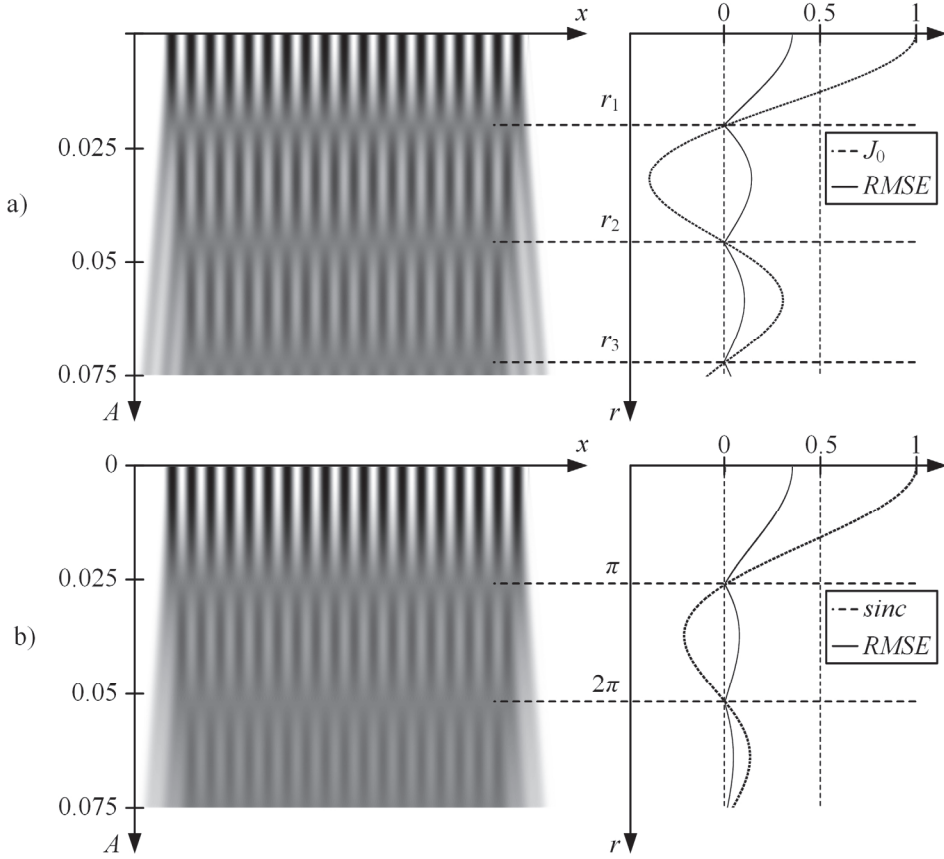


Fig. 3.9. Oscillation of the inelastic one-dimensional moiré grating ($\lambda = 0.02$) produces time-averaged fringes. A time averaged image is shown on the left; the RMSE errors from the equilibrium and the graph of sinc or the Bessel function are shown in the right part of the figure. Time-averaged fringes do form if a harmonic grating is oscillated according to the harmonic law (a).

If the grating is oscillated according to triangular wave-form function (b), fringes form only at the sinc function's roots.

Let the deformation from the state of equilibrium at point x at time moment t be equal to $u(x, t)$. Then, the explicit deformation of the moiré grating reads as defined in Eq. (35): $F(x, t) = \frac{1}{2} + \frac{1}{2} \cos\left(\frac{2\pi}{\lambda} \mu(x, t)\right)$ where x can be explicitly expressed in form Eq. (37).

Let us describe an oscillation around the state of equilibrium with function $u(x, t)$:

$$u(x, t) = a(x) \cdot t. \quad (57)$$

It is the simplified form of a triangular wave-form function where $a(x)$ is the Eigen-shape of in-plane oscillations and time $t \in [-1, 1]$. The field of amplitudes $a(x)$ can be linearized around point x_0 , the same as in Subsection 3.1.1, and x yields

the following form:

$$x = \frac{z - (a_0 - \dot{a}_0 x_0)t}{1 + \dot{a}_0 t}. \quad (58)$$

Finally, the grayscale level of the moiré grating at coordinate x and time moment t reads:

$$F(x, t) = \frac{1}{2} + \frac{1}{2} \cos\left(\frac{2\pi}{\lambda} \cdot \frac{x - (a_0 - \dot{a}_0 x_0)t}{1 + \dot{a}_0 t}\right). \quad (59)$$

3.2.1.1. Non-Deformable Moiré Grating

Let us assume that $a(x) = A$ (A is a constant) and that the analyzed structure oscillates according to the triangular wave-form function. This means that the deflection which describes the oscillation of a non-deformable body around the state of equilibrium is $u(x, t) = At$ (Ragulskis *et al.*, 2009a). Then, the grayscale level of the moiré grating at time step t reads:

$$F(x, t) = \frac{1}{2} + \frac{1}{2} \cos\left(\frac{2\pi}{\lambda} \cdot (x - At)\right). \quad (60)$$

Time-averaging techniques can be used to register the image of the grating (Ragulskis *et al.*, 2009a, Kobayashi, 1993):

$$\begin{aligned} \bar{F}(x) &= \frac{1}{2} \int_{-1}^1 F(x, t) dt \\ &= \frac{1}{2} + \frac{1}{4} \int_{-1}^1 \left[\cos\left(\frac{2\pi}{\lambda} x\right) \cos\left(\frac{2\pi}{\lambda} At\right) + \sin\left(\frac{2\pi}{\lambda} x\right) \sin\left(\frac{2\pi}{\lambda} At\right) \right] dt \\ &= \frac{1}{2} + \frac{1}{4} \cos\left(\frac{2\pi}{\lambda} x\right) \int_{-1}^1 \cos\left(\frac{2\pi}{\lambda} At\right) dt + 0 \\ &= \frac{1}{2} + \frac{1}{4} \cos\left(\frac{2\pi}{\lambda} x\right) \frac{\lambda}{2\pi A} \sin\left(\frac{2\pi}{\lambda} At\right) \Big|_{-1}^1 \\ &= \frac{1}{2} + \frac{1}{4} \cos\left(\frac{2\pi}{\lambda} x\right) \frac{\lambda}{2\pi A} 2 \sin\left(\frac{2\pi}{\lambda} A\right) = \frac{1}{2} + \frac{1}{2} \cos\left(\frac{2\pi}{\lambda} x\right) \frac{\sin\left(\frac{2\pi}{\lambda} A\right)}{\frac{2\pi}{\lambda} A} \\ &= \frac{1}{2} + \frac{1}{2} \cos\left(\frac{2\pi}{\lambda} x\right) \operatorname{sinc}\left(\frac{2\pi}{\lambda} A\right), \end{aligned} \quad (61)$$

where $\operatorname{sinc}(x) = \frac{\sin(x)}{x}$ is the cardinal sine function. We should note that the distribution of the grayscale level in the time-averaged image does not depend on the characteristics of triangular wave-form function (57) and this is why the simple form could be used in the provided calculations.

Gray time-averaged moiré fringes only form when $\frac{2\pi}{\lambda} A_k = r_k = \pi k$, where $r_k = \pi k$ are the roots of $\operatorname{sinc}(x) = 0$, $k = 1, 2, \dots$ (Fig. 3.9(b)).

3.2.1.2. Deformable Moiré Grating; Linear Deformation Field

Next, let us assume that $a(x) = Ax$. The principal difference from non-deformable moiré gratings (as described in Subsection 3.2.1.1) is that the moiré grating will deform proportionally to coordinate x when the body is oscillated in time. However, a harmonic moiré grating can still be formed on the surface of the one-dimensional body in the state of equilibrium.

Linearization around x_0 yields: $a(x) = Ax_0 + A(x - x_0)$; $a_0 = Ax_0$; $\dot{a}_0 = A$. Thus Eq. (12) now reads:

$$F(x, t) = \frac{1}{2} + \frac{1}{2} \cos\left(\frac{2\pi}{\lambda} \frac{x}{1 + \dot{a}_0 t}\right) = \frac{1}{2} + \frac{1}{2} \cos\left(\frac{2\pi}{\lambda} (1 - (\dot{a}_0 t + O(\dot{a}_0 t)^2))x\right) \quad (62)$$

$$\approx \frac{1}{2} + \frac{1}{2} \cos\left(\frac{2\pi}{\lambda} x - \frac{2\pi}{\lambda} Axt\right), \quad t \in [-1, 1].$$

We should note that a singularity occurs at $A = 1$ in Eq. (62). Thus it is assumed that $0 < A \ll 1$. Finally, the time-averaged image reads:

$$\begin{aligned} \bar{F}(x) &= \frac{1}{2} \int_{-1}^1 F(x, t) dt \\ &= \frac{1}{2} + \frac{1}{4} \int_{-1}^1 \left[\cos\left(\frac{2\pi}{\lambda} x\right) \cos\left(\frac{2\pi}{\lambda} Axt\right) + \sin\left(\frac{2\pi}{\lambda} x\right) \sin\left(\frac{2\pi}{\lambda} Axt\right) \right] dt \quad (63) \\ &= \frac{1}{2} + \frac{1}{4} \cos\left(\frac{2\pi}{\lambda} x\right) \frac{\lambda}{2\pi Ax} \sin\left(\frac{2\pi}{\lambda} Axt\right) \Big|_{-1}^1 \\ &= \frac{1}{2} + \frac{1}{2} \cos\left(\frac{2\pi}{\lambda} x\right) \text{sinc}\left(\frac{2\pi}{\lambda} Ax\right). \end{aligned}$$

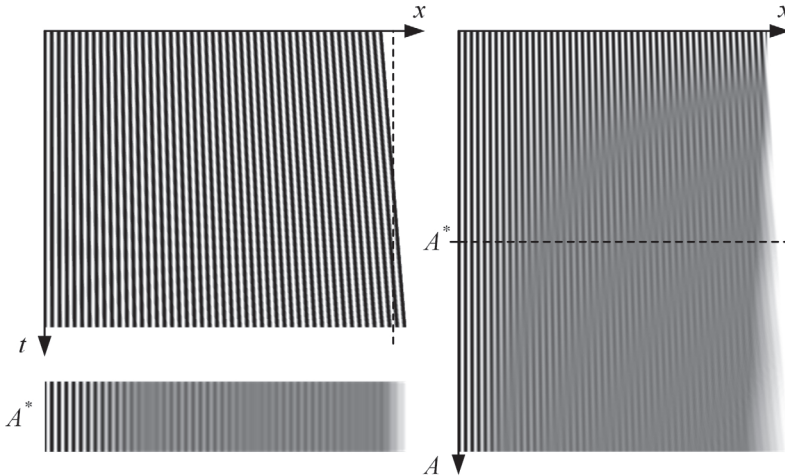


Fig. 3.10. Deformable one-dimensional moiré grating produces time-averaged fringes when oscillated according to the triangular wave-form. One period ($t \in [-1, 1]$) of oscillations is shown in the top left image; one-dimensional time-averaged image at $A^* = 0.035$ is shown at the bottom on the left; the formation of time-averaged fringes when employing different amplitudes is illustrated on the right; $A = 0.001, 0.07$.

Here, time-averaged moiré fringes form at $\frac{2\pi}{\lambda}Ax = r_k = \pi k; k = 1, 2, \dots$ Figure 3.10 shows the oscillating moiré grating in the left upper image. The one-dimensional moiré grating is motionlessly fixed on the left side whereas the right side of the grating deforms at amplitude $A^* = 0.035$. The vertical dashed line marks the equilibrium state of the one-dimensional deformable structure; the pitch of the moiré grating is $\lambda = 0.02$. The right part of Fig. 3.10 shows time-averaged images of the one-dimensional moiré grating at different amplitudes A . The left bottom part of Fig. 3.10 illustrates time-averaged moiré fringes at $A^* = 0.035$.

