KAUNO TECHNOLOGIJOS UNIVERSITETAS
MATEMATIKOS IR GAMTOS MOKSLŲ FAKULTETAS

Irma Dirsytė

VAIZDŲ PARINKIMAS DINAMINĖJE VIZUALINĖJE KRIPTOGRAFIJOJE

Baigiamasis magistro projektas

Vadovas
Doc. dr. Algiment Aleksa

KAUNAS, 2016

KAUNO TECHNOLOGIJOS UNIVERSITETAS

MATEMATIKOS IR GAMTOS MOKSLŲ FAKULTETAS

VAIZDŲ PARINKIMAS DINAMINĖJE VIZUALINĖJE KRIPTOGRAFIJOJE

Baigiamasis magistro projektas

Taikomoji matematika (612G10003)

Vadovas
(parašas) Doc. dr. Algiment Aleksa
(data)

Recenzentas
(parašas) dr. Vilma Petrauskienė
(data)

Projektą atliko
(parašas) Irma Dirsytė
(data)

KAUNAS, 2016

KAUNO TECHNOLOGIJOS UNIVERSITETAS

MATEMATIKOS IR GAMTOS MOKSLŲ FAKULTETAS

Irma, Dirsytė

Taikomoji matematika (612G10003)

Baigiamojo projekto „Vaizdų parinkimas dinaminėje vizualinėje kriptografijoje“

AKADEMINIO SĄŽININGUMO DEKLARACIJA

2016 m.gegužės mėn. 30 d.

Kaunas

Patvirtinu, kad mano, **Irma Dirsytė,** baigiamasis darbas tema „Vaizdų parinkimas dinaminėje vizualinėje kriptografijoje“ yra parašytas visiškai savarankiškai, o visi pateikti duomenys ar tyrimų rezultatai yra teisingi ir gauti sąžiningai. Šiame darbe nei viena darbo dalis nėra plagijuota nuo jokių spausdintinių ar internetinių šaltinių, visos kitų šaltinių tiesioginės ir netiesioginės citatos nurodytos literatūros nuorodose. Įstatymu nenumatytų piniginių sumų už šį darbą niekam nesu mokėjęs.

Aš suprantu, kad išaiškėjus nesąžiningumo faktui, man bus taikomos nuobaudos, remiantis Kauno technologijos universitete galiojančia tvarka.

_____ _____

(studento vardas ir pavardė, įrašyti ranka) (parašas)

Dirsytė, Irma. Selection of Images in Dynamic Visual Cryptography. *Master's work* / supervisor doc. dr. Algiment Aleksa; The Faculty of Mathematics and Natural science, Kaunas University of Technology.

Research area and field: Mathematical Modeling.

Key words: *Dynamic Visual Cryptography, Averaging in Time, Moire Fringes, Correlation analysis.*

Kaunas, 2016. 75 pp.

SUMMARY

In this paper we consider selection of images in dynamic visual cryptography. Dynamic visual cryptography is a new visual cryptography technique, which allows visual information to be encoded into a single moire grating. The secret information can be leaked only when the image is oscillated into a predefined direction and amplitude [22]. The decryption of the secret image is completely visual and can be performed by the person's visual system.

We use the digital computer equipment and programming software to identify the range of oscillation, at which the human eye is able to detect the encoded letters. The secret image is oscillated until a person can recognize a single letter of alphabet.

It is shown that the ability to detect the secret letters depends on the person's age, physical state, sex and eye sight. Although we have not enough evidence to confirm that the decoding algorithm depends on the person's characteristics, we can say that detection of letters: x, z, S very much depends on the factors: sex, age, eye sight and physic state. Also we have to reject the null hypothesis that there is any relationship between letters detection and time.

The interesting results it is shown, when we compare all into a single moire grating embedded letters detection range and a person characteristics. Then the relationship between age, sex, eye sight and the decoding range is not significant; the correlation between time and decoding algorithm oscillation is significant. In fact, we can say, that if a person has more experience with a decoding algorithm, relationship between time and detection of letters is growing.

Dirsytė, Irma. Vaizdų parinkimas dinaminėje vizualinėje kriptografijoje. *Magistro* baigiamasis projektas/ vadovas doc. dr. Algiment Aleksa; Kauno technologijos universitetas, Matematikos ir gamtos mokslų fakultetas.

Mokslo kryptis ir sritis: matematinis modeliavimas.

Reikšminiai žodžiai: *Dinaminė vizualinė kriptografija, muaro metodas, vidurkiniams laike, koreliacinė analizė.*

Kaunas, 2016.75 pp.

SANTRAUKA

Šiame darbe yra nagrinėjama vaizdų parinkimo dinaminėje vizualinėje kriptografijoje problema. Dinaminė vizualinė kriptografija – tai nauja vizualinės kriptografijos technika, kuri leidžia slaptą informaciją užkoduoti vienmatėje muaro gardelėje. Paslėptas vaizdas yra dekoduojamas pagal iš anksto pasirinktą virpinimo amplitudę ir kryptį [22]. Dekodavimo algoritmas yra absoliučiai vizualus ir yra atliekamas tik pasitelkus žmogaus vizualinę sistemą.

Mes naudojome skaitmeninį įrenginį ir programinę įrangą dekodavimui atlikti. Tokiu būdu dekoduojant yra parenkamas individualus virpinimo dažnis, kuris leidžia atpažinti užkoduotas atskiras raides.

Darbe parodoma, kad dekodavimas yra individualus procesas, kuris priklauso nuo šių veiksnių: lyties, amžiaus bei fizinės būsenos. Hipotezė, dėl stebėjimo laiko ir raidės atpažinimo virpinant užkoduotą vaizdą, yra atmetama. Atskirų raidžių dekodavimas priklauso nuo skirtingų veiksnių, tačiau labiausiai lytis, amžius, rega bei asmens fizinė būklė įtakoja raidžių x, S, z atpažinimą

Palyginimui pateikti rezultatai, gauti fiksuojant ne pavienių raidžių atpažinimą, bet visų paveiksle esančių raidžių atpažinimą; dekodavimo algoritmas kartojamas tol, kol asmuo atpažins visą užkoduotą vaizdą. Iš pateiktų rezultatų analizės matyti, kad viso vaizdo dekodavimo proceso dažnis labiausiai priklauso nuo laiko. Amžiaus, lyties ar regos sąryšis su paveiksle užkoduotu vaizdo atpažinimu neįrodytas.

TURINYS

PAVEIKSLŲ SĄRAŠAS

LENTELIŲ SĄRAŠAS

Priedai

Temos aktualumas ir naujumas

Dinaminė vizualinė kriptografija – tai alternatyvi informacijos slėpimo technika, koduojanti vaizdą geometrinėje muaro gardelėje. Slaptos informacijos dekodavimas nusakomas virpinimo amplitudės kitimu, kurios reikšmė priklauso nuo užkoduoto vaizdo parametrų [22]. Dekodavimo procedūra yra paprasta mechaninė operacija, paremta optiniais ir fizikiniais reiškiniais; algoritmas yra sąlyginai nesudėtingas ir priklausantis tik nuo dekodavimo procese dalyvaujančio asmens gebėjimo sekti besikeičiančius vaizdus. Besikeičiančių vaizdų atpažinimas yra individualus procesas, priklausantis nuo tam tikrų asmens bei laiko charakteristikų [17].

Vaizdų parinkimas ir sudarymas yra aktuali problema dinaminėje vizualinėje kriptografijoje. Užkoduotos slaptos informacijos harmoninių virpesių dažnio parinkimas priklauso ne tik nuo minėtų asmens bei laiko charakteristikų, bet ir nuo koduojamos slaptos informacijos; tas pats asmuo vienus simbolius atpažįsta generuojant vaizdą mažesniu virpinimo dažniu, kitų simbolių atpažinimui jam prireikia kur kas didesnio virpinimo dažnio.

Atsitiktinai parinktų abėcėlės raidžių kodavimas geometrine muaro gardele leidžia parinkti kiekvienai raidei optimalų dekodavimo algoritmo dažnį. Statistinė analizė, interpretuojanti harmoniniais virpesiais virpinamo vaizdo atpažinimo dažnio priklausomybę nuo asmenį apibūdinančių charakteristikų, pateikta šiame darbe. Pateiktos nepalankiausios dekodavimui abėcėlės raidės, kurių dekodavimo dažnio parinkimas yra labiau priklausomas nuo asmens savybių nei nuo objektyvių dekoduojamo simbolio savybių. Taip pat palyginami rezultatai, gauti atliekant dekodavimo algoritmą iki tol, kol yra atpažįstamos ne pavienės raidės, bet visa užkoduota informacija.

Tyrimo objektai

1. Analitiniai sąryšiai, kuriais formuojami bei dekoduojami vaizdai, pagrįsti interferencinių juostų susidarymo metodu.
2. Statistiniai sąryšiai, tarp vaizdų dekodavime naudojamo, dinaminiais virpesiais paremto vaizdo atpažinimo dažnio bei asmens ir laiko charakteristikų.
3. Dekoduojamo objekto optimalumas dinaminės vizualinės kriptografijos kodavimo schemoje.

Darbo tikslai

1. Išanalizuoti ir pritaikyti matematiniais ryšiais paremtus kodavimo bei dekodavimo algoritmus.
2. Sudaryti optimalius, statistiniais metodais pagrįstus dinaminėje vizualinėje kriptografijoje konstruotinus simbolius.

3. Pritaikyti statistinės analizės metodus.

Tyrimo uždaviniai

1. Suformuoti vaizdus, paremtus laike vidurkintu geometrinio muaro metodu.
2. Vizualizuoti ir dekoduoti vaizdus, keičiant harmoninių virpesių dažnį, atitinkantį asmens gebėjimą atpažinti virpinamą simbolį.
3. Ištirti simbolius, kurių atpažinimo dažnio priklausomybė nuo asmens bei laiko charakteristikų stipriausia; atsekti optimalius simbolius.

1.TEORINĖ DALIS

1.1 ESMINIAI KRIPTOGRAFIJOS PRINCIPAI

Moderniame pasaulyje privatumas tampa vis aktualesnis. Internetu, bevieliu ryšiu ar įvairiais vietiniais tinklais yra siunčiami milžiniški kiekiai informacijos. Todėl pagrindinis kriptografijos uždavinys yra šiuos nesaugius kanalus paversti saugiais. Informacijos saugumo užtikrinimui duomenys yra užkoduojami siuntėjo ir dekoduojami teisėto informacijos gavėjo. Kodavimo bei dekodavimo procesas vykdomas asmens, kompiuteriu ar tam skirto kietojo disko įrenginių.

Tradicinėse kriptosistemose kodavimo bei dekodavimo procesas dažniausiais yra paprastos atvirkštinės matematinės operacijos: pakeitimai, perstatymai, sudėtis bei daugyba moduliu.

Viena iš esminių tradicinės kriptografijos charakteristikų yra tai, kad kodavimui bei dekodavimui naudojamas bendras raktas, kuris privalo būti saugomas ir žinomas tik siuntėjui bei gavėjui. Vadinasi, prieš pradedant bendrauti, abi komunikuojančios grupės turi susitikti arba panaudoti saugius kanalus tam, kad pasidalintų raktais.

Tačiau ši problema buvo išspręsta, kai Diffie Hellman (1976) pristatė naujos kartos asimetrinę viešojo rakto kriptosistemą [4]. Pagal šią koncepciją dekodavimo bei atkodavimo schemose yra naudojami skirtingi kriptografiniai raktai; jei dekodavimo raktas turi būti saugomas slaptai, atkodavimo raktas gali būti publikuojamas.

Kadangi gavėjo kodavimo raktas yra viešas, tai bet kuris asmuo gali siųsti žinutę užkoduodamas ją gavėjo viešu kodavimo raktu. Tačiau atkoduoti žinutę gali tik legitimus gavėjas, kuris turi atitinkamą dekodavimo raktą.

Vizualinė kriptografija skiriasi nuo tradicinės kriptografijos tuo, kad informacijos šifravimui yra naudojami matematiniai algoritmai, tačiau dešifravimas sąlyginai nesudėtingas ir jam atlikti reikalingas tik vienas iš distancinių žmogaus pojūčių – rega.

Lyginant su kai kuriomis kriptografinėmis schemomis, kurios yra saugios tik esant tam tikroms sąlygoms, vizualinės kriptografijos dekodavimas yra besąlygiškai saugus. Kitas vizualinės kriptografijos privalumas jos paprastumas bei lengvas įsisavinimas; taikant šią schemą, nereikalaujama jokių sudėtingų skaičiavimų bei dekodavimo algoritmų. Elektroninis slaptas vaizdas gali būti pasidalijamas tiesiogiai arba atspausdintas ant peršviečiamo popieriaus ir sutapdinamas, tokiu būdu atskleidžiant slaptą vaizdą.

1.2 VIZUALINĖ KRIPTOGRAFIJA

Vizualinė kriptografija yra aprašoma „kaip naujo tipo kriptografinė schema, kuri slapto vaizdo dekodavimui nenaudoja jokių kriptografinių skaičiavimų“ [13]. Užkodavimas yra apibrėžiamas kaip (k, n) paslapties dalijimo schema.

Tegul duotas paveikslas *I, k* dalių yra generuojamos ir slaptas vaizdas išryškėja, kai bet kurios *k* dalių yra sujungiamos. Analogiškai, paslaptis lieka saugi, jei $n - 1 < k$.

Kiekvienas paveikslo I taškas yra aprašomas kaip *n* modifikuotų dalių [13]. Dalys yra tam tikras rinkinys *m* baltų ir juodų taškų. Rezultatų matrica gali būti aprašyta kaip Būlio matrica $S = S_{ij}$

$S_{ij} = 1$, jei i –tasis taškas i- tojoje dalyje baltas;

$S_{ij} = 0$, jei j-tasis taškas j- tojoje dalyje yra juodas.

Kai dalys sujungiamos vaizdas yra matomas, bet paveikslo *I* dydis padidėja *m* kartų. Atkurto paveikslo pilkio lygis yra proporcingas vektoriaus V hemingo svoriui (angl.hamming weigtht); čia V-kiekvieno originalaus taško (pixelio) poaibis.

Pagrindiniai aprašytos schemos parametrai yra šie [11, 27]:

- *m* - pixelių skaičius dalyje (angl. share);
- α - reliatyvus svorio skirtumas tarp kombinuotos dalies, kuri gaunama iš baltų ir juodų originalaus paveikslo pixelių, t.y. kontrasto praradimas;
- γ – matricų aibės C_0 dydis.

Tokiu būdu juodas pixelis yra gaunamas, kai $H(V) \leq d$, baltas - $H(V) \leq d - \alpha$; su visais $1 \leq d \leq m$ ir $\alpha > 0$.