3.2.1.3. Deformable Moiré Grating; Nonlinear Deformation Field

In order to develop an image hiding scheme based on deformable moiré gratings on finite element grids, the deformation field $a(x)$ needs to be a nonlinear function. Let us set $x_0 = 0$ and denote $\bar{a}(x) = a_0 + \dot{a}_0 x$. Then, Eq. (59) reads:

$$\begin{aligned} F(x, t) &= \frac{1}{2} + \frac{1}{2} \cos\left(\frac{2\pi x - a_0 t}{\lambda(1 + \dot{a}_0 t)}\right) \approx \frac{1}{2} + \frac{1}{2} \cos\left(\frac{2\pi}{\lambda}(x - a_0 t)(1 - \dot{a}_0 t)\right) \\ &= \frac{1}{2} + \frac{1}{2} \cos\left(\frac{2\pi}{\lambda}((x + a_0 \dot{a}_0 t^2) - \bar{a}(x)t)\right). \end{aligned} \quad (64)$$

If $\dot{a}_0 \ll 1$ and $t^2 \leq 1$ then $a_0 \dot{a}_0 t^2 \ll 1$ and:

$$\begin{aligned} \tilde{F}(x, t) &= \frac{1}{2} + \frac{1}{2} \cos\left(\frac{2\pi}{\lambda}x - \frac{2\pi}{\lambda}\bar{a}(x)t\right) \\ &= \frac{1}{2} + \frac{1}{2} \cos\left(\frac{2\pi}{\lambda}x\right) \cos\left(\frac{2\pi}{\lambda}\bar{a}(x)t\right) + \frac{1}{2} \sin\left(\frac{2\pi}{\lambda}x\right) \sin\left(\frac{2\pi}{\lambda}\bar{a}(x)t\right). \end{aligned} \quad (65)$$

We should note that $\int_{-1}^1 \sin\left(\frac{2\pi}{\lambda}\bar{a}(x)t\right) dt = 0$ due to the evenness of the sine function. Then, the time-averaged image reads:

$$\begin{aligned} \bar{F}(x) &= \frac{1}{2} \int_{-1}^1 F(x, t) dt \approx \frac{1}{2} \int_{-1}^1 \tilde{F}(x, t) dt \\ &= \frac{1}{2} + \frac{1}{4} \int_{-1}^1 \left[\cos\left(\frac{2\pi}{\lambda}x\right) \cos\left(\frac{2\pi}{\lambda}\bar{a}(x)t\right) + \sin\left(\frac{2\pi}{\lambda}x\right) \sin\left(\frac{2\pi}{\lambda}\bar{a}(x)t\right) \right] dt \\ &= \frac{1}{2} + \frac{1}{4} \cos\left(\frac{2\pi}{\lambda}x\right) \int_{-1}^1 \cos\left(\frac{2\pi}{\lambda}\bar{a}(x)t\right) dt \\ &= \frac{1}{2} + \frac{1}{4} \cos\left(\frac{2\pi}{\lambda}x\right) \frac{\lambda}{2\pi\bar{a}(x)} \sin\left(\frac{2\pi}{\lambda}\bar{a}(x)t\right) \Big|_{-1}^1 \\ &= \frac{1}{2} + \frac{1}{2} \cos\left(\frac{2\pi}{\lambda}x\right) \text{sinc}\left(\frac{2\pi}{\lambda}\bar{a}(x)\right). \end{aligned} \quad (66)$$

Thus time averaged moiré fringes form at $\frac{2\pi}{\lambda}\bar{a}(x) = r_k = \pi k; k = 1, 2, \dots$, which corresponds well to the results produced in Subsections 3.2.1.1 and 3.2.1.2. The next goal is to transform the whole image into a time-averaged moiré fringe (only by varying pitch $\lambda(x)$). Thus the distribution of the pitch (Eq. (50)) reads:

$$\lambda(x) = \frac{2\pi}{k} \bar{a}(x), \quad k = 1, 2, \dots \quad (67)$$

In the previous relationship, λ still depends on the linearized field of amplitudes $\bar{a}(x)$. The conjecture that $\bar{a}(x)$ can be replaced with $a(x)$ will be tested and validated by using computational tools. Let us assume that a one-dimensional elastic structure oscillates according to the following law:

$$u(x, t) = 0.1 \sin(\pi x) \cdot t, \quad 0 \ll x \ll 1, \quad t \in [-1; 1]. \quad (68)$$

The above stated presumption implies that a time-averaged moiré fringe must form in the whole domain of x when the stationary moiré grating has the variable pitch in respect of x :

$$\lambda(x) = 0.1 \cdot \frac{2\pi}{r_k} \cdot \sin(\pi x), \quad k = 1, 2, \dots \quad (69)$$

Parameter k is fixed to 1 because the contrast around the first time-averaged moiré fringe is the highest (the first root of sinc is $r_1 = \pi$). Now, instead of applying the oscillations of the moiré grating according to Eq. (68), the oscillation process is set to:

$$u(x, t) = b \sin(\pi x) \cdot t, \quad 0 \ll x \ll 1, \quad t \in [-1; 1], \quad (70)$$

where parameter b varies from 0 to 0.2 (Fig. 3.11). It can be clearly seen that the time-averaged moiré fringe does form at $b = 0.1$. Thus the conjecture stating that the linearized field $\bar{a}(x)$ can be replaced by $a(x)$ in Eq. (67) holds for the triangular wave-form law of motion.

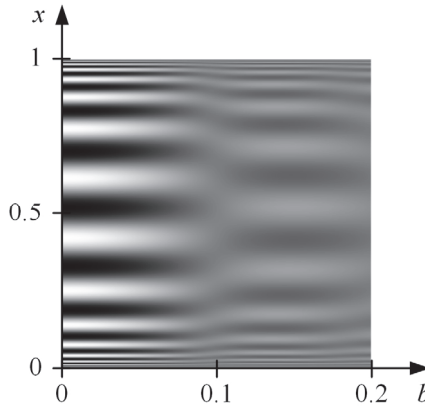


Fig. 3.11. Time-averaged image of the one-dimensional grating (the variation of the pitch is determined according to Eq. (69)); the variation of amplitude b is determined by Eq. (70).

3.2.2. Ronchi-Type Moiré Gratings on Finite Element Grids

The main objective of this Subsection is to develop an image hiding scheme based on deformable Ronchi-type moiré gratings on finite element grids. In other words, the cover image should only have two colors: black and white. In

Subsection 3.2.1, it was proved that time-averaged fringes form when a harmonic moiré grating is oscillated according to the triangular wave-form function. This raises a hypothesis that the same should hold true with Ronchi-type moiré gratings (see Eq. (54)).

This hypothesis can be confirmed experimentally by using the same experimental tools as in the case with harmonic moiré gratings. From Fig. 3.12, it can be seen that time-averaged fringes do form at $r_k = \pi k$ if a Ronchi-type moiré grating is oscillated according to the triangular wave-form function. We should note that a Ronchi-type grating is used in Fig. 3.12 instead of the harmonic grating presented in Fig. 3.9 (b).

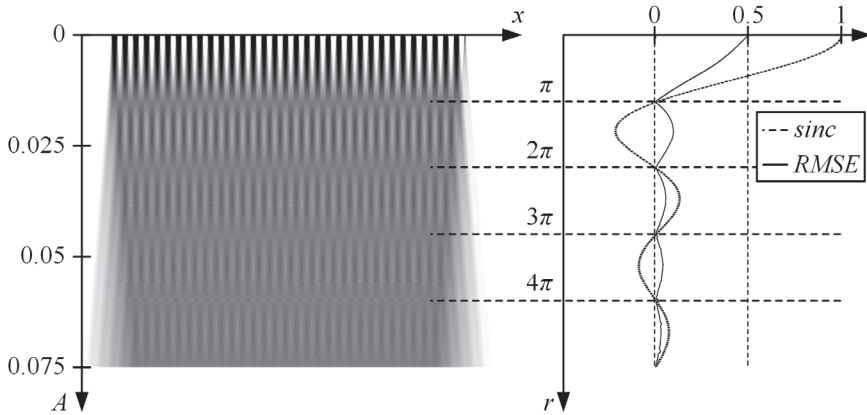


Fig. 3.12. Time-averaged fringes form if a Ronchi-type moiré grating is oscillated according to the triangular wave-form function. Time-averaged fringes form at sinc function’s roots.

3.2.3. Dynamic visual Cryptography Based on Deformable Moiré Gratings on Finite Element Grids

The nonlinear deformation field is used for the formation of time-averaged moiré fringes. The process of 2D deformation determined by FEM computations is illustrated in Fig. 3.13.

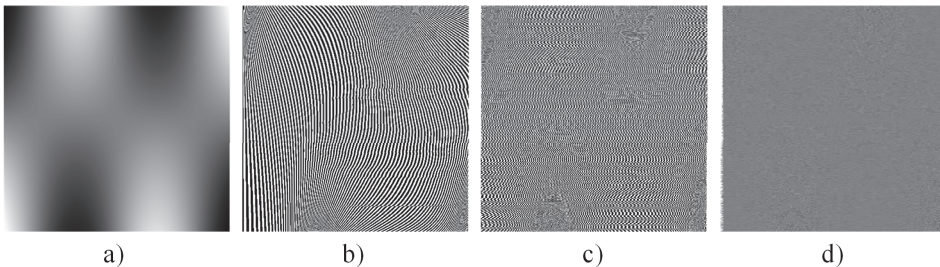


Fig. 3.13. Triangular wave-form oscillations according to the 12-th Eigen-mode of a Ronchi-type moiré produce a gray two-dimensional image; part (a) shows the Eigen-shape; part (b) illustrates the stationary moiré grating (the pitch of the grating varies within interval $\lambda = [0.002, 0.02]$; $\lambda(x) = 2a(x)$); part (c) shows the cover image produced from the moiré grating; part (d) illustrates the time-averaged image when the cover image is oscillated according to the 10-th Eigen-mode.

The 2D deformation field is shown in Fig. 3.13 (a) where the 12-th Eigen-shape of a plate is selected. The dark zones stand for no oscillation, and the white zones stand for maximum deformations from the equilibrium. The resolution of Fig. 3.13 (a) is 500×500 pixels; therefore, all further calculations are related to this size. As the provided model forms feature only one-dimensional time-averaged moiré, an array of 500 one-dimensional moiré gratings must be formed and concatenated vertically. This results in a 2D stationary moiré grating shown in Fig. 3.13(b). The pitch of the grating is constructed by using Eq. (69) where the linearized deformation field $\bar{a}(x)$ is replaced by $ka(x) + b$. This transformation of the numerical values of the Eigen-shapes $a(x)$ is necessary in order to avoid singularities at the points where amplitudes $a(x)$ become equal to 0. k , b are positive constants greater than 0, and all further computations are set to $k = 0.0045$ and $b = 0.0055$. Thus if the initial range of the Eigen-mode is $[-1, 1]$, after this transformation, the working range of amplitudes becomes $[0.001, 0.01]$.

Now, we must take note that the initial phase of all 500 horizontal 1D gratings is the same and equals to 0. This results in an interpretable Eigen-shape function. In order to avoid this issue, the stochastic initial phase scrambling algorithm (Ragulskis *et al.*, 2009a) should be used to complicate the pattern (Fig. 3.13 (c)) (during this process, the pitch in every single one-dimensional grating is not altered).

After this preparation, every one-dimensional grating is time-averaged according to the x -axis by using the triangular function. These in-plane unidirectional oscillations result in an almost gray image shown in Fig. 3.13 (d). Thus we have experimentally proved that the Ronchi-type grating does actually result in time-averaged moiré fringes in the domain of every one-dimensional grating when the nonlinear amplitude function is used.

The last step is to encode the secret image into the cover image, which is done by modifying the phase regularization algorithm introduced in (Ragulskis *et al.*, 2009a) (Fig. 3.14). The variation of amplitude $a(x)$ is depicted in Fig. 3.14 (a). The corresponding grayscale level of the one-dimensional moiré grating is illustrated in Fig. 3.14 (b). Let us place the block of ‘secret’ information in the middle of the grating, which means that the time-averaged moiré fringe should form everywhere except in the middle. Now, the white zones (the left and the right-third of Fig. 3.14 (b) as well as the middle-third of Fig. 3.14 (d)) are taken into the composite grating illustrated in Fig. 3.14 (e). Direct copying results in a discontinuous grating with phase jumps at the joining points. Phase jumps are eliminated with the phase-regulation algorithm (Fig. 3.14 (f)). We should note that the variation of the pitch is not altered in this process. Lastly, the time-averaging of Fig. 3.14 (f) results in Fig. 3.14 (g) as it is oscillated by the law defined by Eq. (37) whereas the field of amplitudes $a(x)$ is determined by Fig. 3.14 (a). Time-averaged moiré fringes form in the middle-third of the time-averaged image; the left-third and the right-third of the image do clearly stand out from the gray background.

In order to assure the functionality of this image hiding scheme in the 2D case, a secret dichotomous image Fig. 3.15 (a) is embedded into the cover image Fig. 3.15 (b). The cover image was generated according to the 12-th Eigen-mode where the initial phase is stochastic in all horizontal one-dimensional gratings, and

phase regularization algorithms are used to hide the secret. The encoding result is uninterpretable to naked eyes.