(2,2) vizualinės kriptografijos schema yra apibrėžiama kaip taškų (pixelių) rinkinys [13] :

$$B_0 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}$$

$$B_1 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

$C_0 =$ {visos matricos gautos, perstatant matricos B_0stulpelius}

$C_1 =$ {visos matricos gautos, perstatant matricos B_1 stulpelius}

Dėl šio taškų (pixelių) perstatymo, vienas originalaus vaizdo pixelis pakeičiamas keturiais. Dalys yra generuojamos tokiu būdu (1.1 pav.):

- Jei originalaus binarinio paveikslo (*I*) pixelis yra baltas, atsitiktinai parenkamas tas pats modelis iš keturių pixelių abiems dalims;
- Jei originalaus binarinio paveikslo (*I*) pixelis yra juodas, tai atsitiktinai parenkamas modelis iš to paties stulpelio.

a) b) c)

1.1 pav. Pagrindinė vizualinės kriptografijos schema. Įvairios padalijimų schemos: a) horizontalūs padalijimai; b) vertikalūs padalijimai; c) diagonalės padalijimai [13]

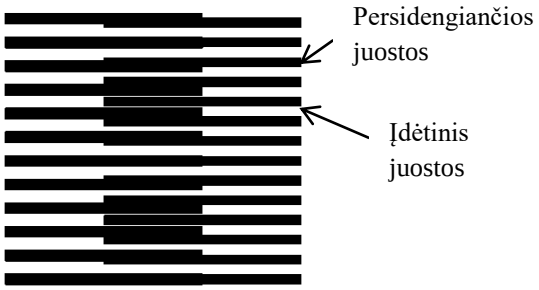
Be pagrindinės vizualinės kriptografijos schemos [13] yra pasiūlyta keletas kitų vizualinės kriptografijos patobulinimų: vizualine kriptografija pilkio lygio vaizdams (angl. gray level images) [1], pustonio (angl. halftone) vizualinė kriptografija [8], vizualinė kriptografija spalvotiems vaizdams [11], progresyvinė (angl. progressive visual) vizualinė kriptografija [5], srities pokyčio vizualinė kriptografija [26] bei išplėsta (angl. extendet) vizualinė kriptografija [10].

Viena iš naujausių vizualinės kriptografijos schemų yra 2009 metais sukurta dinaminė vizualinė kriptografija [22]. Tai dinaminis vieno vaizdo metodas, paremtas laike vidurkintų muaro interferencinių juostų susidarymu.

1.3 MUARO METODO PAGRINDINIAI PRINCIPAI

Muaro fenomenas pasireiškia, kai sutapdinami du skaidrūs sluoksniai, kurie apima periodiškai pasikartojančias neskaidrias paralelias linijas ar taškus. Tai klasikinis neardančios kontrolės metodas, naudojamas paviršiaus nelygumams ir deformacijoms tirti [2, 12].

Sutapdintas vaizdas nesikeičia, jei skaidrūs sluoksniai yra atvirkštiniai neskaidriam modeliui. Dviejų sluoksnių modelio periodas, t.y. tarpas tarp paralelių linijų ašių, turi būti nedidelis [7]. Tegul bazinio sluoksnio juostų periodas žymimas p_b, atskleidžiančio sluoksnio juostų periodas - p_r, t.y atstumas nuo persidengiančios juostos taško (figūros apačios) iki kito analogiško taško (figūros viršaus).



1.2 pav. Sutapdintos gardelės, kurias sudaro periodiškai pasikartojančios paralelios linijos [7]

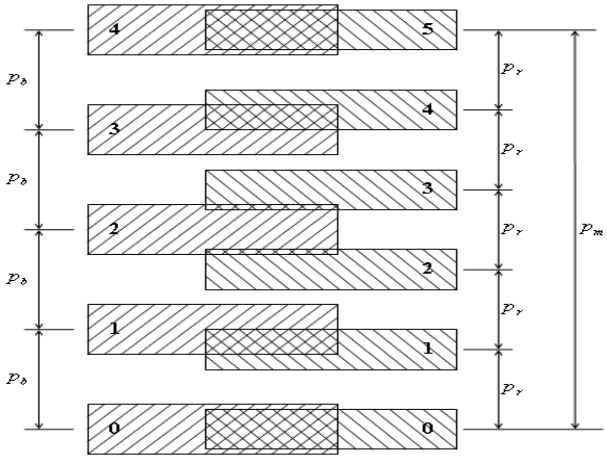
Šviesios sutapdinto vaizdo spalvos apibrėžia juostas, kurios persidengia, juodos juostos susiformuoja ten, kur abiejų sluoksnių zonos „įsideda“, paslėpdamos baltą pagrindą. Juodos ir baltos juostos formuojasi periodiškai [1.2 pav., 7].

Bazinio sluoksnio juostos gali įgyti atstumą p_m, kurį sudaro tiek juostų (p_m/p_b), kiek yra atskleidžiančio sluoksnio juostų (p_m/p_r) tam pačiam atstumui minus 1 [1.3 pav.], t.y.

$$\frac{p_m}{p_r} = \frac{p_m}{p_b} + 1. \tag{1.1}$$

Iš (2.1) gauname:

$$p_m = \frac{p_b . p_r}{p_b - p_r}. \tag{1.2}$$



1.3 pav. Muaro gardelės periodo skaičiavimo schema [7]

Aprašytas metodas yra skiriamas į kelias pagrindines šakas: geometrinis muaro metodas, šešėlinis muaro metodas [12], projekcinis muaro metodas [12] bei laike vidurkintas geometrinio muaro metodas [20, 21, 9], kurio pagrindinės ypatybės yra dinaminės vienmatės gardelės naudojimas.

1.4. VAIZDO SLĖPIMAS MUARO GARDELĖJE

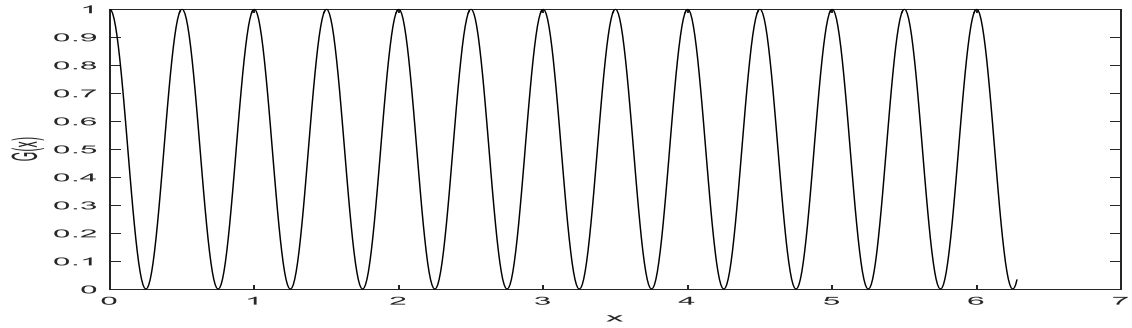
Laike vidurkintas geometrinio muaro metodas neapsiriboja vien tik paviršiaus nelygumų ir defektų tyrimu. Šis metodas taip pat yra pasitelktas informacijos slėpimui dinaminėje vizualinėje kriptografijoje [22, 23, 25]. Dinaminėje vizualinėje kriptografijoje slapto vaizdo kodavimo bei dekodavimo procedūra yra pagrįsta optiniais bei fizikiniais reiškiniais ir skaitmeniniais vizualizavimo algoritmais. Kaip jau minėta, vizualinės kriptografijos esminis principas yra slapto vaizdo skaidymas į n dalių [3]. Dinaminėje vizualinėje kriptografijoje naudojamas vienas

vaizdas, kuris nėra skaidomas į n dalių [16]. Kita vertus, vaizdo dekodavimo procedūrai atlikti naudojamos paprastos mechaninės operacijos ir žmogaus rega.

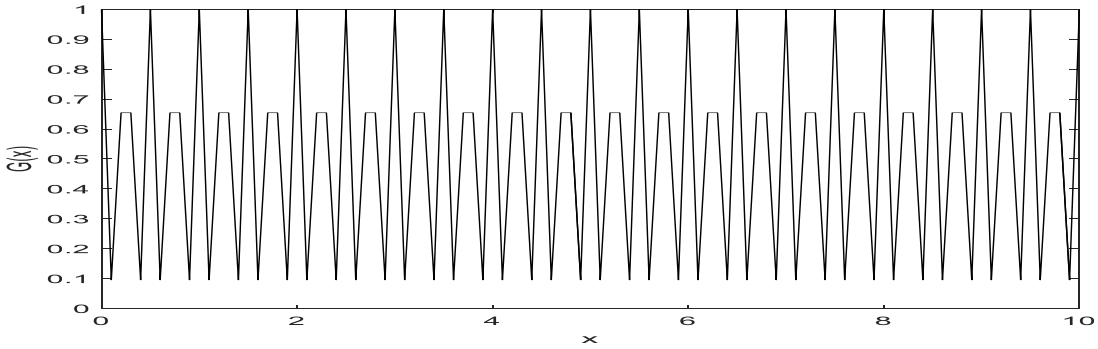
Statinis slaptas paveikslas yra sudarytas iš slaptos informacijos ir tos informacijos fono. Toks slaptas vaidas yra užkoduojamas pilkio lygių muaro gardelėje, kurią aprašo lygtis (1. 4pav.) [22]:

$$G(x) = \frac{1}{2} + \frac{1}{2}\cos(\frac{2\pi}{\lambda}x); \tag{1.3}$$

čia x yra koordinatė, $G(x)$ −pilkos spalvos lygis taške x, λ yra gardelės periodas. Skaitinė lygties (1.1) reikšmė 0 atitinka juodą spalvą, 1–baltą spalvą, tarpinės reikšmės atitinka pilkos spalvos lygį.



1.4 pav. Vaizdo kodavimui naudojama funkcija *G (x)*, kai $\lambda = 0{,}5$



1.5 pav.. Vaizdo kodavimui naudojama funkcija *G (x)*, kai $\lambda = 0{,}25$

Jei netinkamai parinksime funkcijos *G (x)* parametrus (1.5 pav.) negalėsime suformuoti gardelės, kuri tiksliai nusakytų pilkio lygį.

Tegul muaro gardelės yra virpinamos apie pusiausvyros taškus ir nuokrypis nuo pusiausvyros padėties nepriklauso nuo *x*. Tuomet nuokrypio nuo pusiausvyros padėties funkcija yra aprašoma lygtimi [22]:

$$u(x,t) = \mathrm{a}(x)\sin(\omega t + \varphi); \tag{1.4}$$

čia *a (x)* yra harmoninių virpesių svyravimų amplitudė, *φ* – fazė, *ω* – ciklinis dažnis.

Vaizdas dekoduojamas – vizualizuojamas laike vidurkintų interferencinių juostų pavidalu, kai atsilenkimas nuo pusiausvyros padėties yra griežtai apibrėžta funkcijos realizacija su iš anksto žinomais šios funkcijos parametrais. Toks pilkos spalvos lygis nusakomas lygtimi [22]:

$$G_1(x) = \lim_{T\to\infty}\frac{1}{T}\int_0^T (\frac{1}{2} + \cos(\frac{2\pi}{\lambda}x - a(x)\sin(\omega t + \varphi)))dt$$
$$= \frac{1}{2} + \frac{1}{2}\cos(\frac{2\pi}{\lambda}x)\lim_{T\to\infty}\frac{1}{T}\int_0^T \cos(\frac{2\pi}{\lambda}a(x)\sin t)\,dt$$
$$+ \frac{1}{2}\sin(\frac{2\pi}{\lambda}x)\lim_{T\to\infty}\int_0^T \sin\left(\frac{2\pi}{\lambda}a(x)sint\right)dt. \quad (1.5)$$

Sinusas yra lyginė funkcija, tai

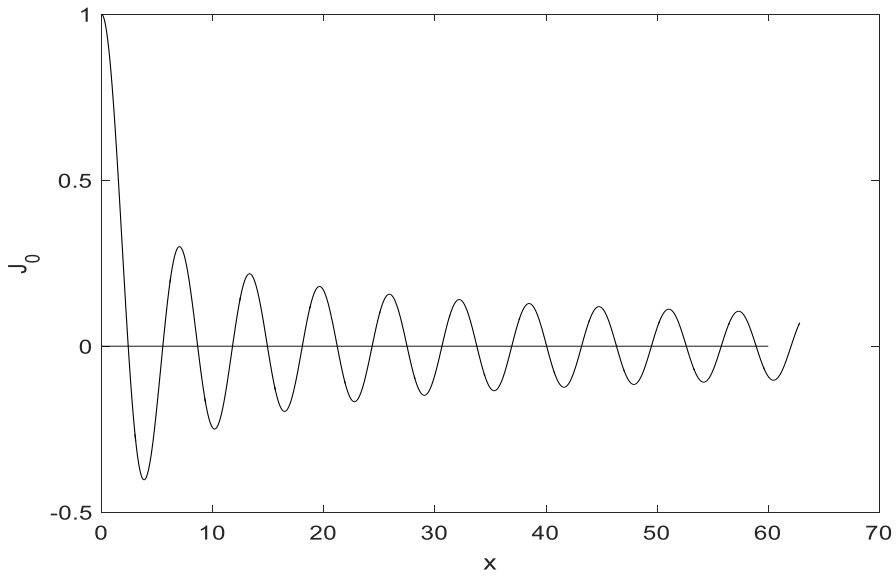
$$\lim_{T\to\infty}\frac{1}{T}\int_0^T \sin(\frac{2\pi}{\lambda}a(x)\sin t)dt = \frac{1}{\pi}\int_{-\frac{\pi}{2}}^{\frac{\pi}{2}}(\sin\frac{2\pi}{\lambda}a(x)\sin t)dt = 0. \quad (1.6)$$

Padauginę abi lygties (1.5) puses iš menamo vieneto *i* ir pakeitę $\sin(\frac{2\pi x}{\lambda})$ į $\cos(\frac{2\pi x}{\lambda})$ gausime [14]:

$$G_1(x) = \frac{1}{2} + \frac{1}{2}\cos(\frac{2\pi}{\lambda}x)\lim_{T\to\infty}\frac{1}{T}\int_0^T \cos\left(\frac{2\pi}{\lambda}a(x)\sin t\right)dt + i$$
$$\cdot\frac{1}{2}\cos(\frac{2\pi}{\lambda}x)\lim_{T\to\infty}\frac{1}{T}\int_0^T \sin\left(\frac{2\pi}{\lambda}a(x)\sin t\right)dt$$
$$= \frac{1}{2}$$
$$+ \frac{1}{2}\cos(\frac{2\pi}{\lambda}x)\lim_{T\to\infty}\frac{1}{T}\int_0^T \cos\left(\frac{2\pi}{\lambda}a(x)\sin t + i\right.$$
$$\left.\cdot\sin\left(\frac{2\pi}{\lambda}a(x)\sin t\right)dt\right)$$
$$= \frac{1}{2} + \frac{1}{2}\cos(\frac{2\pi}{\lambda}x)\lim_{T\to\infty}\frac{1}{T}\int_0^T \exp\left[\frac{2\pi}{\lambda}a(x)sint\right] = \frac{1}{2}$$
$$+ \frac{1}{2}\cos\left(\frac{2\pi}{\lambda}x\right)J_0\left(\frac{2\pi}{\lambda}a(x)\right); \quad (1.7)$$

čia T – ekspozicijos laikas, λ -gardelių periodas, $a(x)$- pastovi svyravimų amplitudė, J_o- nulinės eilės pirmos rūšies Beselio funkcija (1.3 pav.):

$$J_o(x) = \lim_{T\to\infty}\frac{1}{T}\int_0^T \exp\left[\frac{2\pi}{\lambda}x\sin t\right]dt. \quad (1.8)$$



1.6 pav. Nulinės eilės pirmos rūšies Beselio šaknis

Laike vidurkintos muaro gardelės formuosis prie tokių amplitudžių a_i, kai nulinės eilės pirmos rūšies Beselio šaknis lygi 0:

$$J_0\left(\frac{2\pi}{\lambda}a(x)\right) = 0. \tag{1.9}$$

Pilkio lygį originaliame vaizde nusako funkcija:

$$\frac{1}{2} \pm \frac{1}{2}J_0\left(\frac{2\pi}{\lambda}a(x)\right). \tag{1.10}$$

Vadinasi, sąryšis tarp muaro gardelės λ, harmoninių virpesių amplitudes a_i ir laike vidurkintos muaro gardelės skaičiaus nusakomas šia lygtimi [22]:

$$\frac{2\pi}{\lambda}a_i = r_i, \qquad i = 1,2,\dots \tag{1.11}$$

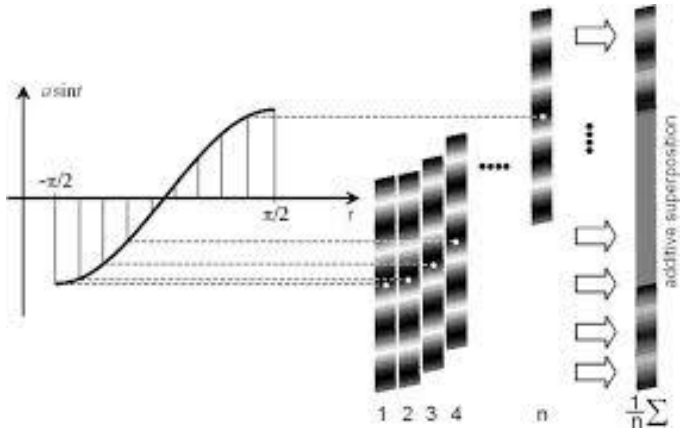
čia r_i – nulinės eilės pirmos rūšies Beselio šaknis, a_i – virpinimo amplitudė *i*-tosios gardelės centre.

Kompiuterinėje realizacijoje (1.6 pav.) dekoduotas vaizdas yra konstruojamas kaip integralinė suma [22]:

$$G_T(x,y) = \lim_{T\to\infty}\frac{1}{n}\sum_{k=0}^{n-1}\cos\left(\frac{2\pi}{\lambda}a(x)\,sin\left(\frac{2\pi k}{n}\right)\right); \tag{1.12}$$

čia λ – gardelių periodas, n –diskretinių kadrų skaičius viename virpesių periode. Kiekvienas kadras yra nuokrypio nuo pusiausvyros padėties atitikmuo, kurių vidurkis – vaizdas vidurkintas laike.

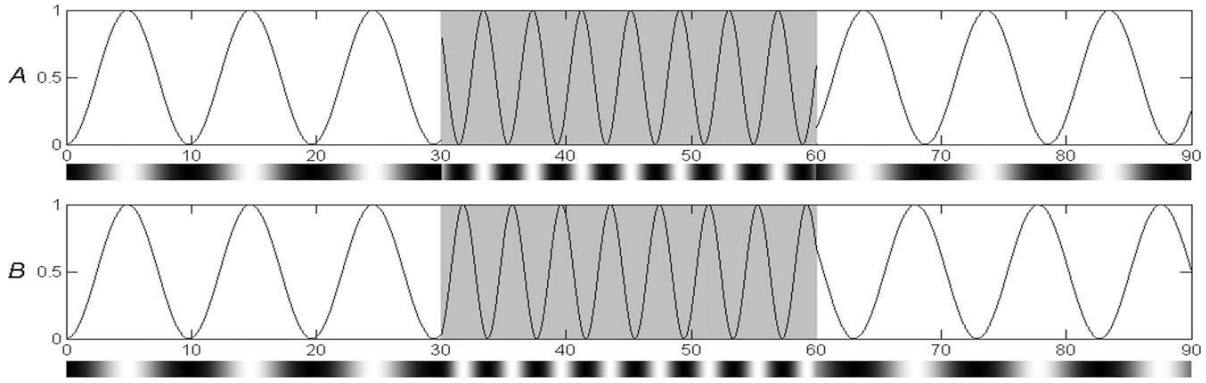
Dekodavimo procedūra yra atliekama pagal (1.11) lygtį.



1.7 pav. Scheminė diagrama, vaizduojanti laike vidurkinto vaizdo rekonstrukciją [22]

Slapta informacija yra užkoduojama (1.8 pav.), sudarant vertikalių taškų (pixelių) stulpelius. Kiekviename stulpelyje slaptos informacijos foną atitinka muaro gardelė, kurios periodas yra λ_1. Informacijos tekstą sudaro periodas λ, kuris randamas iš lygties (1.11) [16].

Statinį vaizdą virpinant pagal harmoninį dėsnį slaptos informacijos tekste susiformuoja interferencinės juostos (muaro gardelės su periodu λ papilkėja). [16].Tam, kad neišryškėtų riba tarp skirtingo periodo slapto vaizdo ir jo fono krašto, naudojamas fazių reguliarizacijos algoritmas .



1.8 pav. Fazių reguliarizacijos algoritmas; pilkio lygis prieš fazių reguliarizaciją (A), pilkio lygis po fazių reguliarizacijos (B)[22]

1.5 SLAPTO VAIZDO KODAVIMAS LAIPTINE MUARO GARDELE

1.4 skyriuje aprašytas metodas nėra visiškai saugus. Dekodavimo procedūra gali būti atlikta bandymų ir klaidų metodu [23], jei tik yra žinoma, kad paslaptis yra užkoduota muaro gardele. Saugesnis kodavimo algoritmas gali būti konstruojamas parenkant harmoninių virpesių

parametrus bei nusakant laiko funkcijos virpesių dėsnį. Informacija paslepiama laiptuotos muaro gardelės funkcija, o dekoduojama harmoniniais trikampės funkcijos pavidalo virpesiais.

Slapta informacija yra koduojama 1.4 skyriuje jau aprašyta f-ja:

$$G(x) = \frac{1}{2} + \frac{1}{2}\sin\left(\frac{2\pi}{\lambda}x\right). \tag{1.13}$$

Tegul funkcija $G(x)$tenkina šias sąlygas [23, 25, 18]:

- $G(x+\lambda) = G(x);\ čia\ \lambda -$ gardelių periodas.
- $0 \le G(x) \le 1$; 1 nusako baltą spalvą. 0 – juodą, o visos tarpinės funkcijos $G(x)$reikšmės nusako pilkos spalvos lygį.
- $G(x)$turi baigtinį skaičių trūkio taškų kiekviename baigtiniame intervale *[a,b]; a<b.*

Kodavimui naudojamos laiptuotos funkcijos pavidalas yra nusakomas lygtimi [25, 20]:

$$\tilde{G}(x) = \begin{cases} 1, kai\ x \in \left[\lambda i; \left(i + \frac{1}{2}\right)\right]; \\ 0, kai\ x \in \left[\lambda i; \left(i + \frac{1}{2}\right);\ \lambda(i+1)\right] \end{cases} \tag{1.14}$$

Tuomet pilkio lygį muaro gardelėje apibrėšime štai tokiu būdu [25, 23, 17]:

$$G_m(x) = y_n, kai\ x \in \left[\frac{(n-1)}{m}\lambda + i\lambda;\ \frac{n\lambda}{m} + i\lambda\right]; n = 1,2,\dots,m, i \in \mathrm{Z} \tag{1.15}$$

čia $y_n,\ n = 1,2,\dots m$ – pilkio lygiai, apibrėžti atitinkamai iš baigtinės aibės n elementų, kurie pasiskirstę tolygiai intervale [0,1] ; $\frac{\lambda}{m}$ – vieno pixelio ilgis.

Tegul f- ją $G(x)$ nusako šie parametrai [25] :

1. $\bar{C} = \sup G(x);$ (1.16)
2. $\underline{C} = \inf G(x);$ (1.17)
3. $\gamma = \frac{1}{\lambda}\int_0^{\lambda} \inf G(z)dz;$ (1.18)
4. $\|G(x)\| = \frac{1}{\lambda}\int_0^{\lambda}\left[G(x) - \frac{1}{2}\right]dz$ (1.19)

Ir tegul galioja šie trys sąryšiai [8]:

1. $0 \le \underline{C} \le G(x) \le \bar{C};$ (1.20)

2. $0 \le \|G(x)\| \le \left|\lambda - \frac{1}{2}\right|$;

3. $F - ja\ G(x)$ gali būti išskleista Furje eilute :

$$G(x) = \frac{a_0}{2} + \sum_{k=1}^{\infty}(a_n \cos\frac{2\pi nx}{\lambda} + b_n \sin\frac{2\pi nx}{\lambda});\ \ a_n, b_n \in R; n = 1,2, \dots; a_0 = 2\gamma. \tag{1.21}$$

Tuomet slaptas vaizdas yra koduojamas šia muaro gardele [25]:

$$G(x) = \frac{1}{2} + \frac{1}{2} sgn\left(sin\left(\frac{2\pi}{\lambda}x\right)\right); \tag{1.22}$$

čia λ -gardelės periodas, $G(x)$- pilkos spalvos lygis taške 0 arba 1.

Pilkos spalvos lygis gali būti išreiškiamas Furje eilute:

$$G(x) = \frac{a_0}{2} + \sum_{n=1}^{+\infty}\left(a_n \cos\frac{2\pi nx}{\lambda} + b_n \sin\frac{2n\pi x}{\lambda}\right), n = 1,2, \dots \tag{1.23}$$

čia a_0, a_n, b_n – Furje eilutės koeficientai.

Konstruojamas laike vidurkintas vaizdas, kai ekspozicijos laikas T artėja į begalybę. Toks vaizdas yra nusakomas sąryšiu [25, 18]:

$$H_A(x|G;\tilde{\xi}) = \frac{a_0}{2} + \sum_{n=1}^{+\infty}\left(a_n \cos\frac{2\pi nx}{\lambda} + b_n \sin\frac{2\pi nx}{\lambda}\right)\frac{\sin(\frac{2\pi A}{\lambda})}{\frac{2\pi}{\lambda}A}; \tag{1.24}$$

čia $H_A(x|G;\tilde{\xi})$- vidurkinimo laike operatorius, A - virpinimo amplitudė, $A \ge 0; x \in R$.

$$H_A(x|G;\tilde{\xi}) = \lim_{T\to\infty}\frac{1}{T}\int_0^T G\big(x - \xi_A(t)\big)dt \tag{1.25}$$

Harmoniniai svyravimai yra apibrėžiami laiko funkcijos lygtimi:

$$\widetilde{\xi_A}(t) = A\sin(\omega t + \varphi); \tag{1.26}$$

čia t – laikas, ω – kampinis dažnis, φ – fazė, A-svyravimų amplitudė.

Dekodavimo procedūra yra atliekama virpinant skaitmeninį vaizdą trikampės periodinės funkcijos pavidalu [25]:

$$\check{\xi}_A(t) = \begin{cases} \frac{2A\omega}{\pi}\left(t - \left(\frac{\pi}{2\omega} - \varphi + \frac{2\pi n}{\omega}\right)\right) - A, kai\ t\epsilon\left[\left(-\frac{2\pi}{2\omega}i - \frac{\pi}{2\omega}\right); \left(\frac{2\pi}{\omega}i + \frac{\pi}{2\omega}\right)\right] \\ -\frac{2A\omega}{\pi}\left(t - \left(\frac{\pi}{2\omega} - \varphi + \frac{2\pi}{\omega}n\right)\right) + A, kai\ t\epsilon\left[\left(\frac{2\pi}{\omega}i + \frac{\pi}{2\omega}\right); \left(\frac{2\pi}{\omega}i + \frac{3\pi}{\omega}\right)\right] \end{cases}; \quad (1.27)$$

čia $\check{\xi}_A(t)$ – laiko funkcija, A – svyravimų amplitudė, ω – kampinis dažnis, φ – fazė.

Laike vidurkinta muaro gardelė formuojasi, kai sąryšis tarp vingiuotos laužtinės linijos pavidalo virpinimo (1.27), laike vidurkintų gardelių eilės ir gardelių žingsnių, yra nusakomas lygtimi [23, 18]:

$$A_i = \frac{i\lambda}{2};\ i = 1,2, \ldots \quad (1.28)$$

čia i - laike vidurkintų gardelių eilė; λ –gardelių periodas.

- Laike vidurkintos muaro gardelės pilkio funkcijos vidurkis apibrėžiamas lygtimi [25] :

$$E(H_A(x\lfloor G;\xi_A) = \frac{1}{\lambda}\int_0^{\lambda} H_A(x\lfloor G,\xi_A)\mathrm{dx}; \quad (1.29)$$

čia E yra vidurkinimo operatorius.