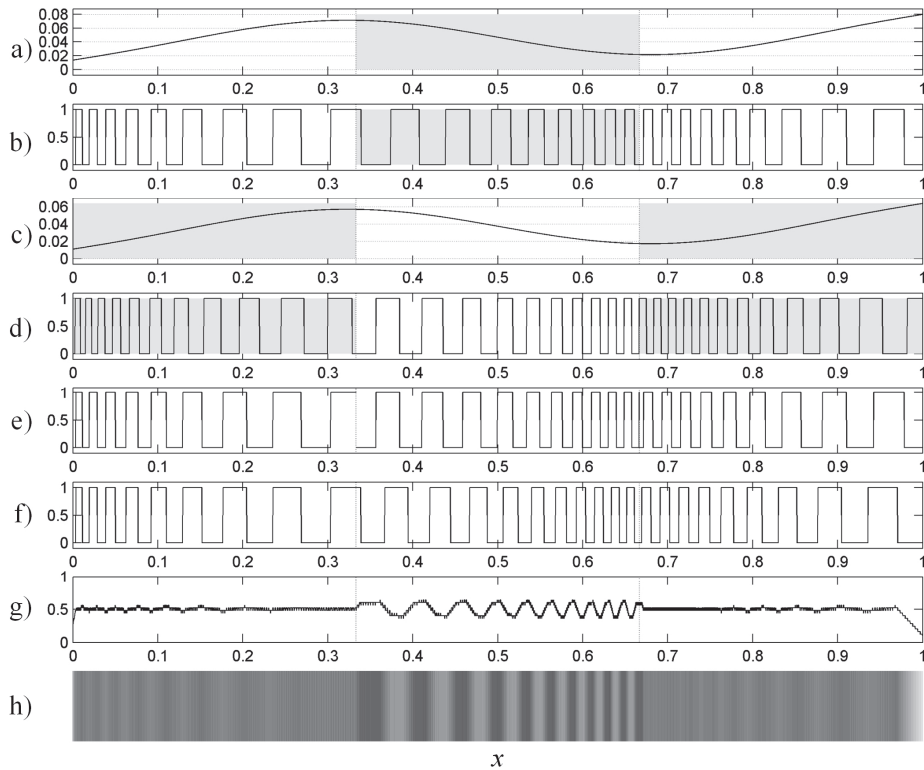


Fig. 3.14. A schematic diagram illustrating the encoding of the secret in a one-dimensional moiré grating. Part a) shows the field of amplitudes $a(x)$. Part b) illustrates the corresponding moiré grating. Part c) shows the field of amplitudes used in the regions occupied by the secret. Part d) illustrates the corresponding moiré grating. The composite moiré grating uses the left and the right thirds from part b) and the middle third from part d). All the discontinuities in part e) are eliminated by the phase regularization algorithm (part f)). The time-averaged image of f) is shown in parts g) and h).



Fig. 3.15. The secret image is shown in part (a); the cover image with the embedded secret according to the 12-th Eigen-mode is shown in part (b).

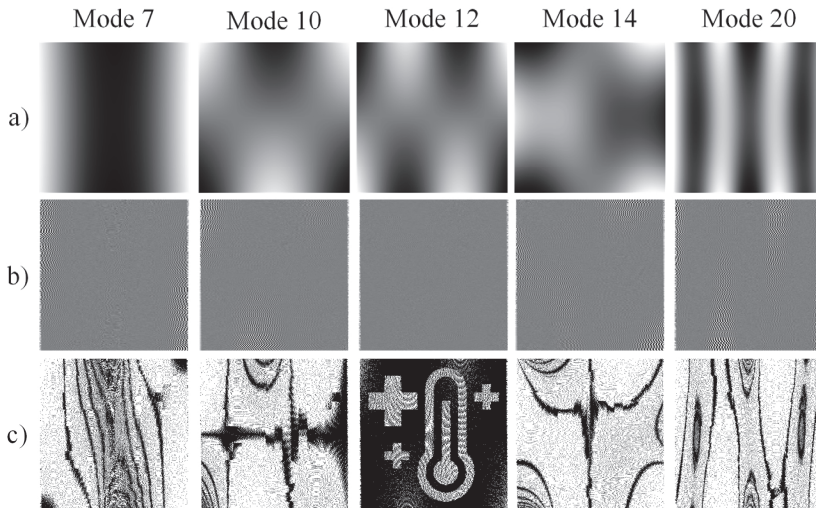


Fig. 3.16. The Eigen-mode serves as the key for the visual decryption of the cover image. The first row shows different Eigen-shapes; the second row presents time-averaged images; the third row contains contrast enhanced time-averaged images.

Moreover, the dependency of the decoding process on the initial Eigen-shape of the structure introduces one more security feature: the secret information is inaccessible without using the correct Eigen-shape used to oscillate the cover image. Thus the Eigen-mode itself can be considered as a key for the visual decoding procedure. Such dependence is shown in Fig.3.16 where visual decoding is executed by using different Eigen-modes. The contrast enhancement procedures (Ragulskis *et al.*, 2009b) are used to highlight moiré fringes in time-averaged images.

3.3. Concluding Remarks

The image hiding scheme in time-averaged moiré gratings on finite element grids is presented in this section. An image encoding scheme in deformable one-dimensional moiré gratings oscillating according to a predefined Eigen-mode is developed and implemented for the construction of two-dimensional digital dichotomous secret images. The secret is leaked from the cover image in the form of a pattern of time-averaged moiré fringes when it is oscillated according to a predefined Eigen-mode. The efficiency of the proposed scheme is illustrated by computational examples employing finite element grids.

Two dynamic visual cryptography schemes are presented by using this technique. The first scheme is based on harmonic oscillations of the deformable harmonic moiré grating whereas the second one is based on Ronchi gratings deformed according to the triangular waveform function. Overall, harmonic moiré grating results in the better image hiding quality. However, the Ronchi-type grating has the advantage in the practical situations. Since the presented image communication scheme mimics physical processes, it can be adapted in the control of MOEMS. Ronchi grating makes it easier to form the stochastic cover moiré

image on the surface of a cantilever or a diaphragm.

Defects of the grid as well as defects of the material (or the geometry) of the FEM model could be considered as the next step in the security of such a DVC scheme. The next step could be a FEM grid (or the FEM model in general) with a micro-crack. It is well known that Eigen-modes can be exploited for the detection of micro-cracks. Thus cover images could be constructed in such a way that the secret image would leak only if the FEM Eigen-mode corresponded to a structure with an exactly predefined micro-crack.

4. THE PSEUDO-ORDER OF A 2D SEQUENCE AND THE COMPLEXITY OF DIGITAL IMAGES¹²

The application of the order of a two-dimensional (2D) sequence is introduced in this Section. The order of a 2D sequence is a natural but not trivial extension of the order of one-dimensional (1D) linear recurrent sequences (Telksnys *et al.*, 2016). The extension of 1D LRS to two dimensions could open new possibilities for the analysis of digital images. It is demonstrated that the order of 2D sequences can be used to estimate the complexity of self-organizing patterns with respect to each spatial coordinate. This advantage could be used in analyzing the pattern's state during its formation and to detect if the pattern is not under- or over-developed.

It is clear that any real-world time series does not have a finite LRS-order simply because real world time series are inevitably contaminated by noise. Otherwise (if the LRS-order of a real-world time series were finite), the dynamics of the sequence would be governed by a deterministic law – which contradicts the definition of noise (Ragulskis *et al.*, 2011b). Thus the concept of the pseudo-order is used to evaluate the order of a 2D sequence.

4.1. Pseudo-Order of a 1D Sequence

A computational framework for the determination of LRS pseudo-orders based on the SVD of the Hankel matrix is presented by (Landauskas *et al.*, 2016).

As the computation of the Hankel determinants (27) is numerically unstable, it is not feasible to use the definition of 2-LRS directly to determine if a given 2D sequence has a finite order. To provide a more stable evaluation of a 2D sequence's order, the concept of the pseudo-order is used.

For a 1D sequence $(p_j; j \in Z_0)$, the pseudo-order is computed by using the SVD by the following algorithm (Landauskas *et al.*, 2016):

1. A Hankel matrix H_K is formed from the sequence $(p_j; j \in Z_0)$ by using the first K elements.
2. The SVD of H_K is performed:

$$H_K = USV^T, \quad (71)$$

where U , V are the matrices of the orthonormal eigenvectors of HH^T , H^TH , respectively, and S is a diagonal matrix containing the ordered singular values:

$$\sigma_1^2 \geq \sigma_2^2 \geq \dots \geq \sigma_K^2 \geq 0. \quad (72)$$

3. For a chosen $\varepsilon > 0$, define pseudo-order \tilde{K} of the given sequence as the number of singular values that are greater than ε :

¹² The results presented in this section have been published as:

The Order of a 2-Sequence and the Complexity of Digital Images.
Telksnys T., Navickas Z., Vaidelys M., Ragulskis M.
Copyright © 2016 World Scientific Publishing Company.

$$\tilde{K}: \sigma_{\tilde{K}}^2 > \varepsilon, \sigma_{\tilde{K}+1}^2 \leq \varepsilon. \quad (73)$$

It has been demonstrated by (Landauskas *et al.*, 2016) that the pseudo-order of a sequence tends to the true order as $\varepsilon \rightarrow 0$; however, setting $\varepsilon = 0$ would lead to a great sensitivity to noise in the sequence $(p_j; j \in \mathbb{Z}_0)$. Thus, for real-world applications, it is recommended to choose $\varepsilon > 0$ and investigate the pseudo-order. A number of algorithms that use the concept of 1-LRS have successfully applied this approach (Landauskas *et al.*, 2013, Landauskas *et al.*, 2014, Landauskas *et al.*, 2016).

4.2. Pseudo-Order of a 2D Sequence

The concept of the pseudo-order outlined in the previous section cannot be applied directly to 2D sequences because they consist of two sets containing infinitely many 1D sequences. However, the problems that occur in the 1D case are magnified when considering 2D sequences. In particular, it is not immediately clear how to evaluate the row and column orders of a given real-world 2D sequence because the characteristic roots of each row (column) are influenced by noise.

We propose the following approach to solve this problem by using the mean order of the rows (columns) of the given 2D sequence. Let $X = [x_{jr}]_{j,r=0}^{+\infty}$ be a 2-LRS that is homogenous. This means that the differences between the 1D orders of rows (columns) are not large. Let us suppose that the row order of X is equal to N . Then, $\text{order}(x_{jr}; r \in \mathbb{Z}_0) = N_j$ where $j \in \mathbb{Z}_0$.

The limit of the mean order of all the rows is considered:

$$\bar{N} = \lim_{j \rightarrow +\infty} \frac{1}{j} \sum_{k=0}^{j-1} N_k. \quad (74)$$

Since $0 \leq N_k \leq N, k \in \mathbb{Z}_0$, the mean order (Eq. (74)) can be written as:

$$\bar{N} = \lim_{j \rightarrow +\infty} \frac{1}{j} \sum_{k=0}^{j-1} (N - q_k) \quad (75)$$

where $0 \leq q_k \leq N$. Equation (75) then yields:

$$N - \max_{j \in \mathbb{Z}_0} q_j \leq \bar{N} \leq N - \min_{j \in \mathbb{Z}_0} q_j \quad (76)$$

which can be rearranged into:

$$\bar{N} + \max_{j \in \mathbb{Z}_0} q_j \leq N \leq \bar{N} + \min_{j \in \mathbb{Z}_0} q_j. \quad (77)$$

If the considered 2D sequence is homogeneous, the differences in order between rows q_j are small, thus (Eq. (77)) yields the approximation:

$$\bar{N} \approx N. \quad (78)$$

By using Eq. (78) and the SVD, the row pseudo-order of a 2D sequence X can

be evaluated by using the algorithm given in Section 4.1 with the same ε on each row and considering the mean value of the obtained pseudo-ranks. Thus the pseudo row rank \tilde{N} of homogenous 2D sequence X computed from the first m rows is defined as:

$$\tilde{N} := \frac{1}{m} \sum_{j=0}^{m-1} \tilde{N}_j. \quad (79)$$

Analogous computations can also be performed for the columns of a given homogenous 2D sequence X .

4.3. A Synthetic Numerical Example

Let us consider two digital images – a black-and-white image of bricks (Fig. 4.1 (e) denoted as image B) and a grayscale image of uniformly distributed random pixels (Fig. 4.1 (a) denoted as image N). Let us construct a sequence of digital images by assuming discrete values of parameter q in the following equation:

$$I(q) = (1 - q)N + qB, \quad 0 \leq q \leq 1. \quad (80)$$

It is clear that $I(0) = N$, $I(1) = B$. The image of bricks evolves from the noise as q varies from 0 to 1 (Fig. 4.1).