- Laike vidurkintos muaro gardelės pilkio funkcijos dispersija apibrėžiama:

$$\sigma\left(H_A(x\lfloor G;\xi_A)\right) = \sqrt{\frac{1}{\lambda}\int_0^{\lambda}(H_A(x\lfloor G;\xi_A) - \ (E(H_A(\lfloor G,\xi_A))^2\, dx}. \quad (1.30)$$

- Laike vidurkintos muaro gardelės funkcijos virpinamos trikampės periodinės funkcijos pavidalu (1.27) standartinis nuokrypis nusakomas lygtimi:

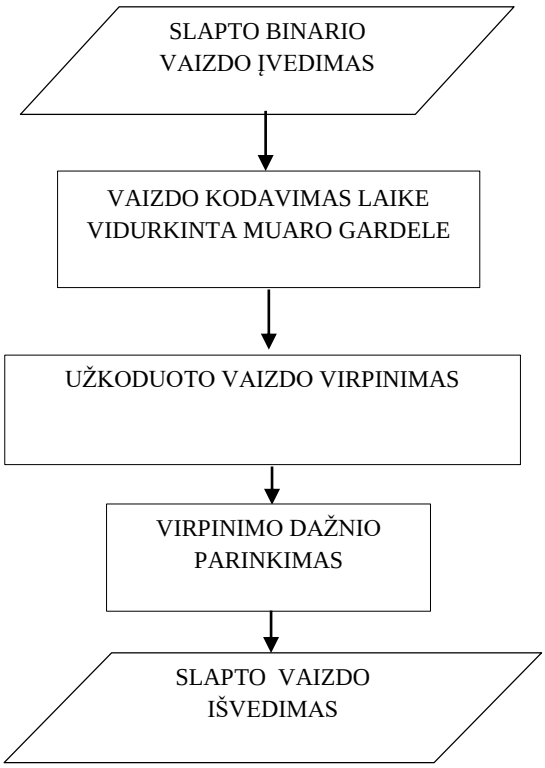
$$\sigma(H_A(x\lfloor G;\check{\xi}_A) = \frac{\sqrt{2\lambda}}{4\pi A}\sqrt{\sum_{k=1}^{\infty}(a_n^2 + b_n^2)\frac{sin^2\left(\frac{2\pi nA}{\lambda}\right)}{n^2}}. \quad (1.31)$$

Muaro metodu užkoduotos slaptos informacijos dekodavimo algoritmas, kai pasirenkamas harmoninių virpesių dažnis bei parametrai yra saugesnė dekodavimo schema. Kita vertus, harmoniniai virpesiai net ir sužadinti nėra tiesiniai. Chaotinės vizualinės schema bei optimalios muaro gardelės sudarymo algoritmai yra plačiau nagrinėjami literatūros šaltinyje [15, 16].

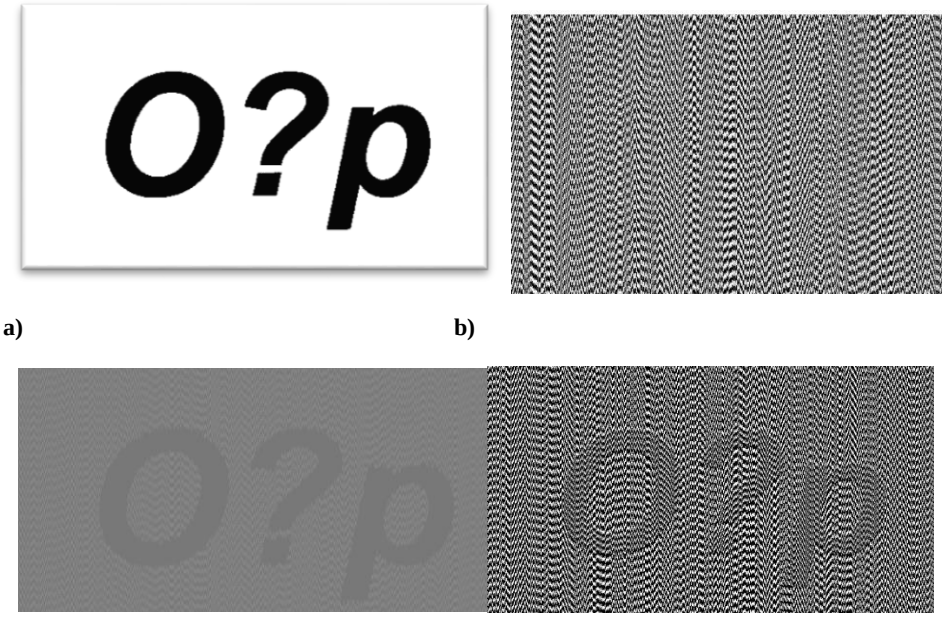
Išnagrinėtu dekodavimo metodu, kai muaro gardele užkoduotas vaizdas yra virpinamas periodinės trikampės laiko funkcijos pagalba, remsimės atlikdami mechaninę dekodavimo procedūrą. Programine įrangą virpinsime vaizdą periodiniais svyravimais, keisdami virpinimo dažnį, tokiu būdu siekdami nustatyti koreliacinius dekodavimo algoritmo ir asmens požymių sąryšius.

1.6 LAIPTINE MUARO GARDELE UŽKODUOTO VAIZDO DEKODAVIMO MECHANINE PROCEDŪRA

Aprašytu metodu užkoduota slapta informacija (1.10.b) pav.) yra dekoduojama, virpinant paveikslą specialia programine įranga (Adobe Flash Profesional CS6), kuri leidžia keisti svyravimų dažnį esamu laiku. Slapto vaizdo dekodavimas ((1.1.d) pav.) nusakomas virpinimo amplitudės kitimu, kurios reikšmė priklauso nuo užkoduoto vaizdo parametrų, susietų su lygtimi (1.21). Tai absoliučiai vizualus dekodavimo algoritmas, priklausantis tik nuo žmogaus gebėjimo atpažinti besikeičiančius vaizdus (1.9)



1.9 pav. Supaprastinta dinaminės vizualinės kriptografijos dekodavimo schema, naudojama vaizdo virpinimui programine įranga



1.10 pav. a) Slapta informacija, b) užkoduota slapta informacija; c) Dekoduota slapta informacija. Skaitmeninė vaizdo rekonstrukcija; d) dekoduota informacija, panaudojant programinę įranga.

Vaizdo kodavimo muaro gardele pseudo kodas.

1. Įvedame [550x1000] dydžio paveikslą.
2. Tegul turime nauja matricą, kurios dydis [*m x n]=[550 x1000]*
3. Sudarome dvi naujas matricas teksto ir fono kodavimui. Fono dydis [mf, nf] =[000000000000 111111111111], teksto dydis [mt, nt] = [000000000 111111111]. 0 atitinka juodą spalvą, 1 – baltą spalvą.
4. Atsitiktinai, pagal matlab funkciją *random,* parenkame slapto fono stulpelį.

random(1:n)=0;

FOR I:=1..n

FOR I:=1:n loop

randomas (I)=mod (round (1000*rand),nf)+1;

END

5. Koduojama stačiakampiais. Sudaromas užkoduotas vaizdas, kai keičiasi fonas ir kai keičiasi tekstas.

img _mod (1:m+nf,1:n)=1;

a) Sudarome užkoduotus stulpelius FOR I = 1:n

J=1;

JJ=1;

b) Sudarome užkoduotas eilutes

WHILE J<=m

```
                    if img (J,I) =1ir JJ=1.
                    img _mod (1:nf, randomas (I);+1:nf);
                    J = nf-randomas (I)+1:nf);
                    JJ = 2;
                ELSE IF img(J,I)==1
                    Img_mod(J:J+nf-1)=f(1:nf)
J = J+nf;
ELSE img_mod(j:j+nf-1,I)=t(1:nt)
                END
            END
        END
END
Img _mod1 (1:m,1:n)=img_mod(1:m,1:n)
Figure
 imshow(img_mod1);
```

2. TIRIAMOJI DALIS

2.1 PROGRAMINĖ ĮRANGA

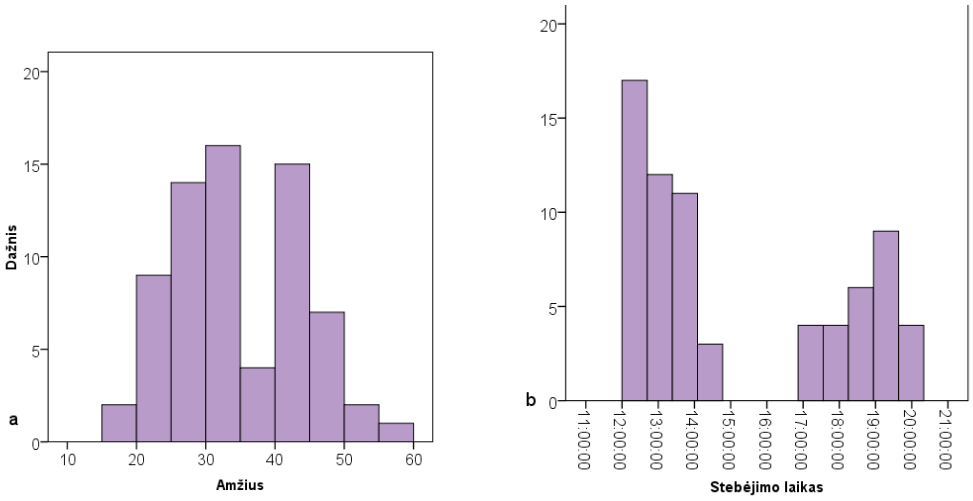
Slaptų atsitiktinai parinktų abėcėlės raidžių, simbolių bei skaičių binarinių vaizdų kombinacijai sudaryti pasirinktas Adobe Photoschop CC programinis paketas (1 priedas).

Pagal kompiuterio ekrano skiriamąją gebą Matlab programine įranga sudaryti užkoduoti vaizdai, kurių parametrai 550x1000 taškų (pixelių). Užkoduota slapta informacija vizualizuota ir dekoduota Adobe Flasch Profesional CS6 programine įranga. Šio programinės įrangos pagrindiniai privalumai yra platus vaizdų animacijos spektras bei interaktyvus virpinimo dažnio parinkimas.

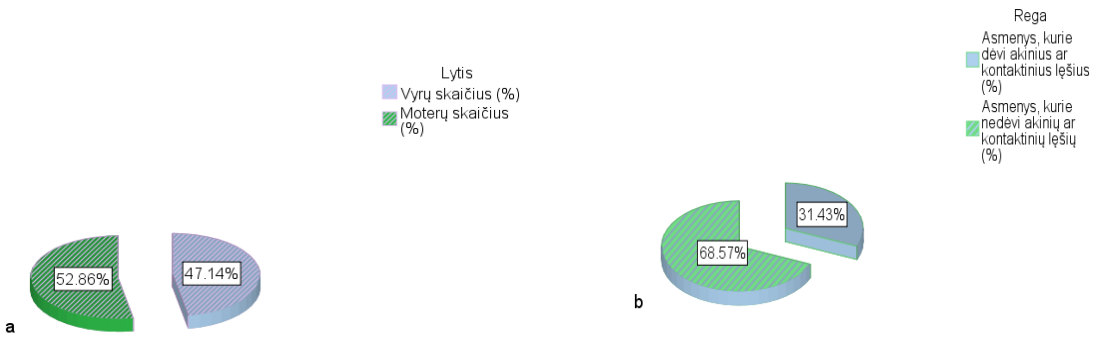
Rezultatų analizei pasirinktas SPSS programinis paketas. Pagrindinis šio programinio paketo privalumas yra platus šiuolaikinių statistinės analizės metodų pasirinkimas ir duomenų analizės vizualizavimo priemonių gausa.

2.2 DUOMENYS

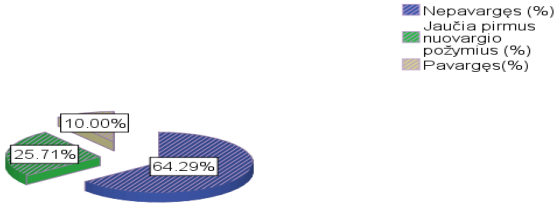
Duomenų analizei ir interpretacijai sudaryta paprastoji atsitiktinė 70 respondentų imtis. Fiksuoti diskretieji kiekybiniai kintamieji (amžius, laikas, 2.1 pav.), nominalieji kintamieji (lytis, rega, 2.2 pav.) bei tvarkos kintamieji (fizinė būsena, 2.3 pav.). Tyrimo tikslas nustatyti optimalius šifravimo simbolius, kurie naudojami dinaminėje vizualinėje kriptografijoje. Minėtam tikslui pasiekti sprendžiami šie uždaviniai: 1) nustatyti veiksnius įtakojančius raidžių (simbolių) atpažinimo dažnį; 2) suskirstyti abėcėlės raides bei tam tikrus simbolius į tinkamas naudoti, vidutiniškai tinkamas naudoti bei apskritai netinkamas naudoti (raides, kurių dekodavimo algoritmas yra labiausiai priklausomas nuo asmens charakteristikos).



2.1 pav. Juostinė diagrama: a) amžius, b) stebėjimo laikas



2.2 pav. Skritulinė diagrama: a) rega, b) lytis



2.3 pav. Fizinės būklės nusakymo skritulinė diagrama

2.3. PARAMETRINIO MODELIO TIKRINIMAS

2.3.1 SĄRYŠIO, TARP ATSKIROS RAIDĖS ATPAŽINIMO BEI AMŽIAUS, TIKRINIMAS

Kaip jau minėta 2.2 dalyje, vienas iš pagrindinių mus dominančių uždavinių – nustatyti ryšį tarp raidžių atpažinimo bei asmenį charakterizuojančių veiksnių. Todėl šioje dalyje išsamiau panagrinėsime dviejų kiekybinių kintamųjų: amžiaus bei atskiros raidės atpažinimo dažnį (matuojamą kadrais per sekundę).

Galima teigti, kad analizuojant kiekybinių rodiklių tarpusavio sąryšį, išskiriami trys pagrindiniai veiksniai [28]:

- ryšio stiprumo laipsnis,
- forma,
- tendencija.

Pirmiausiai apskaičiuosime imties koreliacijos koeficientą r. Tačiau tam, kad imties koreliacijos koeficientas tiksliai nusakytų sąryšį, patikrinsime, ar mūsų nagrinėjamų kiekybinių rodiklių (amžiaus bei raidžių atpažinimo dažnio) matavimo poros, tenkina būtiną prielaidą, kad rodiklių jungtinis skirstinys yra dvimatis normalusis.

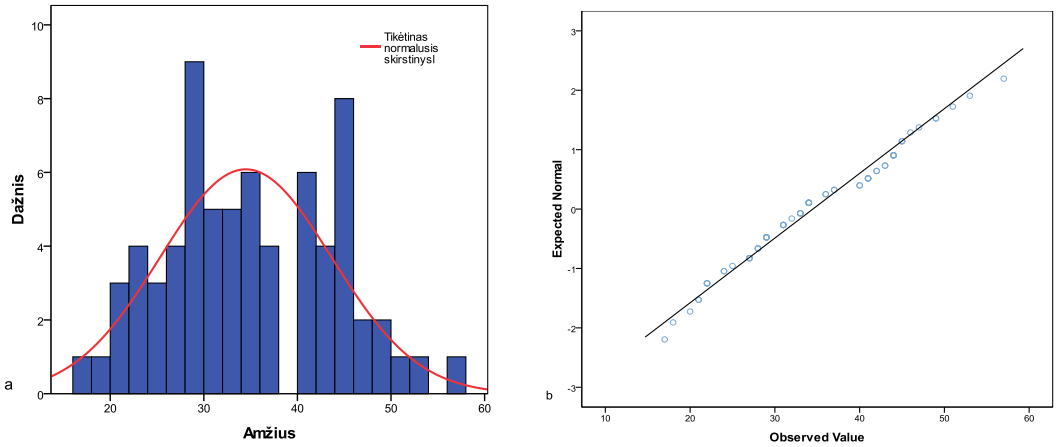
Patikrinti, ar mūsų nagrinėjami atsitiktiniai dydžiai pasiskirstę pagal normalųjį skirstinį,

$$w(x) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left[-\frac{(x-m)^2)}{2\sigma^2}\right];$$

čia m- vidurkis, σ – dispersija.

naudosime tris kriterijus:

- vizualinė patikrą (2.4 pav.),
- patikrinsime, ar *z* reikšmės yra tarp $\mp 1{,}96$,
- apskaičiuosime Shapiro Wilk kriterijų apie normalųjį pasiskirstymą.



2.4 pav. a Amžiaus histograma; b. kvantilinis grafikas

Nulinei hipotezei H_0: „kintamojo skirstinys pasiskirstęs pagal normalųjį dėsnį“ su alternatyva H_a: „kintamojo skirstinys nėra pasiskirstęs pagal normalųjį dėsnį“ naudosime Shapiro-Wilk kriterijų (2.1 lent).

Shapiro-Wilk kriterijaus statistika nusakoma lygtimi [24]:

$$W = \frac{(\sum_{t=2}^{n} a_t y_t)^2}{\sum_{t=1}^{n}(x_t - \overline{y})^2} \qquad (2.1)$$

čia n – stebėjimų skaičius, y_t- surūšiuotos imties x_t reikšmės $(y_1 < y_1 < \cdots < y_n)$, a_t – koeficientai.

Paskaičiuosime ir Kolmogorov-Smirnov kriterijų (2.1 lent.), tačiau jis nėra tikslus, jei imties tūris mažesnis nei 200, todėl šiuo kriterijumi nesivadovausime. Iš lentelės 2.1 matyti, kad reikšmė *p=0,218>0,05,* vadinasi negalime atmesti H_0 hipotezės.

2.1 lentelė. Hipotezės apie amžiaus normalųjį pasiskirstymą tikrinimas

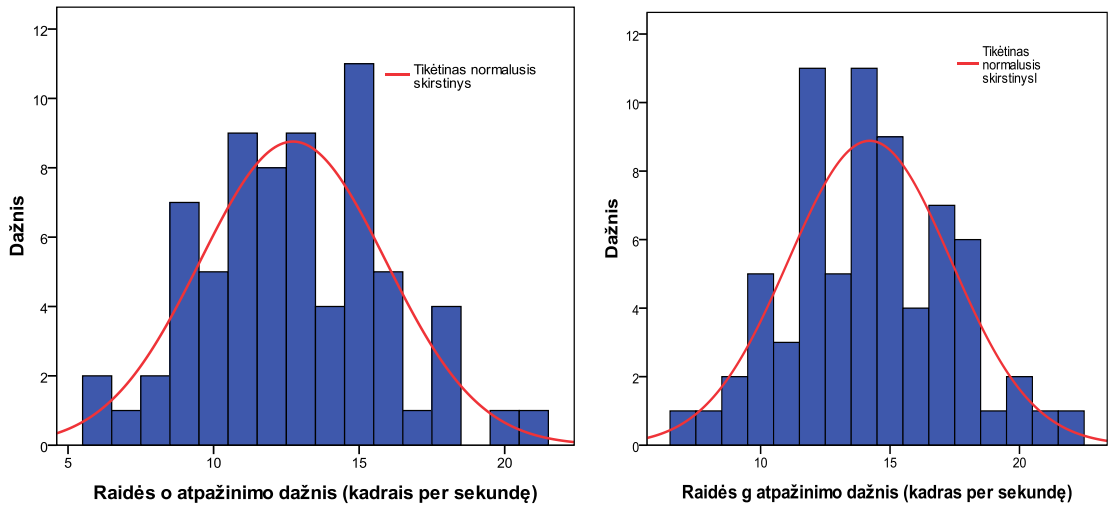
	Kolmogorov-Smirnov			Shapiro-Wilk		
	Statistic	Df	Sig.	Statistic	Df	Sig.
Amžius	.107	70	.046	.977	70	.218

Taip pat galime teigti, kad *z* reikšmės neviršija leistinų ribų ($\pm 1{,}96$): $z_1 = 0{,}72, z_2 = 1{,}15$ (2.2 lent). Kvantilinio grafiko reikšmių išsidėstymas arti arba ant tiesės taip pat byloja apie artimą normaliajam atsitiktinių reikšmių pasiskirstymą (2.4 b pav.).

2.2 lentelė. Amžiaus eksceso ir asimetrijos reikšmės

Amžius	Statistic	Std. Error
Skewness	.208	.287
Kurtosis	-.655	.566

Patikrinti abėcėlės raidžių atpažinimo pasiskirstymą yra kur kas sudėtingiau. Atskirų abėcėlės raidžių bei ženklų atpažinimo pasiskirstymas (net to paties asmens) gana skirtingas, todėl pirmiausiais išsamiau panagrinėsime (vėliau aptarsime ir tarpusavio ryšį) tik tas raides, kurių atpažinimo pasiskirstymas normalusis (2.3 lent.).



2.5 pav. Raidžių g ir o atpažinimo dažnių histograma

Kaip matyti iš lentelės (2.3 lent.) ir 2 priedo daugiausiai įrodymų apie atsitiktinio dydžio (raidės atpažinimą) normalųjį pasiskirstymą turi raidės g bei o (2.5 pav.). Kadangi neturime pagrindo prieštarauti, kad raidžių atpažinimo dažnis (a, x, y, z,!,q, F, f, n, k, g, G, H, h, A, B, i, d, Y, Z, u, o, v, N, s, S, m, t, C, X) yra pasiskirstęs pagal normalųjį dėsnį (2.3 lent.), galime nagrinėti tiesinį sąryšį tarp amžiaus bei minėtų raidžių. Sąryšiui nusakyti apskaičiuosime Pirsono koreliacijos koeficientą *r*, kuris skaičiuojamas pagal šią formulę [27]:

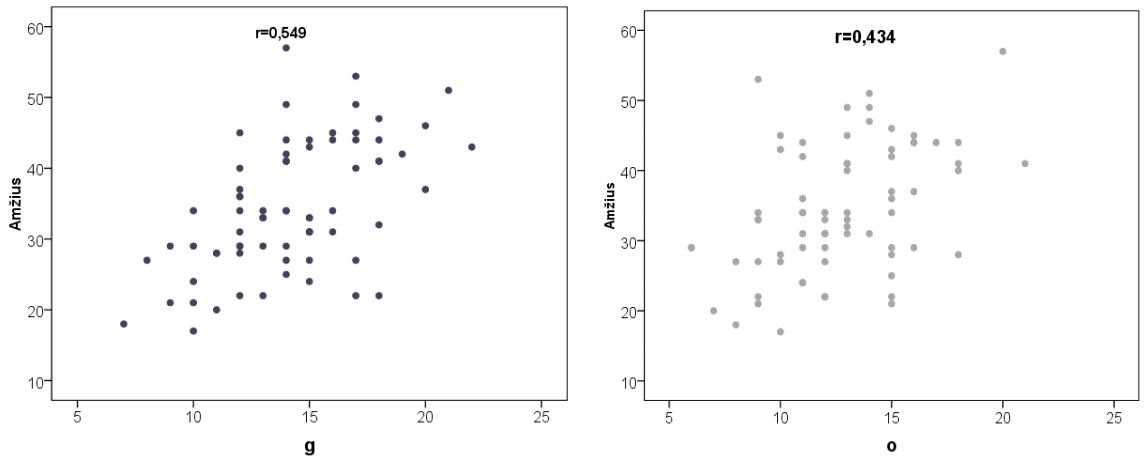
$$r = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2 \sum_{i=1}^{m}(y_i - \bar{y})^2}}; \qquad (2.2)$$

čia $\bar{x}$ ir $\bar{y}$ – imčių vidurkiai.

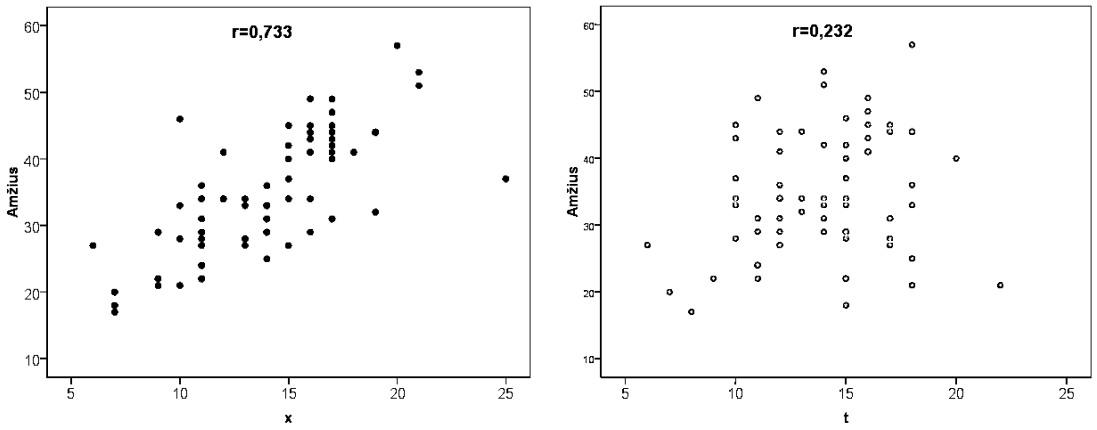
2.3 lentelė. Raidžių atpažinimo hipotezės apie normalųjį pasiskirstymą tikrinimas

	Kolmogorov-Smirnov[a]			Shapiro-Wilk				Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	Df	Sig.		Statistic	Df	Sig.	Statistic	Df	Sig.
x	.108	70	.043	.980	70	.307	F	.108	70	.043	.973	70	.128
y	.096	70	.184	.979	70	.304	f	.094	70	.200	.969	70	.079
z	.102	70	.068	.981	70	.376	G	.114	70	.024	.975	70	.186
!	.112	70	.028	.966	70	.058	g	.088	70	.200	.986	70	.608
q	.094	70	.200*	.983	70	.452	H	.115	70	.023	.977	70	.212
n	.095	70	.190	.973	70	.135	h	.115	70	.023	.977	70	.212
k	.117	70	.019	.976	70	.187	A	.080	70	.200	.980	70	.333
d	.104	70	.059	.973	70	.136	i	.103	70	.065	.977	70	.223
A	.093	70	.200*	.974	70	.146	b	.095	70	.189	.982	70	.396
B	.093	70	.200*	.974	70	.146	S	.108	70	.041	.972	70	.124
C	.093	70	.200*	.974	70	.146	S	.109	70	.040	.976	70	.202
Y	.132	70	.004	.970	70	.090	A	.140	70	.002	.979	70	.279
N	.122	70	.011	.976	70	.204	a	.098	70	.091	.969	70	.084
o	.090	70	.200	.983	70	.443	t	.129	70	.005	.978	70	.264
u	.114	70	.024	.979	70	.284	X	.132	70	.004	.972	70	.112
Z	.129	70	.006	.970	70	.094	m	.087	70	.200	.981	70	.380

Vizualizavus tiesinio sąryšio stiprumą (2.6 pav.), matyti, kad raides g ir o sieja vidutinio stiprumo teigiamas koreliacinis ryšys (r>0,3). Stipriausias sąryšis sieja raidės z atpažinimą ir asmens amžių (r>0,6), o silpniausias sąryšis tarp raidės t atpažinimo ir amžiaus (2.7 pav.).



2.6 pav. Monotoninis ryšis tarp raidžių o, g bei amžiaus



2.7 pav. Monotoninis ryšis tarp raidžių x, t ir amžiaus

Raidžių atpažinimą bei amžių nusako stiprus, teigiamas tiesinis monotoninis ryšis (2.4 lent.) bei vidutinio stiprumo teigiamas monotoninis sąryšis (2.5 lent.) ir tik raidę t bei amžių sieja silpnas sąryšis (2.5 lent.).

2.4 lentelė. Pirsono koreliacijos koeficiento reikšmės tarp amžiaus bei raidžių atpažinimo

		x	z	n	k	D	H	B	C	h	A	i	a	b	S
Amžius	Pearson Correlation	.733	.763	.602	.671	.607	.634	.646	.646	.634	.686	.652	.602	.662	.628
	Sig. (2-tailed)	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.000	.00	.000	.000

2.5 lentelė. Pirsono koreliacijos koeficiento reikšmės tarp amžiaus bei raidžių atpažinimo

		!	G	q	Z	F	f	X	m	t	g	u	o	Y	y	N
Amžius	Pearson Correlation	.484	.512	.547	.377	.548	.466	.384	.570	.232	.549	.348	.434	.409	.544	.315
	Sig. (2-tailed)	.000	.000	.000	.001	.000	.000	.001	.000	.054	.000	.003	.000	.00	.00	.008

Tačiau prieš galutinai patvirtinant ryšį tarp asmenų amžiaus bei jų reakcijos atpažįstant raides, būtina tikrinti r patikimumą. Patikrinsime hipotezę [28]: H_0: „$\rho = 0$“ su alternatyva H_a: „$\rho \neq 0$“ (ρ −populiacijos įvertis). Tam pasitelksime t-kriterijaus su n-2 laisvės laipsnių statistiką:

$$t = \frac{r\sqrt{n-2}}{\sqrt{1-r^2}} \tag{2.3}$$

Rezultatų išklotinėje (3 priedas) matyti, kad $p = 0$ <0,01, vadinasi galime atmesti H_0: „$\rho = 0$“ hipotezę. Galime daryti išvadą, kad kuo vyresnis asmuo, tuo didesnis virpinimo dažnis yra reikalingas slaptai informacijai dekoduoti.

Raidžių a, b, x, y, z, !, q, F, f, n, k, g, G, H, h, A, B, i, d, Y, Z, u, o, v, N, s, S, m, t, C, X atpažinimo dažnis yra tiesiogiai susijęs su asmens amžiumi. Kita vertus, nagrinėti likusių abėcėlės raidžių priklausomybės nuo amžiaus (pagal Pirsono koreliacijos koeficientą) neturime pakankamai įrodymų.

2.3.2 SĄRYŠIS TARP RAIDŽIŲ A, a, B, b, H, h, x, z, S BEI ASMENS LYTIES

2.3.1 skyriuje patvirtinome, kad tam tikrų dekoduotų raidžių atpažinimą bei amžių sieja stiprus koreliacinis ryšys. Panagrinėkime stipriu teigiamu koreliaciniu sąryšiu su amžiumi susietų raidžių (A, a, B, b, H, h, x, z, S) ryšį su kategoriniu kintamuoju – lytimi. Ryšiui tarp dviejų nepriklausomų imčių nustatyti, naudosime porinių imčių t kriterijų (paired sample t-test) su n-1 laisvės laipsnių. t – kriterijaus statistika nusakoma lygtimi:

$$t = \frac{\sum d}{\sqrt{\frac{n(\sum d^2) - (\sum d)^2}{n-1}}}; \tag{2.4}$$

čia *n*-imties dydis, *d* – skirtumas tarp dviejų imčių.