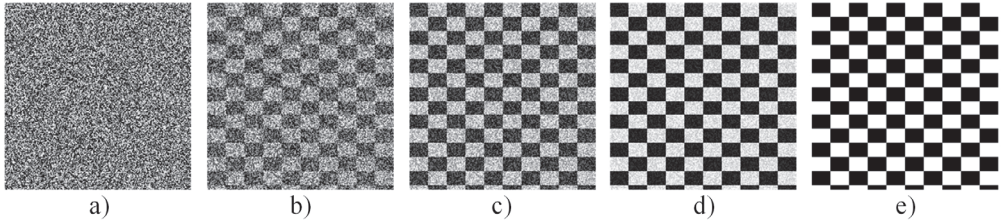


Fig. 4.1. The digital image of bricks evolves from noise as parameter q varies from 0 to 1. Digital images in parts a)–e) are shown at $q = 0, 0.25, 0.5, 0.75$ and 1, accordingly.

4.3.1.1. LRS Pseudo Order and Shannon Entropy

It is well known that Shannon entropy $H(X)$ of a digital image determines the randomness of that image (Borda, 2011). We use standard techniques for the computation of the entropy:

$$H(X) = - \sum_{k=1}^m p_k \log_2 p_k, \quad (81)$$

where p_k is the histogram count for the k th of m bins of the given digital image X .

The entropy Eq. (81) is computed for a series of digital images as q varies from 0 to 1 according to Eq. (80) (Fig. 4.2). We should note that we visualize the inverse of the entropy scaled to the interval $[0, 1]$ in Fig. 4.2. Such a representation helps to clearly interpret the randomness of the evolving image. The entropy is maximal at $q = 0$, and it monotonically decreases as the image of bricks becomes clearer (Fig. 4.2).

There exists a natural relation between the LRS order of a sequence and the algebraic complexity of that sequence (Ragulskis *et al.*, 2011b). Therefore, one could expect a similar relationship between the 2-LRS order and the complexity of the digital image as well.

We use the same series of digital images represented by Eq. (80) and compute the averaged LRS pseudo-orders for rows and columns while using the algorithm described in Section 4.1 (the dimension of the Hankel matrix is set to 80; ε is set to 0.5). However, since the inverse of the entropy is visualized in Fig. 4.2, we also visualize inverse pseudo-orders in Fig. 4.2.

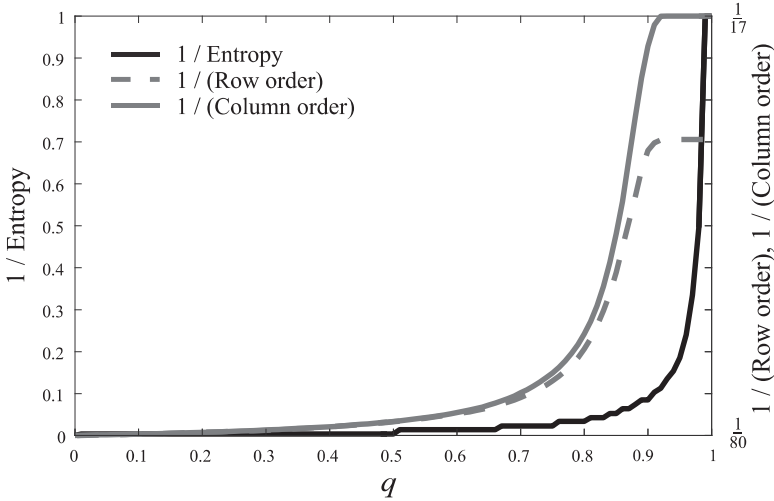


Fig. 4.2. Evolution of entropy and row/column LRS pseudo-order as parameter q varies from 0 to 1. The left y-axis represents the inverse of entropy $H(X)$. The right y-axis represents the inverse of the average row and column LRS-pseudo-order.

The 2-LRS pseudo-order for the image of noise is equal to $(80, 80)$ – which corresponds to $\left(\frac{1}{80}, \frac{1}{80}\right)$ in Fig. 4.2 at $q = 0$. Then, the LRS pseudo-orders for rows and columns monotonically decrease as q varies from 0 to 1 (Fig. 4.2). However, the variation of the LRS pseudo-orders for rows and columns is not identical. The periodicity of the image of bricks along the rows is longer than the periodicity of this image along the columns (this is due to the shape of the bricks). The shorter average period results in a smaller LRS pseudo-order. The 2-LRS pseudo-order for the image of bricks (without noise) is equal to $(22, 17)$ corresponding to $\left(\frac{1}{22}, \frac{1}{17}\right)$ in Fig. 4.2 at $q = 1$.

Therefore, the variation of the 2-LRS pseudo-order of digital image $I(q)$ reveals not only the evolution of the complexity of the image but also the geometrical orientation of the evolving pattern.

4.3.1.2. LRS Pseudo Order and Image Correlation

Shannon entropy is a general measure of image randomness; thus, it cannot be used to measure randomness horizontally (along the rows) or vertically (along the

columns) in a given image. To perform measurements of randomness in horizontal and vertical directions, we use correlation, one of the Haralick's features derived from co-occurrence matrices (Haralick, 1979):

$$\rho_{H(X)} := \frac{1}{\sigma_x \sigma_y} \left(\sum_{i=1}^{N_g} \sum_{j=1}^{N_g} (ij) p(i, j) - \mu_x \mu_y \right), \quad (82)$$

where N_g is the number of gray levels in image X ; $p(i, j)$ is the entry of the co-occurrence matrix (the probability that the pixel with gray level i is adjacent to the pixel with gray level j); μ_x , σ_x , μ_y , σ_y are the means and standard deviations of the partial probability density functions of the co-occurrence matrices.

The horizontal and vertical adjacency is used to compute two correlations for each image by using Eq. (82); the correlation computed while using horizontal and vertical adjacency is referred to as row and column correlations, respectively.

A comparison of row and column LRS pseudo orders and correlations of the image sequence of bricks (Fig. 4.1) is pictured in Fig. 4.3. As q varies from 0 to 1, both row and column correlations increase – while row and column orders decrease monotonically. As it has been noted previously, the periodicity of the image sequence of bricks in Fig. 4.1 is not equal along the rows and columns. This effect can be explained because the period is longer along the rows. Thus the LRS pseudo order of rows is larger if compared with the pseudo order of columns. The LRS pseudo order for rows and columns is 22 and 17 respectively at $q = 1$. A similar effect is observed with respect to the Haralick's feature of correlation – row correlation is higher than column correlation because more adjacent pixels are of the same gray level. Row correlation is almost equal to 1 when $q > 0.9$ and column correlation is 0.82 in the same range.

This computational experiment demonstrates that LRS pseudo-orders do represent the evolution of complexity in the digital images along the horizontal and vertical axes.

4.4. 2D Sequence Pseudo-Order of Self-Organizing Patterns

We shall use the Beddington-de-Angelis-type predator-prey model with self- and cross-diffusion (Saunoriene *et al.*, 2011, Wang *et al.*, 2011):

$$\frac{\partial N}{\partial t} = r \left(1 - \frac{N}{K} \right) - \frac{\beta N}{B + N + \omega P} P + D_{11} \nabla^2 N + D_{12} \nabla^2 P, \quad (83)$$

$$\frac{\partial P}{\partial t} = \frac{\epsilon \beta N}{B + N + \omega P} P - \eta P + D_{21} \nabla^2 N + D_{22} \nabla^2 P, \quad (84)$$

where t is time; N and P are the densities of preys and predators; β is a maximum consumption rate; B is a saturation constant; w is a predator interference parameter; η represents the per capita predator death rate; and ϵ is the conversion efficiency of food into offspring. Nonzero initial conditions $N(x, y, 0) > 0$; $P(x, y, 0) > 0$ are set in a rectangular domain with periodic boundary conditions. The following set $D_{11} = 0.01$, $D_{12} = 0.0115$, $D_{21} = 0.01$, $D_{22} = 1$, $r = 0.5$, $\epsilon = 1$, $\beta = 0.6$, $K = 2.6$, $w = 0.4$, $B =$

0.3154 results in the evolution of a self-organizing pattern from the equilibrium point $(N^*, P^*) = (0.430580, 0.718555)$ which is perturbed by small random perturbation (Saunoriene *et al.*, 2011). The computational reconstruction of the evolution of a self-organizing pattern of preys from random initial conditions is illustrated in Fig. 4.4.

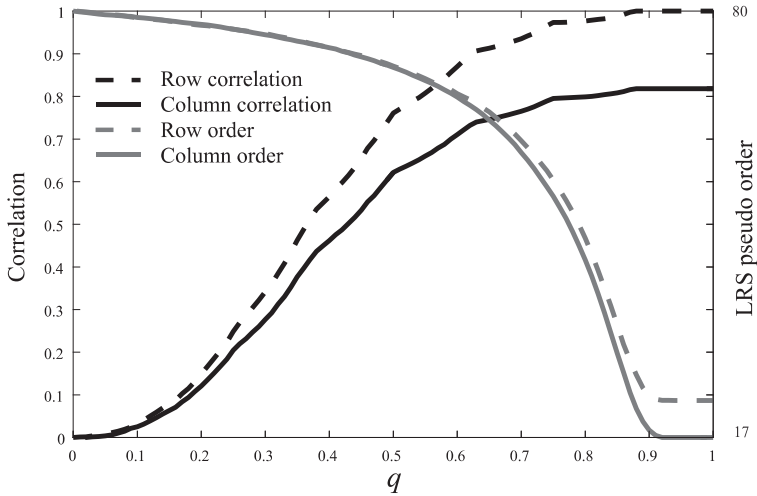


Fig. 4.3. Evolution of row/column correlation and row/column LRS pseudo-order as parameter q varies from 0 to 1. The left y -axis represents the row/column correlations $\rho_H(X)$. The right y -axis represents the row/column LRS-pseudo-order.

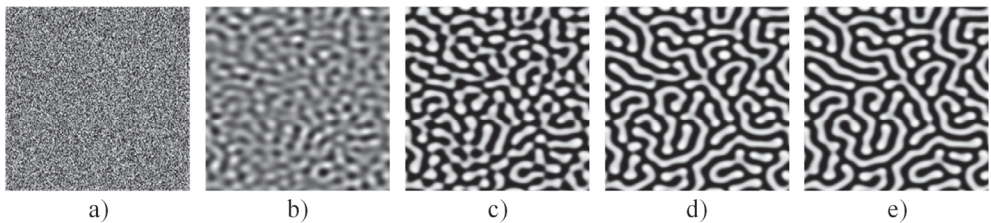


Fig. 4.4. The evolution of self-organizing Beddington-DeAngelis type patterns. Digital images in parts a)-e) are shown at 0, 15000, 25000, 50000 and 70000 time forward steps accordingly.

We repeat the computational experiments with a sequence of images representing the evolution of self-organizing patterns (Fig. 4.5) with ε set to 0.5. Now, the evolution of the entropy is very complex and nonmonotonous (Fig. 4.5). However, the computation of 2-LRS pseudo-orders reveals the hidden rules of the complexity variation during the evolution of the self-organizing pattern.

Initially, the image is random – so 2-LRS pseudo-order for the image of noise is equal to (80, 80) (Fig. 4.5). Then, the self-organizing pattern starts to evolve, and the complexity of the image decreases – 2-LRS pseudo-order is equal to (16.6, 13.7) at $t = 15000$ (the time step of time forward iteration is 0.01). However, the complexity of the image suddenly starts to increase again at $15000 \leq t \leq 25000$. Astonishingly, the complexity of the fully developed pattern is higher compared to

the complexity of pattern in the middle stage of development (2-LRS pseudo-order is equal to (24.2, 21.2) at $t = 70000$).

Such an effect can be explained by a rather simple (though not trivial) consideration. The fully developed pattern is not a regular pattern. The distribution of stripes (and the shapes of stripes) in the fully developed image are governed by a large scale spatial chaos law. We should note that this pattern is unique for every initial condition – different random initial conditions result in different patterns of stripes.