Dviejų imčių nepriklausomumo t – kriterijus (independent samples t test) rezultatai yra reikšmingi, kai tenkinamo šios prielaidos [24]:

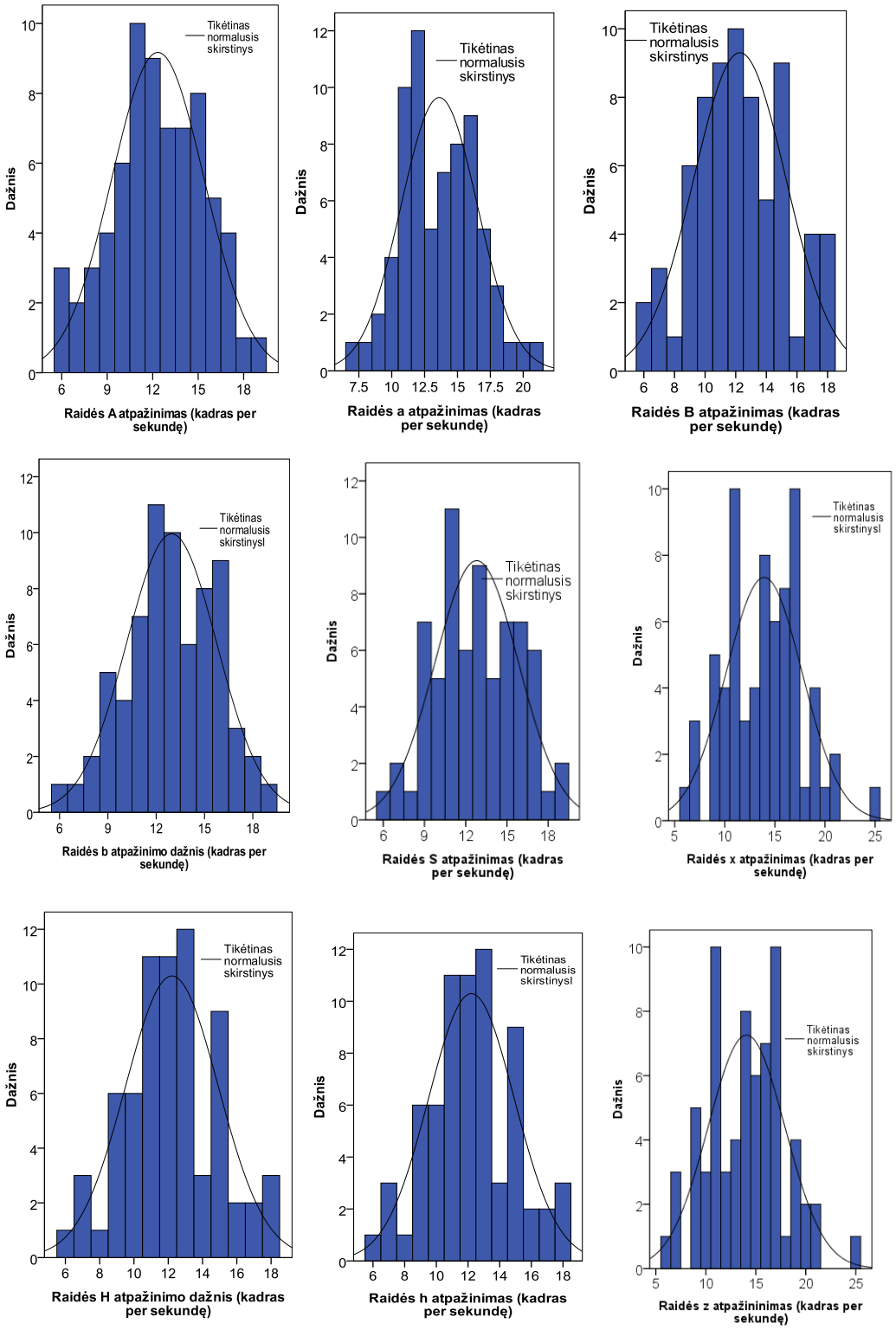
- Priklausomas kintamasis (raidės atpažinimo dažnis) yra kiekybinis;
- Nepriklausomas kintamasis yra kategorinis (vyras, moteris);
- Imtys tarpusavyje nepriklausomos;
- Nėra išskirčių;
- Priklausomo kintamojo (raidės A, a, B, b, H, h, x, z, S atpažinimo dažnis) skirstinys yra normalusis (2.8 pav.);
- Tenkinama homogeniškumo sąlyga (2.7 lentelė).

Pagal Levene kriterijų (2.7 lent.) galime atmesti hipotezę H_0: „ apie imčių skirstinio lygumą“, nes $p_A = 0{,}473 > 0{,}05,\ p_a = 0{,}683 > 0{,}05,\ p_B = 0{,}818 > 0{,}05, p_h = p_H = 0{,}981 > 0{,}05, p_x = 0{,}181 > 0{,}05, p_z = 0{,}215 > 0{,}05, p_S = 0{,}297 > 0{,}05.$

Levene kriterijus naudojamas tikrinti hipotezę: H_a: „ $\sigma_1^2 = \sigma_2^2 = \cdots \sigma_k^2$" su alternatyva $\sigma_i^2 \neq \sigma_j^2$ nors vienai porai *(i ,j).* Kriterijaus statistika apibrėžiama [6]:

$$W = \frac{(N-k)\sum_{i=1}^{k} N_i(\bar{Z}_{i.} - \bar{Z}_{..})^2}{(k-1)\sum_{i=1}^{k}\sum_{j=1}^{N_i}(Z_{ij} - \bar{Z}_{i.})^2}; \tag{2.5}$$

čia $Z_{ij} = |Y_{ij} - \bar{Y}_{i.}|$, kai $\bar{Y}_{i.}$ – yra *i-tosios* tarpinės grupės vidurkis; $\bar{Z}_i$ – grupių Z_{ij}vidurkis; $\bar{Z}_{..}$ – Z_{ij} sumos vidurkis.



2.8 pav.. Raidžių A, a, B, b, H, h, S, x, y pasiskirstymas

2. 6 lentelė. Levene kriterijus tarp lyties grupių ir raidžių atpažinimo

	Levene Statistic	df1	df2	Sig.		Levene Statistic	df1	df2	Sig.		Levene Statistic	df1	df2	Sig.
A	.520	1	68	.473	H	.611	1	68	.437	x	.002	1	68	.181
a	.168	1	68	.683	H	.611	1	68	.437	z	.000	1	68	.215
B	.053	1	68	.818	B	.001	1	68	.981	S	.000	1	68	.297

Pagal (2.4) formulę apskaičiuotos parametrų reikšmės rezultatų išklotinėje (2.7 lent.) rodo, kad dekoduojant simbolius, vyrai atpažįsta raides virpinant užkoduotus simbolius (raides A, a, B, b, H, h, x, z, S) mažesniu dažniu nei moterys. Taip pat galime atmesti hipotezę H_0: „skirstiniai yra lygūs“ su pasikliautinuoju intervalu $\alpha = 0{,}05$ (2.8 lent.), $p_B = 0{,}003 < 0{,}01, p_H = p_h = 0{,}001 < 0{,}01, p_x = p_z = p_A = p_a = p_b = 0{,}00 < 0{,}01$.

2. 7 lentelė. Raidžių atpažinimo dažnio tikrinimas tarp lyties grupių

	Lytis	N	Mean	Std. Deviation	Std. Error Mean		Lytis	N	Mean	Std. Deviation	Std. Error Mean
B	Vyrai	33	11.15	2.906	.506	b	Vyrai	33	12.39	2.999	.522
	Moterys	37	13.27	2.755	.453		Moterys	37	15.00	2.925	.481
H	Vyrai	33	11.15	2.751	.479	A	Vyrai	33	10.88	2.966	.516
	Moterys	37	13.16	2.328	.383		Moterys	37	13.65	2.497	.410
h	Vyrai	33	11.15	2.751	.479	a	Vyrai	33	12.33	2.570	.447
	Moterys	37	13.16	2.328	.383		Moterys	37	14.76	2.712	.446
x	Vyrai	33	11.76	3.103	.540	S	Vyrai	33	11.39	2.806	.488
	Moterys	37	15.86	3.326	.547		Moterys	37	14.05	2.707	.445
z	Vyrai	33	11.70	2.995	.521						
	Moterys	37	16.19	3.256	.535						

2. 8 lentelė Raidžių atpažinimo dažnio tikrinimas tarp lyties grupių. t- statistika

	Levens test of equality	F	Sig	T	Df	Sig.(2-tailed)		Levens test of equality	F	Sig	t	df	Sig.(2-tailed)
B	Equal variances assumed	.053	.818	-3.130	68	.003	b	Equal variances assumed	.001	.981	-3.677	68	.000
H	Equal variances assumed	.611	.437	-3.311	68	.001	A	Equal variances assumed	.520	.473	-4.241	68	.000
h	Equal variances assumed	.611	.437	-3.311	68	.001	a	Equal variances assumed	.168	.683	-3.825	68	.000
x	Equal variances assumed	.002	.960	-5.322	68	.000	S	Equal variances assumed	.000	.994	-4.034	68	.000
z	Equal variances assumed	.000	.994	-5.983	68	.000							

Galime daryti išvadą, kad vyrai virpinamą dekoduojamą vaizdą (raides a, A, B, b, H, h, x, z, S) atpažįsta, virpinant jį mažesniu kadrų per sekundę skaičiumi nei moterys. 4 priede matyti, kad absoliučiai visų abėcėlės raidžių, kurių pasiskirstymas yra normalusis, atpažinimo dažnis statistiškai skiriasi pagal lytį.

Vadinasi, su pasikliautinuoju intervalu $\alpha = 0{,}01$ galime teigti, kad abėcėlės raidžių (A, a, H, h, B, b, x, z, S) atpažinimą sieja ne tik stiprus monotoninis ryšys su amžiumi (kuo jaunesnis asmuo, tuo mažesnis virpinimo dažnis reikalingas jam atpažįstant raides), bet ir egzistuoja tam tikras ryšis tarp gebėjimo atpažinti dinaminės vizualinės kriptografijos metodu užkoduotą slaptą informaciją ir lyties.

Nors negalime išmatuoti ar nusakyti ryšio tarp lyties grupių, tačiau galime teigti, kad asmens lytis turi įtakos virpinimo dažnio parinkimui.

2.3.3 REGOS ĮTAKA RAIDŽIŲ A, a, B, b, H, h, x, z, S ATPAŽINIMUI

Darome prielaidą, kad stipriu sąryšiu su amžiumi ir lytimi susijusių raidžių (A, a, B, b, H, h, x, z, S) atpažinimą lemia taip pat ir rega, t.y. asmens dėvėjimas akinius ar kontaktinius lęšius.

2. 9 lentelė. Raidžių atpažinimo dažnio ryšis tarp regos grupių

	Rega	N	Mean	Std. Deviation	Std. Error Mean		Rega	N	Mean	Std. Deviation	Std. Error Mean
B	0*	48	11.92	3.141	.453	b	0*	48	13.33	3.435	.496
	1**	22	13.05	2.572	.548		1**	22	14.73	2.492	.531
H	0*	48	11.96	2.858	.413	A	0*	48	11.90	3.263	.471
	1**	22	12.77	2.329	.496		1**	22	13.32	2.276	.485
h	0*	48	11.96	2.858	.413	a	0*	48	13.44	3.031	.438
	1**	22	12.77	2.329	.496		1**	22	14.00	2.600	.554
x	0*	48	13.17	3.761	.543	S	0*	48	12.31	3.109	.449
	1**	22	15.59	3.432	.732		1**	22	13.86	2.660	.567
z	0*	48	13.33	3.817	.551						
	1**	22	15.68	3.469	.740						

* 0 – asmuo nedėvi akinių ar kontaktinų lęšių, ; * *1 – asmuo dėvi akinius ar kontaktinus lęšius asmuo

Rezultatai (2.9 lent.) patvirtina, kad asmenys, kurie nedėvi akinių ar kontaktinių lęšių atpažįsta raides prie mažesnio virpinimo dažnio nei tie, kurie juos dėvi. Nedėvinčių akinių asmenų raidės atpažinimo virpinimo dažnio vidurkių suma ($\mu_1 = 11{,}92 < \mu_2 = 13{,}05;\ \mu_3 = 11{,}96 < \mu_4 = 12{,}77;\quad \mu_5 = 13{,}33 < \mu_6 = 17{,}73;\ \mu_7 = 11{,}90 < \mu_8 = 13{,}32;\ \mu_9 = 13{,}44 < \mu_{110} = 14{,}00, \mu_{11} = 13{,}17 < \mu_{12} = 15{,}59, \mu_{13} = 13{,}33 < \mu_{14} = 15{,}68, \mu_{15} = 12{,}31 < \mu_{16} = 13{,}86$) yra mažesnė.

Pagal 2.9 lent. reikšmes, darome prielaidą kad stebėti asmenys, kurie dėvi akinius atpažįsta raides (A, a, B, b, H, h, x, z, S) virpinant jas mažesniu kadrų per sekundę dažniu.

2. 10 lentelė. Raidžių atpažinimo dažnio ryšis tarp regos grupių

		t	Df	Sig. (2-tailed)	Mean Difference	Std. Error Difference
H	Equal variances assumed	-1.169	68	.246	-.814	.697
h	Equal variances assumed	-1.169	68	.246	-.814	.697
A	Equal variances assumed	-1.846	68	.069	-1.422	.771
a	Equal variances assumed	-.752	68	.455	-.563	.748
B	Equal variances assumed	-1.473	68	.145	-1.129	.766
b	Equal variances assumed	-1.668	68	.100	-1.189	.713

Tačiau pagal nepriklausomų imčių t- kriterijų raidžių (A, a, B, b, H, h) atpažinimo sąryšį su asmens rega, galime atmesti hipotezę: H_0: „nedėvinčių akinių asmenų raidės atpažinimo skirstinys yra lygus dėvinčių asmenų skirstiniui“ su alternatyva H_a: „nedėvinčių akinių asmenų raidės atpažinimo pasiskirstymas nėra lygus dėvinčių asmenų pasiskirstymui“ (2.10 lent.), nes $p_H = p_h = 0{,}246 > 0{,}05,$ $p_A = 0{,}069 > 0{,}05, p_a = 0{,}455 > 0{,}05, p_a = 0{,}145, p_b = 0{,}1 > 0{,}05.$

Antra vertus, raidžių (x, z, S) atpažinimas susijęs ne tik su asmens amžiumi, lytimi, bet ir rega. Galime teigti, kad asmenys, kurie nedėvi akinių ar kontaktinių lęšių atpažįsta raides (x, z, S) virpinant jas mažesniu dažniu nei tie, kurie dėvi. Rezultatų išklotinė (2.11 lent.) patvirtina ($p_x = 0{,}012 < 0{,}05, p_S = 0{,}047 < 0{,}05, p_z = 0{,}017 < 0{,}05$), kad statistiškai daugiau asmenų, kurie dėvi akinius ar kontaktinius lęšius atpažįsta dekoduojamas raides (x, z, S) prie mažesnio virpinimo dažnio su pasikliautinuoju intervalu $\alpha = 0{,}05.$

2. 11 lentelė. Raidžių atpažinimo dažnio ryšis tarp regos grupių t – kriterijus.

		Levene's Test for Equality of Variances		t-test for Equality of Means		
		F	Sig.	t	df	Sig. (2-tailed)
x	Equal variances assumed	1.828	.181	-2.571	68	.012
S	Equal variances assumed	1.104	.297	-2.023	68	.047
z	Equal variances assumed	1.565	.215	-2.457	68	.017

2.3.4 FIZINĖS BŪSENOS ĮTAKA RAIDŽIŲ A, a, B, b, H, h, x, z, S ATPAŽINIMUI

Fizinės būsenos įtakos tikrinimui pasitelksime Tiukei kriterijų (angl. Tukey test), kuris yra tikslus tuomet, kai grupių imčių dydžiai nėra vienodi. Tokiu būdu apskaičiuosime visus

įmanomus porų (pavargęs, nepavargęs bei jaučia pirmus nuovargio požymius) skirtumus tuo pat metu.

Pasitelksime ANOVA tam, kad surastume grupių vidurkius, kurie reikšmingai skiriasi vieni nuo kitų. Tiukei kriterijus yra paremtas stjudentizuotu pasiskirstymu (q) ir naudojamas, kai tikrinamų grupių standartiniai nuokrypiai yra nehomogeniški (2.12 lent.).

Porų vidurkių palyginimui naudojamos vios galimos porų sekos:

$$\{\mu_i - \mu_j\} \tag{2.6}$$

Stjudentizuotas q pasiskirstymas skaičiuojamas pagal formulę [6]:

$$q_{r,\upsilon} = \frac{\omega}{s}; \tag{2.7}$$

čia $y_1, \dots, y_r$ – nepriklausomi stebėjimai pasiskirstę pagal normalųjį dėsnį, ω – aibės $y_1, \dots y_r$ eilė, ν – laisvės laipsniai, s^2 yra dispersijos σ^2 įvertis.

Tiukey kriterijaus pasikliautinasis intervalas visiems porų palyginimams [6]:

$$\bar{y}_i - \bar{y}_j \pm \frac{1}{\sqrt{2}} q_\alpha; r, N - r, \hat{\sigma}_\epsilon \sqrt{\frac{2}{n}}, i, j = 1, \dots, r; i \neq j \tag{2.8}$$

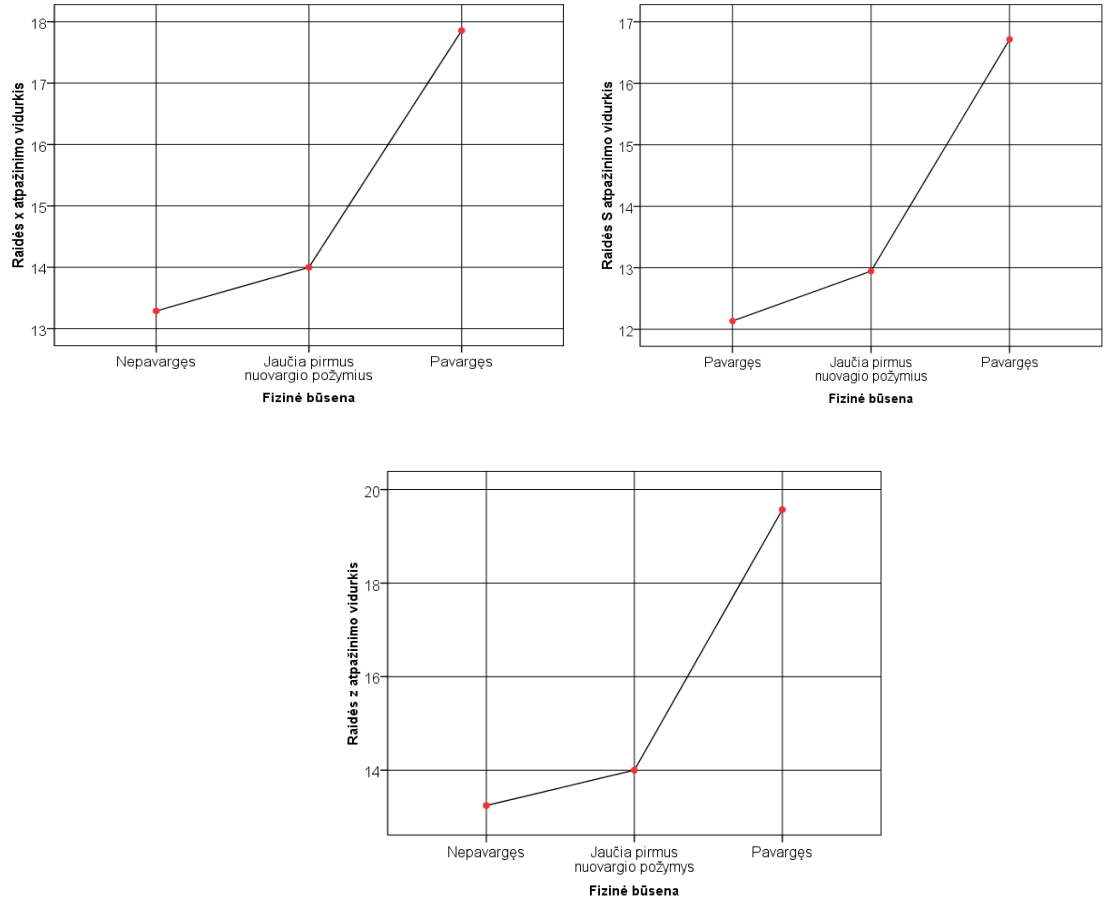
Pagal pateiktus rezultatus matyti (2.9 pav.), kad raidžių S, x, z atpažinimui didelę įtaka daro asmens fizinė būsena, t.y. ar jis jaučiasi labai pavargęs. Jei asmuo jaučia nuovargį, raidės atpažinimo dažnio kreivė dramatiškai kyla į viršų, t.y. kuo labiau pavargęs jaučiasi asmuo, tuo dekoduotos raidės atpažinimo dažnis didesnis. Palyginus fizinių grupių (pavargęs, nepavargęs bei jaučia pirmus nuovargio simptomus) vidurkių sumas bei jų statistikos reikšmingumą (2.12 lent.), matyti, kad yra (2.9 pav.) ryškus skirtumas tarp visų trijų grupių (pavargęs, nepavargęs ar jaučia pirmus nuovargio ženklus). Tačiau ypač ryškus skirtumas tarp grupių: jaučiasi pavargęs ir jaučia pirmus nuovargio ženklus.

2. 12 lentelė. Raidžių x, z, S atpažinimo homogeniškumo statistika

	Levene Statistic	df1	df2	Sig.
x	2.185	2	67	.120
z	1.644	2	67	.201
S	2.332	2	67	.105

2. 13 lentelė. Raidžių x, z, S statistikos tarp fizinės būsenos grupių

		Sum of Squares	Df	Mean Square	F	Sig.
x	Between Groups	126.541	2	63.271	4.850	.011
z	Between Groups	242.617	2	121.309	10.447	.000
S	Between Groups	127.627	2	63.813	8.358	.001



2.9 pav. Raidžių x, z S atpažinimo dažnių vidurkių skirtumai pagal fizinę būklę

2.3 skyriaus išvados

Pagal gautus statistinius rezultatus galime prieiti prie išvados, kad pagal Gauso skirstinį pasiskirstęs raidžių ir simbolio (x, y, z, q, n, k, d, A, B, C, f, F, g, G, h, H, A, i, b, S, s, a, m, t, X, Y, Z, u, o, v, N) dekodavimo atpažinimas susijęs su šiais veiksniais:

- Raidžių (x, y, z, n, k, d, B, A, H, h, C, i ,b, S, a) atpažinimas su amžiumi yra susietas stipriu, teigiamu monotoniniu sąryšiu. Kuo jaunesnis asmuo, tuo mažesnis virpinimo dažnis yra reikalingas dekoduoti šias slaptas raides;

- Stipriu, teigiamu koreliaciniu sąryšiu su amžiumi susietų raidžių atpažinimą stipriai įtakoja asmens lytis. Vyrai dekoduojamus vaizdus (raides x, y, z, n, k, d, B, A, H, h, C, i ,b, S, a) atpažįsta prie mažesnio virpinimo dažnio nei moterys;
- Užkoduotų raidžių x, z, S dekodavimą sieja statistinis ryšys su rega (akinių dėvėjimu). Asmuo atpažįsta mažesniu dažniu virpinamame paveiksle užkoduotas minėtas raides x, z, S, jei nedėvi akinių ar kontaktinių lęšių.
- Dinaminės vizualinės kriptografijos metodu dekoduojamam slaptų raidžių x, z, S atpažinimui turi įtakos visi nagrinėti asmenį charakterizuojantys veiksniai: lytis, rega bei amžius.
- Fizinė būsena taip pat įtakoja asmens gebėjimą atpažinti besikeičiančius vaizdus. Raidžių x, z, S atpažinimo vidurkių palyginimas patvirtino, kad kuo asmuo labiau pavargęs, tuo labiau kyla kreivė, iliustruojanti raidės atpažinimą.

2.4 RYŠYS TARP RAIDŽIŲ, KURIOMS NEGALIME PATVIRTINTI NORMALIOJO PASISKIRSTYMO, IR AMŽIAUS

Kaip jau minėjome, negalime tvirtinti, kad raidžių (E, T, U, R ,M, O,W,L, Q,J, F, D,K, e, j, c,?, kvadratas, M) atpažinimo skirstinys yra normalusis. Todėl sąryšiui tarp amžiaus bei raidžių atpažinimo panagrinėsime Spirmano koreliacijos koeficientą, kurio taikymui naudojama prielaida, kad jungtinis raidžių atpažinimo bei amžiaus skirstinys yra tolygusis. Priešingai nei Pirsono koreliacijos koeficientas, Spirmano koreliacijos koeficientas yra mažiau jautrus išskirtims.

Tegul turime kiekybinio kintamojo modelį (X,Y), atsitiktinę imtį $(x_1, y_1), (x_2, y_2), \dots, (x_n, y_n)$. Imtyje esančios reikšmės pakeičiamos rangais. Gaunamos rangų poros $(R_{x1,}R_{y1}), (R_{x1,}R_{y1}), \dots, (R_{xn,}R_{yn})$. Spirmano koreliacijos koeficientas apskaičiuojamas pagal lygtį [28]:

$$r_s = \frac{\sum_{i=1}^{n} R_{x1} - (n+1)/2(R_{yi} - (n+1)/2)}{(\sum_{i=1}^{n} R_{xi} - (n+1)/2)^2 \sum_{i=1}^{n}(R_{yi} - (n+1)/2^2)^{1/2}}; \quad (2.9)$$

čia R_{xi} yra x_i rangas, o R_{yi} - y_i rangas.

Tam, kad nusakytume sąryšį tarp likusių abėcėlės raidžių bei amžiaus, paskaičiuosime Spirmano koreliacijos koeficiento reikšmes šių raidžių: E, T, U, R ,M, r, O,W,L, Q,J, D,K, e, j, c,?, kvadratas ir amžiaus.

2.14 lentelė. Spirmano koreliacijos koeficiento reikšmės

			Amžius	E	T	U	R	L	Q	Kvad
Spearman's rho	1.000	.686**	.686**	.686**	.648**	.703**	.673**	.329**	.312**	.357**
	.	.000	.000	.000	.000	.000	.000	.000	.002	.001

Spirmano koreliacijos koeficiento reikšmės taip pat byloja apie daugumos raidžių stiprų ir vidutinio stiprumo sąryšį (2.14 lent., 2.15 lent.) ir tik tris abėcėlės raides (e, D, K) bei amžių sieja silpnas ($r_s < 0{,}3$) ryšis (2.14 lent.).

2.15 lentelė. Spirmano koreliacijos koeficiento reikšmės

			v	W	L	R	J	c	O	?	I	Kvad
Spearman's rho	Amžius	Correlation Coefficient	.526**	.544**	.504**	.504**	.334**	.364**	.434**	.329**	.312**	.357**
		Sig. (2-tailed)	.000	.000	.000	.000	.002	.000	.000	.000	.002	.001

2.16 lentelė. Spirmano koreliacijos koeficiento reikšmės

			Amžius	e	D	K
Spearman's rho	Amžius	Correlation Coefficient	1.000	.294*	.212	.203
		Sig. (2-tailed)	.	.013	.078	.092

Matyti, kad sąryšis statiškai reikšmingas, kai pasikliautinasis intervalas $\alpha = 0{,}01$ (žym.**) ir $\alpha = 0{,}05$ (žym. *) .

Vadinasi, galime teigti, kad koreliacija tarp amžiaus bei raidžių atpažinimo yra reikšminga su pasikliautinuoju intervalu $\propto = 0{,}01$

2.5 LYTIES, REGOS, FIZINĖS BŪSENOS NEPRIKLAUSOMUMO TIKRINIMAS

Kiti mūsų stebėti atsitiktiniai dydžiai yra kategoriniai (lytis, rega, fizinė būklė). Tam, kad įvertintume kategorinių dydžių tarpusavio ryšį, patikrinsime χ^2 kriterijų. Pirsono homogeniškumo kriterijus nusakomas formule [19]:

$$\chi^2 = mn \sum_{i=1}^{k} \frac{1}{m_i + n_i} \left(\frac{m_i}{m} - \frac{n_i}{n}\right)^2 \tag{2.10}$$

čia m – objektų pirmoje grupėje skaičius, n – objektų antroje grupėje skaičius, m_i- i-tąjį įvertinimą gavusių objektų skaičius pirmoje grupėje, n_i- i-tąjį įvertinimą gavusių objektų skaičius antrojoje grupėje.

Pagal χ^2 kriterijaus reikšmes galima teigti, kad stebimi atsitiktiniai dydžiai yra tarpusavyje susiję, kaip *p* reikšmė didesnė nei 0,05 (galimybė suklysti yra 1 iš 20).

Asimptotinis kriterijus yra tikslus tuomet, kai tenkinamos šios prielaidos: didesnėse nei keturlaukėse lentelėse 80% ląstelių dažniai yra ne mažesni nei 5 ir (2.17 lent.) nėra lentelių su nuliniais dažniais (2.17 lent). χ^2kriterijaus tarp fizinės būsenos ir regos (2.17lent.) reikšmė yra lygi p=0,009<0,05, vadinasi galime teigti, kad egzistuoja statistinis ryšys tarp fizinės asmens būklės bei regos.