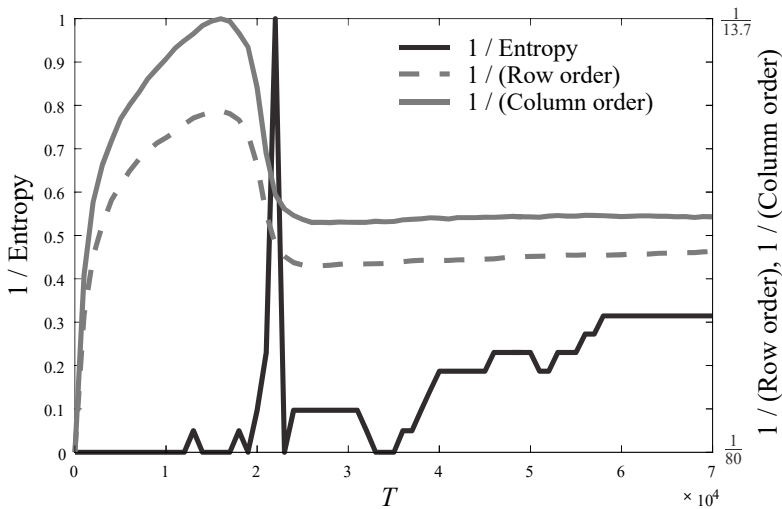


Fig. 4.5. Evolution of entropy and row/column LRS pseudo-order of the Beddington-DeAngelis type self-organizing pattern for 70000 time-forward steps. The left y-axis represents the inverse of entropy $H(X)$. The right y-axis represents the inverse of the average row and column LRS-pseudo-order.

The initial random conditions could be considered as small scale spatial chaos in that respect. However, it is interesting to observe that the evolution from small scale spatial chaos to large scale spatial chaos is not straightforward. First, random initial conditions evolve into a seemingly regular pattern of spatial waves. However, Turing instability (Murray, 2013) deforms these almost regular waves into a complex irregular pattern of large scale stripes. 2-LRS pseudo-orders allow efficient and clear visualization of these complex processes of transformation.

Nonmonotonous effects are observed in the evolution of the row and column correlation (Fig. 4.6). Both row and column correlations reach a peak value of almost 1 at $t = 20000$. After this peak, both correlations dip slightly but do not fluctuate: they maintain values above 0.98 in the interval $20000 < t \leq 70000$. We should note that the values of row and column correlations do not differ significantly one from another during the evolution of the image. This situation is completely different for row and column pseudo orders – they do separate one from another. This feature enables to draw conclusions about the complexity of the digital image in the horizontal and vertical directions.

Moreover, 2-LRS pseudo-orders exemplify the orientation of stripes in

self-organized patterns. The bricks are elongated along the horizontal axis in Fig. 4.1. Thus the period along the rows is longer, and the mean LRS-order of the rows is larger compared to the columns (Fig. 4.2). The same effect can be observed for self-organizing patterns (Fig. 4.4). Figures 4.5 and 4.6 demonstrate that the mean row LRS-order is larger compared to the mean column LRS-order. This implies that the pseudo-period along the rows in Fig. 4.4 is longer compared to the columns.

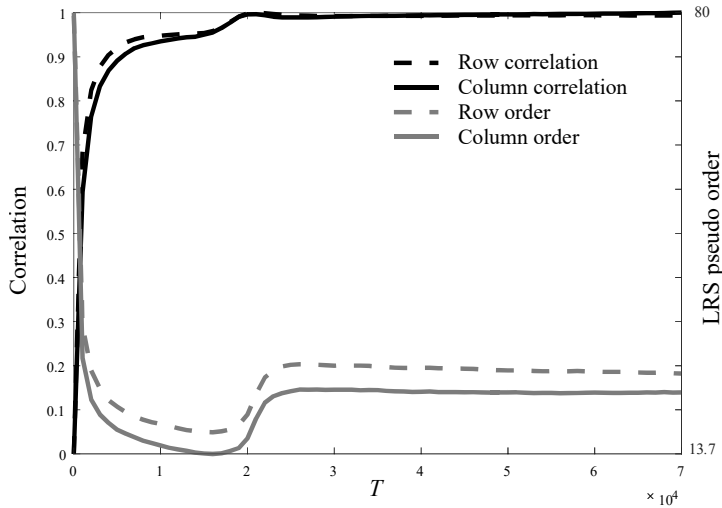


Fig. 4.6. Evolution of row/column correlation and row/column LRS pseudo-order of the Beddington-DeAngelis type self-organizing pattern for 70000 time-forward steps. The left y-axis represents the row/column correlations $\rho_H(X)$. The right y-axis represents the average row/column LRS-pseudo-order.

4.5. Optimal Time Period of Pattern Formation¹³

Let us employ 2-LRS pseudo orders to estimate the complexity of the self-organizing patterns based on the spiral waves model presented in Section 1.2.4. The initial conditions and parameters for the pattern formation are set the same as in Fig. 1.10, except that the domain size is increased to $L = 200$, and ε , which is required to define the pseudo order of the row (column), is set to 0.5. The pattern evolution and the corresponding order are shown in Fig. 4.7.

A pattern warm-up period continues till $T = 25$, when the column order is decreasing because of the vertical initial conditions. After the wave caused by the initial conditions propagates away, the order of both the row and the column starts increasing. Between $T = 60$ and 80, there is a short stable period induced by wave reflection from the boundaries of the pattern followed by the second increase interval when the brakeage all over the domain starts forming. Since $T = 120$, the

¹³ The results presented in this section have been published as:

formation of the pattern is almost complete, but the order is still slowly increasing; and, finally, at $T = 140$, the pattern is complete. The subsequent interactions of the waves do not increase the complexity of the pattern, thus $T = 140$ is the optimal time-period required to prepare the pattern. Similar pattern complexity with respect to each spatial coordinate guarantees no horizontal or vertical directionality.

The 2-LRS based pattern complexity estimation can help finding an optimal pattern computational time-period. The optimal time-period $T = 140$ is close to the one used in Section 2.3.3 where $T = 145$ was selected upon visually inspecting many patterns. A 2-LRS estimator can eliminate the need for human inspection of the pattern and even make the pattern evolution shorter (Vaidelys *et al.*, 2017a).

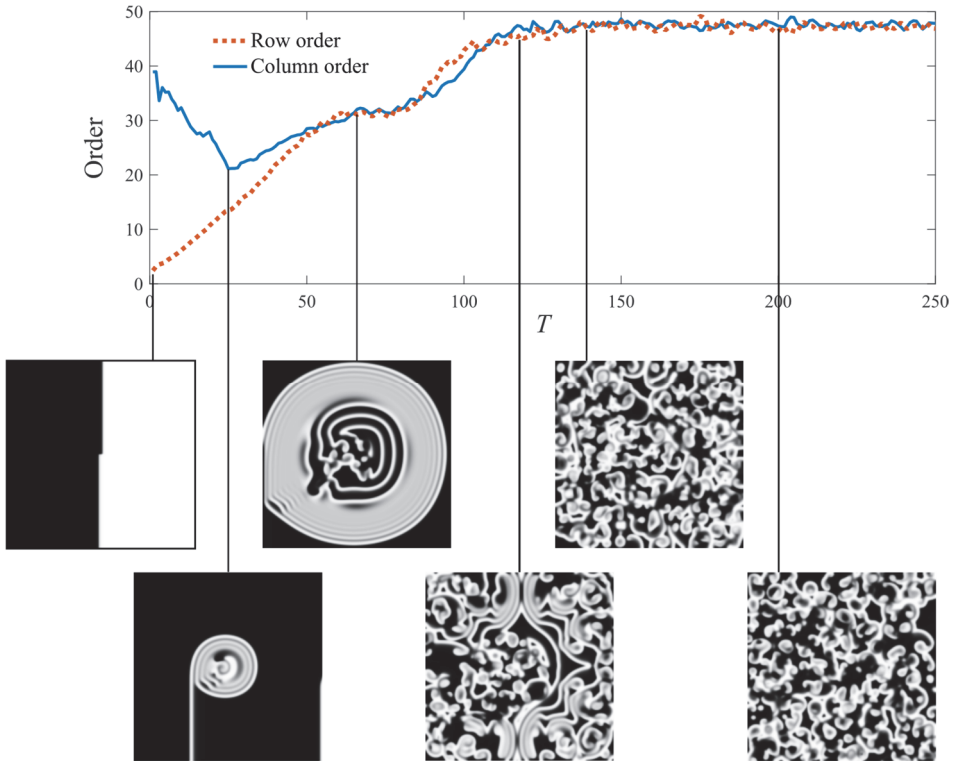


Fig. 4.7. The complexity of an evolving pattern in time.
Maximum pattern complexity is reached at $T = 140$.

4.6. Concluding Remarks

The practical application of the order of a 2D sequence is presented in this section. It has been demonstrated that, while using the SVD, the concept of 2-LRS can be successfully applied for the analysis of image complexity. Because of the ability to measure complexity along the x and y axes, the row and the column 2-LRS pseudo-orders provide a deeper insight into the complexity of images compared with Shannon entropy.

2-LRS can also be used to analyze self-organizing patterns. It is shown that, unlike Shannon entropy, 2-LRS pseudo-order can be applied to detect the formation

of almost regular patterns which evolve from small scale spatial chaos and deform due to Turing instability as time moves forward and large scale spatial chaos appears. This advantage can be used to determine the optimal timing for the perfect pattern formation.

5. CONCLUSIONS

1. It was demonstrated that self-organizing patterns can be used to conceal secret images and enable a secure communication scheme. Three communication schemes based on competitively and non-diffusively coupled nonlinear maps, an atrial fibrillation model and breaking spiral waves were developed, which helped overcome most of the drawbacks observed in previous implementations.

2. The scheme based on breaking spiral waves proved to feature additional advantages. Firstly, no keys (private or public) which would determine the generation of the initial random conditions are required; secondly, it appears that perturbation, which is made in the middle of the pattern formation process, is sensitive to the geometrical locations of the traveling fronts of the breakup waves. To control the pattern formation, an adaptive perturbation technique is required, which adds a novel and additional security level. Despite the required adaptive perturbation procedure, the decoding of the secret image remains as simple and straightforward as before.

3. An image encoding scheme in deformable one-dimensional harmonic moiré gratings oscillating according to a predefined Eigen-mode is developed and implemented for the construction of two-dimensional digital dichotomous secret images. The secret is leaked from the cover image when it is oscillated according to a predefined Eigen-mode in a form of a pattern of time-averaged moiré fringes.

4. The main problem pertaining to the scheme is the formation of a moiré grating with a harmonic variation of grayscale levels on the surface of a deformable structure, which becomes a challenging technological problem in practical applications. Thus the formation of cover images based on Ronchi-type moiré grating is introduced. The resulting image communication scheme mimics the physical processes and could be implemented, e.g., in the optical control of MOEMS (micro-opto-electro-mechanical systems).

5. It was demonstrated that, by using the SVD, the concept of 2-LRS can be successfully applied for the analysis of the image as well as self-organizing pattern complexity. Because of the ability to measure the complexity along the x - and y -axis, the row and column 2-LRS pseudo-orders provide a deeper insight into the complexity of images compared with Shannon entropy. Unlike Shannon entropy or row/column correlation, 2-LRS pseudo-order can be applied to detect the formation of almost regular patterns that evolve from small scale spatial chaos and deform due to Turing instability as time moves forward when large scale spatial chaos appears, which is an important criterion of the pattern formation when seeking to ensure the creation of a steganographically secure pattern.

REFERENCES

1. ALTAAY, A.A.J., *et al.* (2012). An Introduction to Image Steganography Techniques. In: *International Conference on Advanced Computer Science Applications and Technologies (ACSAT)*. 2012, 122–126. ISSN 2379-7738.
2. AVERILL, B., ELDRIDGE, P. (2011). *General Chemistry: Principles, Patterns, and Applications*. Saylor Academy. ISBN 9781453322307.
3. BALL, P. (1994). *Designing the Molecular World: Chemistry at the Frontier*. Princeton University Press. 384pp. ISBN 9780691029009.
4. BÄR, M., EISWIRTH, M. (1993). Turbulence due to Spiral Breakup in a Continuous Excitable Medium. In: *Physical Review E*. 1993, 48, 1635–1637. ISSN 2470-0045.
5. BARKLEY, D. (2008). Barkley Model. (2008). In: *Scholarpedia*. 2008, 3(11), 1877. ISSN 1941-6016.
6. BARKLEY, D., KNESS, M., TUCKERMAN, L.S. (1990). Spiral-Wave Dynamics in a Simple Model of Excitable Media: the Transition from Simple to Compound Rotation. In: *Physical Review A*. 1990, 42, 2489–2492. ISSN 2469-9926.
7. BEIM GRABEN, P., SELLERS, K.K., FROHLICH, F., HUTT, A. (2016). Optimal Estimation of Recurrence Structures from Time Series. In: *Europhysics Letters*. 2016, 114, 38003. ISSN 0295-5075.
8. BOLLIGER, J., *et al.* (2013). Self-Organization and Complexity in Historical Landscape Patterns. In: *Oikos*. 2013, 100(3), 541–553. ISSN 0030-1299.
9. BORDA, M. (2011). *Fundamentals in Information Theory and Coding*. Berlin, Heidelberg: Springer-Verlag. 485pp. ISBN 9783642203466.
10. CACHIN, C. (2004). An Information-Theoretic Model for Steganography. In: *Information and Computation*. 2004, 192(1), 41–56. ISSN 0890-5401.
11. CHANDRA, S., *et al.* (2014). A Comparative Survey of Symmetric and Asymmetric Key Cryptography. In: *International Conference on Electronics, Communication and Computational Engineering (ICECCE)*. 2014, 83–93. ISBN 9781479957484.
12. CHEDDAD, A., *et al.* Digital Image Steganography: Survey and Analysis of Current Methods. In: *Signal Processing*. 2010, 90(3), 727–752. ISSN 0165-1684.
13. CHEN, Y.-C., *et al.* (2012). A New Authentication Based Cheating Prevention Scheme in Naorshamirs Visual Cryptography. In: *Journal of Visual Communication and Image Representation*. 2012, 23(8), 1225–1233. ISSN 1047-3203.
14. CHEN, Y.Y., *et al.* (2017). Design of Image Barcodes for Future Mobile Advertising. In: *EURASIP Journal on Image and Video Processing*. 2017, 2017(11). ISSN 1687-5281.
15. CHERRY, E.M., *et al.* (2008). Visualization of Spiral and Scroll Waves in Simulated and Experimental Cardiac Tissue. In: *New Journal of Physics*. 2008, 10, 125016. ISSN 1367-2630.
16. CHRISTENSEN, K., MANANI, K.A., PETERS, N.S. (2015). Simple Model for Identifying Critical Regions in Atrial Fibrillation. In: *Physical Review Letters*. 2015, 114, 028104. ISSN 0031-9007.
17. CLAYTON, R.H. (2001). Computational Models of Normal and Abnormal Action Potential Propagation in Cardiac Tissue: Linking Experimental and Clinical Cardiology. In: *Physiological Measurement*. 2001, 22, 15–34. ISSN 0967-3334.

18. CLAYTON, R., BERNUS, O., CHERRY, E., DIERCKX, H., FENTON, F., MIRABELLA, L., PANFILOV, A., SACHSE, F., SEEMANN, G., ZHANG, H. (2011). Models of Cardiac Tissue Electrophysiology: Progress, Challenges and Open Questions. In: *Progress in Biophysics and Molecular Biology*. 2011, 104, 22–48. ISSN 0079-6107.
19. DAHAT, A.V., *et al.* (2016). Secret Sharing Based Visual Cryptography Scheme Using cmy Color Space. In: *1st International Conference on Information Security and Privacy*. 2016, 78, 563–570. ISSN 1877-0509.
20. DAS, P.K., *et al.* (2014). Image Cryptography: a Survey towards its Growth. In: *Advance in Electronic and Electric Engineering*. 2014, 4(2), 179–184. ISSN 2231-1297.
21. DIAZ-MENDEZ, A., MARQUINA-PEREZ, J., CRUZ-IRISSON, M., VAZQUEZ-MEDINA, R., DEL-RIO-CORREA, J.L. (2009). Chaotic Noise MOS Generator Based On Logistic Map. In: *Microelectronics Journal*. 2009, 40, 638–640. ISSN 0026-2692.
22. DOWLE, M., MANTEL, R.M., BARKLEY, D. (1997). Fast Simulations of Waves in Three-Dimensional Excitable Media. In: *International Journal of Bifurcation and Chaos*. 1997, 7, 2529–2546. ISSN 0218-1274.
23. EVEREST, G., VAN DER POORTEN, A., SHPARLINSKI, I.E., WARD, T., *et al.* (2003). *Recurrence Sequences*. American Mathematical Society Providence. 2003, 104, 318pp. ISBN 9781470423155.
24. FENG BINGWEN, *et al.* (2017). Steganalysis of Content-Adaptive Binary Image Data Hiding. In: *Journal of Visual Communication and Image Representation*. 2017, 46, 119–127. ISSN 1047-3203.
25. FIELD, R.J., NOYES, R.M. (1974). Oscillations in Chemical Systems. IV. Limit Cycle Behavior in a Model of a Real Chemical Reaction. In: *The Journal of Chemical Physics*, 1974, 60, 1877. ISSN 0021-9606.
26. FRIDRICH, J., GOLJAN, M., DU, R. (2001). Reliable Detection of LSB Steganography in Color and Grayscale Images. In: *Proceedings of the 2001 Workshop on Multimedia and Security, New Challenges*. 2001, 27–30. ISBN 1581133936.
27. GARZIA, F. (2013). *Handbook of Communications Security*. WIT Press. 2013, 680. ISBN 9781845647681.
28. GRINDROD, P. (1996). *The Theory and Applications of Reaction-Diffusion Equations: Patterns and Waves*. Clarendon Press. 1996, 285pp. ISBN 9780198500049.
29. GUPTA, T., *et al.* (2015). Review and Classification of Cryptography. In: *International Journal of Advanced Technology in Engineering and Science*. 2015, 3(12), 38–41. ISSN 2348-7550.
30. GURUNG, S., *et al.* (2015). Multiple Information Hiding Using Circular Random Grids. In: *International Conference on Computer, Communication and Convergence*. 2015, 48, 65–72. ISSN 1877-0509.
31. HAN, Y.Y., *et al.* (2015). Multi-Secret Sharing Visual Cryptography Based on Random Grids. In: *International Conference on Information Science and Intelligent Control*. 2015, 612–617. ISBN 9781605952956.
32. HARALICK, R.M. (1979). Statistical and Structural Approaches to Texture. In: *Proceedings of the IEEE*. 1979, 67, 786–804. ISSN 0018-9219.

33. HUANG, L., *et al.* (2012). The Study on Data Hiding in Medical Images. In: *International Journal of Network Security*. 2012, 14(6) 301–309. ISSN 1816-353X.
34. ISHIMURA, K., KOMURO, K., SCHMID, A., ASAI, T., MOTOMURA, M. (2014). Image Steganography Based on Reaction Diffusion Models Toward Hardware Implementation. In: *Nonlinear Theory and Its Applications, IEICE*. 2014, 5(4), 456–465. ISSN 2185-4106.
35. JANSEN, V.A., LLOYD, A.L. (2000). Local Stability Analysis of Spatially Homogeneous Solutions of Multi-Patch Systems. In: *Journal of Mathematical Biology*. 2000, 41(3), 232–252. ISSN 0303-6812.
36. JOHNSON, N., DURIC, Z., JAJODIA, S. (2012). *Information Hiding: Steganography and Watermarking – Attacks and Countermeasures: Steganography and Watermarking*. Springer Science and Business Media. 2012, 137pp. ISBN 978-0-7923-7204-2.
37. JOSHI, K., *et al.* (2015). A New LSB-S Image Steganography Method Blend with Cryptography for Secret Communication. *3rd International Conference on Image Information Processing (ICIIP)*. 2015, 86–90. ISBN 9781509001484.
38. JUANG, J.-N., PAPPA, R.S. (1985). An Eigensystem Realization Algorithm for Modal Parameter Identification and Model Reduction. In: *Journal of Guidance, Control, and Dynamics*. 1985, 8, 620–627. ISSN 0731-5090.
39. KAUR, S., *et al.* (2014). Steganography and Classification of Image Steganography Techniques. In: *International Conference on Computing for Sustainable Global Development (Indiacom)*. 2014, 870–875.
40. KILLINGBACK, T., LOFTUS, G., SUNDARAM, B. (2013). Competitively Coupled Maps and Spatial Pattern Formation. In: *Physical Review E*. 2013, 87(2), 022902. ISSN 2470-0045.
41. KLEIN, A., *et al.* (2017). Simple Mechanisms of Early Life – Simulation Model on the Origin of Semi-Cells. In: *Biosystems*. 2017, 151, 34–42. ISSN 0303-2647.
42. KOBAYASHI, A. (1993). *Handbook on Experimental Mechanics*. 2nd Ed. Bethel, SEM. 1993, 1074. ISBN 9781560816409.
43. KURAKIN, V., KUZMIN, A., MIKHALEV, A., NECHAEV, A. (1995). Linear Recurring Sequences over Rings and Modules. In: *Journal of Mathematical Sciences*. 1995, 76, 2793–2915. ISSN 1072-3374.
44. LANDAUSKAS M., NAVICKAS Z., VAINORAS A., RAGULSKIS M. (2016). Weighted moving aver-aging revisited: an algebraic approach. *Computational and Applied Mathematics*. 2016, 1–14. ISSN 0101-8205.
45. LANDAUSKAS, M., RAGULSKIS, M. (2014). A Pseudo-Stable Structure in a Completely Invertible Bouncer System. In: *Nonlinear Dynamics*. 2014, 78, 1629–1643. ISSN 0924-090X.
46. LANDAUSKAS, M., RAGULSKIS, M. (2003). Clocking Convergence to Arnold Tongues – the H-rank Approach. In: *AIP Conference Proceedings*. 2013, 1558, 2457–2460. ISSN 0094-243X.
47. LI, P.P., *et al.* (2012). Cooperative Behavior in Evolutionary Snowdrift Games with the Unconditional Imitation Rule on Regular Lattices. In: *Physical Review E*. 2012, 85(2), 021111. ISSN 2470-0045.

48. LING, J., *et al.* (2011). Information Hiding Algorithm Based on Stentiford Visual Attention Model. In: *7th International Conference on Computational Intelligence and Security*, 2011, 564–567.
49. LIU, J., *et al.* (2013). A Secure Steganography for Privacy Protection in Healthcare System. In: *Journal of Medical Systems*. 2013, 37(2), 9918. ISSN 0148-5598.
50. LU, P., LIU, M., OBERST, U. (2004). Linear Recurring Arrays, Linear Systems and Multidimensional Cyclic Codes over Quasi-Frobenius Rings. In: *Acta Applicandae Mathematicae*. 2004, 80, 175–198. ISSN 0167-8019.
51. LUKE, R.A., SAFFITZ, J.E. (1991). Remodeling of Ventricular Conduction Pathways in Healed Canine Infarct Border Zones. In: *The Journal of Clinical Investigation*. 1991, 87, 1594–1602. ISSN 0021-9738.
52. MAQSOOD FAIQA, *et al.* (2017). Cryptography: a Comparative Analysis for Modern Techniques. In: *International Journal of Advanced Computer Science and Applications*. 2017, 8(6), 442–448. ISSN 2158-107X.
53. MARCELLA, A., MENENDEZ, D. (2007). *Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes*. Second Edition. CRC Press. 2007, 528pp. ISBN 9780849383281.
54. MARWAN, N., ROMANO, M.C., THIEL, M., KURTHS, J. (2007). Recurrence Plots for the Analysis of Complex Systems. In: *Physics Reports*. 2007, 438, 237–329. ISSN 0370-1573.
55. MIKHALEV, A., NECHAEV, A. (1996). Linear Recurring Sequences over Modules. In: *Acta Applicandae Mathematicae*. 1996, 42, 161–202. ISSN 0167-8019.
56. MISHRA, R., *et al.* (2015). A Review on Steganography and Cryptography. In: *International Conference on Advances in Computer Engineering and Applications (ICACEA)*. 2015, 119–122. ISBN 978-1-4673-6911-4.
57. MITALI, *et al.* (2014). A Survey on Various Cryptography Techniques. In: *International Journal of Emerging Trends and Technology in Computer Science (IJETTCS)*. 2014, 3(4), 307–312. ISSN 2278-6856.
58. MOIZUDDIN, M., *et al.* (2017). A Comprehensive Survey: Quantum Cryptography. *2nd International Conference on Anti-Cyber Crimes (ICACC)*. 2017, 98–102. ISBN 9781509058150.
59. MOHAN, A., *et al.* (2016). Quality Improvement in Color Extended Visual Cryptography Using ABM and PRWP. In: *Proceedings of 2016 International Conference on Data Mining and Advanced Computing (Sapience)*. 2016, 273–278. ISBN 9781467385947.
60. MOORE, T., *et al.* (2014). Self-Organizing Actomyosin Patterns on the Cell Cortex at Epithelial Cell-Cell Junctions. In: *Biophysical Journal*. 2014, 107(11), 2652–2661. ISSN 0006-3495.
61. MUHAMMAD, K., *et al.* (2017). CISSKA-LSB: Color Image Steganography Using Stego Key-Directed Adaptive LSB Substitution Method. In: *Multimedia Tools and Applications*. 2017, 76(6), 8597–8626. ISSN 1380-7501.
62. MUKUNDAN, P.M., *et al.* (2016). Hash-One: a Lightweight Cryptographic Hash Function. In: *IET Information Security*. 2016, 10(5), 225–231. ISSN 1751-8709.
63. MURRAY, J.D. (2013). *Mathematical Biology*. Springer Science and Business Media. 2013, 770pp. ISBN 9783662085424.

64. NAGARAJA ARUN, *et al.* (2016). Privacy Preserving and Data Security – a Survey. In: *International Conference on Engineering & MIS (ICEMIS)*. ISBN 9781509055791.
65. NAGATANI, T. (2008). Vehicular Motion through a Sequence of Traffic Lights Controlled by Logistic Map. In: *Physics Letters A*. 2008, 372, 5887–5890. ISSN 0375-9601.
66. NAKAMURA, K., FUNABASHI, N., UEHARA, M., UEDA, M., MURAYAMA, T., TAKAOKA, H., KOMURO, I. (2011). Left Atrial Wall Thickness in Paroxysmal Atrial Fibrillation by Multislice-CT Is Initial Marker of Structural Remodeling and Predictor of Transition from Paroxysmal to Chronic Form. In: *International Journal of Cardiology*. 2011, 148, 139–147. ISSN 0167-5273.
67. NANDAKUMAR, A., *et al.* (2011). A Secure Data Hiding Scheme Based on Combined Steganography and Visual Cryptography Methods. In: *Advances in Computing and Communications, Part 2*. 2011, 191, 498–505. ISSN 1865-0929.
68. NAOR, M., SHAMIR, A. (1994). Visual Cryptography. In: *Advances in Cryptology – EUROCRYPT'94*. 1994, 1–12. ISSN 0302-9743.
69. NAVICKAS, Z., BIKULCIENE, L., RAHULA, M., RAGULSKIS, M. (2013). Algebraic Operator Method for the Construction of Solitary Solutions to Nonlinear Differential Equations. In: *Communications in Nonlinear Science and Numerical Simulation*. 2013, 18, 1374–1389. ISSN 1007-5704.
70. NIVEDITHA, R. (2014). A Survey on Cryptography and Steganography. In: *International Journal of Science and Research (IJSR)*. 2014, 3(4), 398–402. ISSN 2319-7064.
71. NOBI, M.N., CHOWDHURY, F., *et al.* (2011). A New Medical Image Segmentation Technique Based on Variational Level Set Method. (2011). *International Journal of Computer and Electrical Engineering*. 2011, 3(5), 690–694. 158. ISSN 1793-8163.
72. ODAT, A.M., *et al.* (2016). Image Steganography Using Modified Least Significant Bit. In: *Indian Journal of Science and Technology*. 2016, 9(39). ISSN 0974-6846.
73. PALIVONAITE, R., ALEKSA, A., PAUNKSNIS, A., GELZINIS, A., RAGULSKIS, M. (2014). Image Hiding in Time-Averaged Deformable Moiré Gratings. In: *Journal of Optics*. 2014, 16(2), 025401. ISSN 2040-8986.
74. PANDEY, A., *et al.* (2016). Applications and Usage of Visual Cryptography: a Review. In: *5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*. 2016, 375–381. ISSN 2469-875X.
75. PARAH, S.A., *et al.* (2012). High Capacity Data Embedding Using Joint Intermediate Significant Bit (ISB) and Least Significant Bit (LSB) Technique. In: *Journal of Information Engineering and Applications*. 2012, 2(11), 1–11. ISSN 2224-5782.
76. PATIDAR, V., PAREEK, N., SUD, K. (2009). A New Substitution-Diffusion Based Image Cipher Using Chaotic Standard and Logistic Maps. In: *Communications in Nonlinear Science and Numerical Simulation*. 2009, 14, 3056–3075. ISSN 1007-5704.
77. PETRAUSKIENE, V., *et al.* (2014). Dynamic Visual Cryptography Based on Chaotic Oscillations. In: *Communications in Nonlinear Science and Numerical Simulation*. 2014, 19(1), 112–120. ISSN 1007-5704.
78. PRIGOGINE, I., NICOLIS, G. (1977). *Self-Organisation in Non-Equilibrium Chemical Systems*. Wiley and Sons. ISBN 97894009623921.

79. PRUNESCU, M. (2011). Linear Recurrent Double Sequences with Constant Border in $M_2(F_2)$ Are Classified according to Their Geometric Content. In: *Symmetry*. 2011, 3, 402–442. ISSN 2073-8994.
80. PRUNESCU, M. (2010). Recurrent Double Sequences that Can Be Produced by Context-Free Substitutions. In: *Fractals*. 2010, 18, 65–73. ISSN 0218-348X.
81. PRUNESCU, M. (2011). Recurrent Two-Dimensional Sequences Generated by Homomorphisms of finite Abelian p -groups with Periodic Initial Conditions. In: *Fractals*. 2011, 19, 431–442. ISSN 0218-348X.
82. RAD, A.E., *et al.* (2014). Level Set and Morphological Operation Techniques in Application of Dental Image Segmentation. In: *International Journal of Medical, Health, Biomedical, Bioengineering and Pharmaceutical Engineering*. 2014, 8(4) 182–185. ISSN 2010-376X.
83. RAFAT, K.F., *et al.* (2016). Secure Steganography for Digital Images. In: *International Journal of Advanced Computer Science and Applications (IJACSA)*. 2016, 7(6), 45–59. ISSN 2156-5570.
84. RAGULSKIS, M., ALEKSA, A. (2009). Image Hiding Based on Time-Averaging Moiré. In: *Optics Communications*. 2009, 282(14), 2752–2759. ISSN 0030-4018.
85. RAGULSKIS, M., ALEKSA, A., MASKELIUNAS, R. (2009). Contrast Enhancement of Time-Averaged Fringes Based on Moving Average Mapping Functions. In: *Optics and Lasers in Engineering*. 2009, 47(7–8), 768–773. ISSN 0143-8166.
86. RAGULSKIS, M., ALEKSA, A., NAVICKAS, Z. (2009). Image Hiding Based on Time-Averaged Fringes Produced by Non-Harmonic Oscillations. In: *Journal of Optics A: Pure and Applied Optics*. 2009, 11(12), 125411. ISSN 1741-3567.
87. RAGULSKIS, M., LUKOSEVICIUTE, K., NAVICKAS, Z., PALIVONAITI, R. (2011). Short-Term Time Series Forecasting Based on the Identification of Skeleton Algebraic Sequences. In: *Neurocomputing*. 2011, 74, 1735–1747. ISSN 0925-2312.
88. RAGULSKIS, M., NAVICKAS, Z. (2011). The Rank of a Sequence as an Indicator of Chaos in Discrete Nonlinear Dynamical Systems. In: *Communications in Nonlinear Science and Numerical Simulation*. 2011, 16, 2894–2903. ISSN 1007-5704.
89. RAGULSKIS, M., SAUNORIENE, L. (2006). Applicability of Optical Geometric Differentiation for Time-Average Geometric Moiré. In: *Strain*. 2006, 42(3), 173–179. ISSN 1475-1305.
90. RAZZAQ, M.A., *et al.* (2017). Digital Image Security: Fusion of Encryption, Steganography and Watermarking. In: *International Journal of Advanced Computer Science and Applications*. 2017, 8(5), 224–228. ISSN 2158-107X.
91. ROGORA, M., *et al.* (2016). Temporal and Spatial Patterns in the Chemistry of Wet Deposition in Southern Alps. In: *Atmospheric Environment*. 2016, 146, 44–54. ISSN 1352-2310.
92. ROHANI, P., MAY, R.M., HASSELL, M.P. (1996). Metapopulation and Equilibrium Stability: The Effects of Spatial Structure. In: *Journal of Theoretical Biology*. 1996, 181(2), 97–109. ISSN 0022-5193.
93. ROY, R., CHANGDER, S. (2016). Quality Evaluation of Image Steganography Techniques: a Heuristics Based Approach. In: *International Journal of Security and Its Applications*. 2016, 10(4), 179–196. ISSN 1738-9976.

94. RURA, L., *et al.* (2016). Implementation and Evaluation of Steganography Based Online Voting System. In: *International Journal of Electronic Government Research*. 2016, 12(3), 71–93. ISSN 1548-3886.
95. SADEK, M.M., *et al.* (2017). Robust Video Steganography Algorithm Using Adaptive Skin-Tone Detection. In: *Multimedia Tools and Applications*. 2017, 76(2), 3065–3085. ISSN 1380-7501.
96. SAHARE, K.P., *et al.* (2015). Securing Digital Images Using Visual Cryptography. In: *International Journal of Emerging Trends in Science and Technology*. 2015, 2(12) 3410–3414. ISSN 2348-9480.
97. SAHIN, U., UGUZ, S., AKN, H., SIAP, I. (2015). Three-State von Neumann Cellular Automata and Pattern Generation. In: *Applied Mathematical Modelling*. 2015, 39(7) 2003–2024. ISSN 0307-904X.
98. SARGENT, T.J. (2009). *Dynamic Macroeconomic Theory*. Harvard University Press.
99. SAUNORIENE, L., RAGULSKIS, M. (2011). Secure Steganographic Communication Algorithm Based on Self-Organizing Patterns. In: *Physical Review E*. 2011, 84, 0562
100. SEDGEWICK, R., FLAJOLET, P. (2013). *An Introduction to the Analysis of Algorithms*. Addison-Wesley. ISBN 9780321905758.
101. SHERWOOD, W.E. (2014). *FitzHugh-Nagumo model*. *Encyclopedia of Computational Neuroscience*. New York: Springer. 2014, 1–11. ISBN 9781461473206.
102. SHESHASAYEE, A., *et al.* (2017). A Framework to Enhance Security for OTP SMS in e-Banking Environment Using Cryptography and Text Steganography. In: *Proceedings of the International Conference on Data Engineering and Communication Technology*. 2017, 469, 709–717. ISSN 2194-5357. 113.
103. SIMON, S. (2010). *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. Knopf Doubleday Publishing Group. ISBN 978-0385495325.
104. STROGATZ, S.H. (2014). *Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering*. Westview Press. 2014. ISBN 9780813349107.
105. SUNDARI, M., *et al.* (2015). Secure Communication Using Digital Watermarking with Encrypted Text Hidden in an Image. In: *Security in Computing and Communications*. 2015, 536, 247–255. ISSN 1865-0929.
106. SZALAI, I., *et al.* (2008). Pattern Formation in the Ferrocyanide-Iodate-Sulfite Reaction: the Control of Space Scale Separation. In: *Chaos*. 2008, 18(2), 026105. ISSN 1054-1500.
107. TAHER, F., *et al.* (2016). A New Hybrid Watermarking Algorithm for MRI Medical Images Using DWT and Hash Functions. In: *38th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*. 2016, 1212–1215. ISSN 1557-170X.
108. TAOUIL, Y., *et al.* (2017). New Image Steganography Method Based on Haar Discrete Wavelet Transform. In: *Europe and Mena Cooperation Advances in Information and Communication Technologies*. 2017, 520, 287–297. ISSN 2194-5357.
109. TELKSUNY, T., NAVICKAS, Z., VAIDELYS, M., RAGULSKIS, M. (2016). The Order of a 2-Sequence and the Complexity of Digital Images. In: *Advances in Complex Systems*. 2016, 19, 1650010. ISSN 0219-5259.

110. UBALE, S.A., *et al.* (2017). Developing Secure Cloud Storage System Using Access Control Models. In: *Proceedings of the International Conference on Data Engineering and Communication Technology*. 2017, 469, 141–147. ISSN 2194-5357.
111. UMBAUGH, S.E. (2010). *Digital Image Processing and Analysis: Human and Computer Vision Applications with CVIptools, Second Edition*. CRC Press. 977pp. ISBN 9781138745919.
112. VAIDELYS, M., ALEKSIENĖ, S., RAGULSKIENĖ, J. (2015). Dynamic Visual Cryptography Scheme on the Surface of a Vibrating Structure. In: *Journal of Vibroengineering*. 2015, 17(8), 4142–4152. ISSN 1392-8716.
113. VAIDELYS, M., LU, C., CHENG, Y., RAGULSKIS, M. (2017). Digital Image Communication Scheme Based on the Breakup of Spiral Waves. In: *Physica A: Statistical Mechanics and Its Applications*. 2017, 467, 1–10. ISSN 0378-4371.
114. VAIDELYS, M., LU, C., CHENG, Y., VAIDELIENE, G. (2017). Image Hiding in Dynamic Unstable Self-Organizing Patterns. In: *Vibroengineering Procedia*. 2017, 14, 328–333. ISSN 2345-0533.
115. VAIDELYS, M., RAGULSKIENĖ, J., ALEKSIENĖ, S., RAGULSKIS, M. (2015). Image Hiding in Time-Averaged Moiré Gratings on Finite Element Grids. In: *Applied Mathematical Modelling*. 2015, 39(19), 5783–5790. ISSN 0307-904X.
116. VAIDELYS, M., RAGULSKIENE, J., ZIAUKAS, P., RAGULSKIS, M. (2015). Image Hiding Scheme Based on the Atrial Fibrillation Model. In: *Applied Sciences*. 2015, 5(4), 1980. ISSN 2076-3417.
117. VAIDELYS, M., ZIAUKAS, P., RAGULSKIS, M. (2016). Competitively Coupled Maps for Hiding Secret Visual Information. In: *Physica A: Statistical Mechanics and its Applications*. 2016, 443, 91–97. ISSN 0378-4371.
118. VERHEULE, S., WILSON, E., EVERETT, T., SHANBHAG, S., GOLDEN, C., OLGIN, J. (2003). Alterations in Atrial Electrophysiology and Tissue Structure in a Canine Model of Chronic Atrial Dilatation due to Mitral Regurgitation. In: *Circulation*. 2003, 107, 2615–2622. ISSN 0009-7322.
119. VILLETTE, V., MALCHAVE, A., TRESSARD, T., DUPUY, N., COSSART, R. (2015). Internally Recurring Hippocampal Sequences as a Population Template of Spatiotemporal Information. In: *Neuron*, 2015, 88, 357–366. ISSN 1941-6016.
120. WALLER, I., KAPRAL, R. (1984). Spatial and Temporal Structure in Systems of Coupled Nonlinear Oscillators. In: *Physical Review A*. 1984, 30, 2047–2055. ISSN 2469-9926.
121. WANG, D., *et al.* (2017). Verification of Implementations of Cryptographic Hash Functions. In: *IEEE Access*. 2017, 5, 7816–7825. ISSN 2169-3536.
122. WANG, D.Q., *et al.* (2017). A High Capacity Spatial Domain Data Hiding Scheme for Medical Images. In: *Journal of Signal Processing Systems for Signal Image and Video Technology*. 2017, 87(2), 215–227. ISSN 1939-8018.
123. WANG, R.Y. (2015). Self-Organized Patterns in the SOM Network. In: *11th International Conference on Natural Computation (ICNC)*. 2015, 123–128. ISBN 9781467376792.
124. WANG, W., LIN, Y., ZHANG, L., RAO, F., TAN, Y. (2011). Complex Patterns in a Predator-Prey Model with Self and Cross-Diffusion. In: *Communications in Nonlinear Science and Numerical Simulation*. 2011, 16, 2006–2015. ISSN 1007-5704.

125. WANG, X., LUAN, D. (2013). A Novel Image Encryption Algorithm Using Chaos and Reversible Cellular Automata. In: *Communications in Nonlinear Science and Numerical Simulation*. 2013, 18(11), 3075–3085. ISSN 1007-5704.
126. WEIR, J., *et al.* (2012). *Visual Cryptography and Its Applications*. Ventus Publishing ApS. ISBN 9788740301267.
127. WEISS, C.O., LARIONOVA, Y. (2007). Pattern Formation in Optical Resonators. In: *Reports on Progress in Physics*. 2007, 70(2), 255. ISSN 0034-4885.
128. WINFREE, A.T. (1994). *Puzzles about Excitable Media and Sudden Death*. *Frontiers in Mathematical Biology*. Berlin: Springer. 100, 139–158. ISBN 9783642501265.
129. WOO, S.J., *et al.* (2008). Spiral Wave Drift and Complex-Oscillatory Spiral Waves Caused by Heterogeneities in Two-Dimensional *In Vitro* Cardiac Tissues. In: *New Journal of Physics*. 2008, 10, 015005. ISSN 1367-2630.
130. XIA, Z., *et al.* (2016). A Privacy-Preserving and Copy-Deterrence Content-Based Image Retrieval Scheme in Cloud Computing. In: *IEEE Transactions on Information Forensics and Security*. 2016, 11(11), 2594–2608. ISSN 1556-6013.
131. XIA, Z., *et al.* (2016). Steganalysis of LSB Matching Using Differences between Nonadjacent Pixels. In: *Multimedia Tools and Applications*. 2016, 75(4), 1947–1962. ISSN 1380-7501.
132. XU, A.P., WANG, L.J, FENG, A., QU, Y.X. (2010). Threshold-Based Level Set Method of Image Segmentation. In: *3rd International Conference on Intelligent Networks and Intelligent Systems (ICINIS)*. 2010, 703–706. ISBN 9781424485482.
133. XU, L., *et al.* (2016). Dependence of Initial Value on Pattern Formation for a Logistic Coupled Map Lattice. In: *PLOS ONE*. 2016, 11(7), e0158591. ISSN 1932-6203.
134. YAMASAKI, K., *et al.* (2011). Symmetry and Entropy of Biological Patterns: Discrete Walsh Functions for 2D Image Analysis. In: *Biosystems*. 2011, 103(1), 105–112. ISSN 0303-2647.
135. YANG, F., XU, Y.-Y., SHEN, H.-B. (2014). Many Local Pattern Texture Features: which Is Better for Image-Based Multilabel Human Protein Subcellular Localization Classification? In: *The Scientific World Journal*. 2014, 429049-14. ISSN 2356-6140.
136. YE, G.D., *et al.* (2017). An Efficient Symmetric Image Encryption Algorithm Based on an Intertwining Logistic Map. In: *Neurocomputing*. 2017, 251, 45–53. ISSN 0925-2312.
137. YU, J., *et al.* (2017). Image Encryption Algorithm by Using the Logistic Map and Discrete Fractional Angular Transform. In: *Optica Applicata*. 2017, 47(1), 141–155. ISSN 0078-5466.
138. ZHANG, J.J., *et al.* (2017). Coverless Text Information Hiding Method Using the Frequent Words Hash. In: *International Journal of Network Security*. 2017, 19, 1016–1023. ISSN 1816-353X.
139. ZHENG, Q., SHEN, J. (2015). Dynamics and Pattern Formation in a Cancer Network with Diffusion. In: *Communications in Nonlinear Science and Numerical Simulation*. 2015, 27(13), 93–109. ISSN 1007-5704.
140. ZHOU, X.Y., *et al.* (2016). An Improved Method for LSB Based Color Image Steganography Combined with Cryptography. In: *IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS)*. 2016, 1339–1342. ISBN 9781509008056.

141. ZHOU, Z., *et al.* (2017). Effective and Efficient Global Context Verification for Image Copy Detection. In: *IEEE Transactions on Information Forensics and Security*. 2017, 12(1), 48–63. ISSN 1556-6013.
142. ZIAUKAS, P., RAGULSKIS, T., RAGULSKIS, M. (2014). Communication Scheme Based on Evolutionary Spatial Games. In: *Physica A: Statistical Mechanics and its Applications*. 2014, 403, 177–188. ISSN 0378-4371.
143. ZIELINSKA, E., *et al.* (2014). Trends in Steganography. In: *Communications of the ACM*. 2014, 57(3), 86–95. ISSN 0001-0782.

LIST OF AUTHOR'S PUBLICATIONS

Papers in Master List Journals of the Institute of Scientific Information (ISI):

1. **Vaidelys, Martynas**; Lu, Chen; Cheng, Yujie; Ragulskis, Minvydas Kazys. Digital Image Communication Scheme Based on the Breakup of Spiral Waves // *Physica A: Statistical mechanics and its applications*. Amsterdam: Elsevier. ISSN 0378-4371. 2017, vol. 467, p. [1–10]. [Science Citation Index Expanded (Web of Science); Scopus; Current Contents (Physical, Chemical & Earth Sciences)]. [IF: 2.243, AIF: 2.777 (2016)]
2. **Vaidelys, Martynas**; Ragulskienė, Jūratė; Aleksienė, Sandra; Ragulskis, Minvydas Kazys. Image Hiding in Time-Averaged Moiré Gratings on Finite Element Grids // *Applied Mathematical Modelling*. New York: Elsevier. ISSN 0307-904X. 2015, vol. 39, iss. 19, spec. iss. SI, p. 5783–5790. [Science Citation Index Expanded (Web of Science); Current Contents (Engineering, Computing & Technology); Science Direct]. [IF: 2.291, AIF: 1.671 (2015)]
3. **Vaidelys, Martynas**; Ragulskienė, Jūratė; Žiaukas, Pranas; Ragulskis, Minvydas. Image Hiding Scheme Based on the Atrial Fibrillation Model // *Applied Sciences*. Basel: MDPI AG. ISSN 2076-3417. 2015, vol. 5, iss. 4, p. 1980–1991. [Science Citation Index Expanded (Web of Science); Current Contents (Physical, Chemical & Earth Sciences); Current Contents (Engineering, Computing & Technology)]. [IF: 1.726, AIF: 4.276 (2015)]
4. **Vaidelys, Martynas**; Žiaukas, Pranas; Ragulskis, Minvydas Kazys. Competitively Coupled Maps for Hiding Secret Visual Information // *Physica A: Statistical Mechanics and Its Applications*. Amsterdam: Elsevier. ISSN 0378-4371. 2016, vol. 443, p. 91–97. [Science Citation Index Expanded (Web of Science); Scopus; Current Contents (Physical, Chemical & Earth Sciences)]. [IF: 2.243, AIF: 2.777 (2016)]
5. **Vaidelys, Martynas**; Aleksienė, Sandra; Ragulskienė, Jūratė. Dynamic Visual Cryptography Scheme on the Surface of a Vibrating Structure // *Journal of Vibroengineering*. Kaunas: JVE International. ISSN 1392-8716. 2015, vol. 17, iss. 8, p. 4142–4152. [Science Citation Index Expanded (Web of Science); Inspec; Academic Search Complete; Central & Eastern European Academic Source (CEEAS); Computers & Applied Sciences Complete; Current Abstracts; TOC Premier]. [IF: 0.384, AIF: 2.315 (2015)]
6. Telksnys, Tadas; Navickas, Zenonas; **Vaidelys, Martynas**; Ragulskis, Minvydas. The Order of a 2-Sequence and the Complexity of Digital Images // *Advances in Complex Systems*. Singapore: World Scientific Publishing. ISSN 0219-5259. 2016, vol. 19, iss. 4–5, article 1650010, p. [1–25]. [Science Citation Index Expanded (Web of Science); Scopus; Current Contents/Physical, Chemical & Earth Sciences]. [IF: 0.833, AIF: 3.263 (2016)]

Publications in Peer-Reviewed Journals and Conference Proceedings:

1. **Vaidelys, Martynas**; Lu, Chen; Yujie, Cheng; Vaidelienė, Gintarė. Image

Hiding in Dynamic Unstable Self-Organizing Patterns // *Vibroengineering Procedia*: [28th International Conference on Vibroengineering, Beijing, China, 19–21 October, 2017]. Kaunas: JVE International. ISSN 2345-0533. 2017, vol. 14, p. 328–333. DOI: 10.21595/vp.2017.18296.

2. Aleksienė, Sandra; **Vaidelys, Martynas**; Aleksa, Algimantas; Ragulskis, Minvydas Kazys. Dynamic Visual Cryptography on Deformable Finite Element Grids // *AIP Conference proceedings: International conference of numerical analysis and applied mathematics (ICNAAM 2016)*. Melville, NY: AIP Publishing. ISSN 0094-243X. 2017, vol. 1863, iss. 1, article 440002, p. 1–4. DOI: 10.1063/1.4992606.

SL344. 2018-05-31, 13.75 leidyb. apsk. l. Tiražas 14 egz. Užsakymas 196.
Išleido Kauno technologijos universitetas, K. Donelaičio g. 73, 44249 Kaunas
Spausdino leidyklos „Technologija“ spaustuvė, Studentų g. 54, 51424 Kaunas