2.17 lentelė. χ^2kriterijaus tarp fizinės būsenos ir regos

	Value	Df	Asymp. Sig. (2-sided)
Pearson Chi-Square	9.339[a]	2	.009
Likelihood Ratio	9.006	2	.011
Linear-by-Linear Association	9.198	1	.002
N of Valid Cases	70		
a. 2 cells (33.3%) have expected count less than 5. The minimum expected count is 2.20.			

Patikrinsime χ^2kriterijų tarp amžiaus ir regos pagal tikėtinumo santykį (angl. Likelihood Ratio), kuris skaičiuojamas pagal formulę [24]:

$$\chi^2 = -2\sum_{i=1}^{n} O_i ln\frac{E_i}{O_i}, \tag{2.11}$$

čia O_i – nustatyti dažniai, E_i – tikėtini dažniai, n – bendras kintamųjų kategorijų ir grupių skaičius.

Pagal šį požymio nepriklausomumo kriterijų galime teigti, kad akinių dėvėjimas ir amžius nėra susiję. Pateikta *p* reikšmė lygi *0,280* , o tai daugiau nei 0,05 (2.19 lent.).

2.18 lentelė. χ^2kriterijaus tikrinimas tarp amžiaus ir regos

	Value	Df	Asymp. Sig. (2-sided)
Pearson Chi-Square	13.981[a]	15	.527
Likelihood Ratio	17.673	15	.280
Linear-by-Linear Association	6.113	1	.013
N of Valid Cases	70		
a. 29 cells (90.6%) have expected count less than 5. The minimum expected count is .31.			

Pagal šio χ^2kriterijaus reikšmes galime teigti, kad yra tam tikras sąryšis tarp asmens fizinės būsenos bei regos, tačiau negalime teigti, kad egzistuoja koks nors ryšys tarp asmens amžiaus bei regos.

2.6 NEPARAMETRINĖ KORELIACIJA

2.6.1 SĄRYŠIS TARP RAIDĖS ATPAŽINIMO IR LAIKO

Teorinėje dalyje sudarytas ir išnagrinėtas skaitmenis slaptos informacijos dekodavimo algoritmas yra paremtas optiniais ir fizikiniais reiškiniais bei harmoniniais virpesiais, todėl darome prielaidą, kad atskiro asmens raidės atpažinimo dažnis priklauso nuo eksperimento atlikimo laiko.

Kaip jau patvirtinome 2.3 dalyje, tam tikrų raidžių atpažinimo dažnio skirstinys yra normalusis, tačiau laikas atpažinimo metu nėra pasiskirstęs pagal normalųjį skirstinį, todėl sąryšiui tarp laiko bei atpažinimo dažnio pasitelksime neparametrinį Kendalo [28] koeficientą

$$\tau = \frac{S}{\frac{n(n-1)}{2}}; \tag{2.12}$$

čia S – skirtumas, n – imties dydis.

Iš lentelės (2.19 lent.) matyti, kad raidžių atpažinimas bei laikas silpnai koreliuoja. Atsitiktinius dydžius (laiką bei atpažinimo dažnį) sieja neigiamas, silpnas ryšys. Matyti (5 priedas), kad didžiosios daugumos abėcėlės raidžių bei simbolių atpažinimo dažnis ir stebėjimo laikas susietas silpnu neigiamu sąryšiu yra susiję, kai pasikliautinasis intervalas $\alpha = 0{,}05$ (žym. *) ir $\alpha = 0{,}01$ (žym. **).

2.19 lentelė. Kendalo τ koeficiento reikšmės

		F	G	H	H	S	B	c	i	b	U	B	A
Stebėjimo laikas	Correlation Coefficient	-.323**	-.291**	-.246**	-.246**	-.219*	-.205*	-.215*	-.209*	-.188*	-.225**	-.225**	-.294**
	Sig. (2-tailed)	.000	.001	.004	.004	.010	.017	.012	.015	.029	.009	.009	.001

Dekoduoto simbolio atpažinimą bei amžių sieja silpnas, neigiamas sąryšis. Vadinasi, galime teigti, kad kuo vėlesnis paros laikas, tuo mažesnis virpinimo dažnis yra reikalingas dekodavimo algoritmui dinaminėje vizualinėje. Ir atvirkščiai, kuo ankstesnis paros laikas, tuo didesnis kadrų per sekundę skaičius, yra reikalingas dekodavimo algoritmui atlikti.

2.6.2 LYTIES ĮTAKA ATSKIROS RAIDĖS ATPAŽINIMO DAŽNIUI

Panagrinėkime lyties bei raidės atpažinimo dažnį. Tikrinama hipotezė H_0: „ dviejų imčių skirstiniai yra lygūs“ su alternatyva H_a: „dviejų imčių skirstiniai nėra lygūs“.

Mann – Whitney kriterijus apskaičiuojamas pagal formulę [28]:

$$U = n_1 n_2 + \frac{n_2(n_2+1)}{2} - \sum_{i=r_1}^{n_2} R_i; \tag{2.13}$$

čia n_1- pirmosios imties dydis, n_2- pirmosios imties dydis, R_i

Mann-Whitney kriterijus taikomas, kai tenkinamos šios prielaidos [24]:

- Priklausomas kintamasis yra kiekybinis (atpažinimo dažnis);
- Nepriklausomas kintamasis yra sudarytas iš dviejų kategorinių kintamųjų grupių (lytis: vyrai ir moterys);
- Stebėjimai skirtingose grupėse yra nepriklausomi;
- Skirtingų kiekybinio kintamojo grupių (vyrų ir moterų) skirstiniai nėra pasiskirstę pagal normalųjį dėsnį.

Rezultatų išklotinėje (2.20 lent.), matyti kad vyrai atpažįsta raides (E, W, w), kai virpinimo dažnis yra mažesnis (vyrų vidurkių rangai mažesni nei moterų vidurkių rangai). Prisiminkime, kad šių raidžių atpažinimą bei amžių taip pat sieja stiprus teigiama neparametrinis sąryšis.

2.20 lentelė. Raidžių (E, W, w) atpažinimo rangų vidurkis pagal lytį

	Lytis	N	Mean Rank	Sum of Ranks
E	Vyrai	33	23.58	778.00
	Moterys	37	46.14	1707.00
	Total	70		
W	Vyrai	33	24.06	794.00
	Moterys	37	45.70	1691.00
	Total	70		
w	Vyrai	33	24.29	801.50
	Moterys	37	45.50	1683.50
	Total	70		

6 priede matyti, kad absoliučiai visų pagal neparametrinį skirstinį pasiskirsčiusių raidžių atpažinimo virpinimo dažnis mažesnis vyrų nei moterų.

2.21 lentelė. Raidžių (E, W, w) atpažinimo statistinis reikšmingumas pagal lytį

	E	W	w
Mann-Whitney U	217.000	233.000	240.500
Wilcoxon W	778.000	794.000	801.500
Z	-4.652	-4.463	-4.373
Asymp. Sig. (2-tailed)	.000	.000	.000
Exact Sig. (2-tailed)	.000	.000	.000

Exact Sig. (1-tailed)	.000	.000	.000
Point Probability	.000	.000	.000

Taip pat galime teigti, kad raidžių (E, W, w) atpažinimas pagal lytį yra statistiškai reikšmingas (2.21 lent.). Lentelėje matyti, kad raidžių atpažinimo *p=0,00* reikšmė mažesnė nei 0,05. Skaičiuojant tikslų (exact sig.) bei asimptotinį (asymp sig.) sprendinį, galime patvirtinti, kad statistiškai vyrai dekoduojamas raides atpažįsta prie mažesnio virpinimo dažnio nei moterys.

2.6.3 REGOS BEI RAIDŽIŲ (E, W, w) ATPAŽINIMO DAŽNIO RYŠYS

Darome prielaidą, kad raidžių E, W, w atpažinimo dažnis yra susijęs ne tik su asmens amžiumi ar lytimi, bet ir su regėjimo kokybe, t.y. asmuo atpažįsta mažesniu dažniu virpinamą paveiksle užkoduotą informaciją, jei nedėvi akinių ar kontaktinių lęšių. 2.22 lent. matyti, kad asmenims, kurie nedėvi akinių ar kontaktinių lęšių, pakanka mažesnio paveikslo virpinimo dažnio tam tikros raidės (E,W, w) atpažinimui.

2.22 lentelė. Raidžių (E,W, w) atpažinimas pagal regą

	Rega	N	Mean Rank	Sum of Ranks
E	0	48	31.41	1507.50
	1	22	44.43	977.50
	Total	70		
W	0	48	31.60	1517.00
	1	22	44.00	968.00
	Total	70		
w	0	48	31.51	1512.50
	1	22	44.20	972.50
	Total	70		
	0* -asmuo nedėvi akinių ar kontaktinių lęšių, 1**- asmuo dėvi akinius ar kontaktinius lęšius			

Rezultatų lentelėje (2.23 lent.) matyti, kad pateikta asimptotinė ir tiksli reikšmės beveik nesiskiria. Pateikta p reikšmė: $p_E = 0{,}012 < 0{,}05, p_W = 0{,}017 < 0{,}05, p_w = 0{,}015 < 0{,}05$, todėl galima tvirtinti, kad regos įtaka dekoduojamo paveikslo virpinimo dažniui statistiškai reikšminga. Jei asmuo nedėvi jokių akinių ar kontaktinių lęšių, tai statistiškai jis atpažįsta simbolius E, W, w virpinat paveikslą mažesniu dažniu, nei tie, kurie juos dėvi.

2.23 lentelė. Raidžių (E, W, w) atpažinimo statistinis reikšmingumas pagal regą.

	E	W	w
Mann-Whitney U	331.500	341.000	336.500
Wilcoxon W	1507.500	1517.000	1512.500
Z	-2.498	-2.377	-2.434
Asymp. Sig. (2-tailed)	.012	.017	.015
Exact Sig. (2-tailed)	.012	.017	.014
Exact Sig. (1-tailed)	.006	.008	.007

2.6.4 RAIDŽIŲ E, W, w ATPAŽINIMO IR FIZINĖS BŪSENOS SĄRYŠIS

Raidžių E, W, w (2.24 lent.) atpažinimas netenkina būtinos prielaidos apie grupių pavargęs, nepavargęs bei jaučia pirmus nuovargio požymius pasiskirstymo homogeniškumą, tai neturime pakankamai įrodymų tikrinti šių raidžių bei fizinės būsenos sąsajos.

2.24 lentelė. Raidžių (E, W, w) atpažinimo homogeniškumo tikrinimas

	Levene Statistic	df1	df2	Sig.
E	4.151	2	67	.020
W	3.955	2	67	.024
w	4.793	2	67	.011

2.6 skyriaus išvados

Išnagrinėję neparametriniu skirstinu pasiskirsčiusių abėcėlės raidžių atpažinimo dažnį, galime prieiti prie šių išvadų:

- daugumos raidžių (E, T, U, R ,M, r, O,W,L, Q,J, j, c,?) atpažinimas yra susietas teigiamu koreliaciniu sąryšiu su amžiumi, t.y. kuo asmuo jaunesnis, tuo mažesnis virpinimo dažnis reikalingas jam atpažinti dekoduotą simbolį;
- Neparametriniu skirstiniu pasiskirsčiusias raidžių (E, W, w) atpažinimo dažnį įtakoja lytis. Vyrai dekoduojamus simbolius atpažįsta prie mažesnio virpinimo dažnio nei moterys
- Regos bei raidžių E, W, w atpažinimo sąryšis taip pat statistiškai reikšmingas. Nedėvintys akinių ar kontaktinių lęšių asmenys šias raides pamato prie mažesnio virpinimo dažnio nei tie, kurie juos dėvi.

2.7 VISŲ PAVEIKSLE UŽKODUOTŲ RAIDŽIŲ ATPAŽINIMO DAŽNIO BEI AMŽIAUS, LAIKO, LYTIES IR REGOS SĄRYŠIS

Ankstesniuose skyriuose jau aptarėme pavienių abėcėlės raidžių dekodavimo algoritmo reikšmes. Šiame skyriuje panagrinėkime ir palyginkime rezultatus, gautus dekodavimo algoritmą kartojant tol, kol asmuo atpažins visas muaro gardelėje užkoduotas raides..

Hipotezės H_0: „paveikslų atpažinimo skirstinys pasiskirstęs pagal normalųjį dėsnį“ su alternatyvą H_a: „paveikslų atpažinimo skirstinys nėra pasiskirstęs pagal normalųjį dėsnį“ rezultatų išklotinėje (2.25 lent.) matyti, kad panašiai kaip ir pavienių raidžių atpažinimas, taip ir visos informacijos atpažinimo maždaug pusės skirstinių dažnis yra apytiksliai normalusis.

2. 25 lentelė Hipotezės apie paveiksluose užkoduotų raidžių normalųjį pasiskirstymą tikrinimas

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	Df	Sig.
Amžius	.194	91	.000	.908	91	.000
AsK.pav_1	.108	91	.011	.986	91	.415
Vgt.pav_2	.148	91	.000	.914	91	.000
gerg.pav_4	.089	91	.070	.981	91	.206
Meg.pav_5	.099	91	.029	.935	91	.000
KTI.pav_6	.083	91	.151	.983	91	.280
Gm.pav_7	.107	91	.012	.981	91	.201
drej.pav_8	.092	91	.055	.978	91	.124
beF.pav_9	.098	91	.032	.970	91	.033
SaM_10	.126	91	.001	.967	91	.022
iFpav_3	.119	91	.003	.931	91	.000

Spirmano ranginės koreliacijos koeficientas byloja, kad su pasikliautinuoju intervalu $\alpha = 0{,}01$ ir $\alpha = 0{,}05$ (2.26 lent.) galime teigti, kad kintamuosius laikas bei virpinimo dažnis sieja statistiškai reikšmingas sąryšis. Pagal empirines imties koreliacijos koeficiento reikšmes matyti, kad kuo asmuo labiau įgunda sekti besikeičiančius vaizdus (pirmojo paveikslo atpažinimą ir laiką sieja silpnas ryšys, o paskutiniųjų vidutinio stiprumo), tuo labiau tikėtina atpažinimo dažnio ir laiko sąsaja. Nulinė hipotezė H_0: „$\rho = 0$“ yra atmetama su 99,9 % tikimybe (p = *0,000* <0.001) 3 pav., 4 pav., 6 pav. 8 pav , 9 ir 10 pav. Vadinasi, galime teigti, kad šių paveikslų atpažinimą ir laiką sieja stiprus monotoninis ryšys.

2. 26 lentelė Spirmano koreliacijos koeficientas tarp laiko ir paveikslo atpažinimo dažnio

			Laikas	pav_1	pav_2	pav_3	pav_4	pav_5	pav_6	pav_7	pav_8	pav_9	pav_10
Spearman's rho	Laikas	Correlation Coefficient	1.000	.272	.313	.388	.375	.287	.384	.345	.494	.534	.539
		Sig. (2-tailed)	.	.009	.003	.000	.000	.006	.000	.001	.000	.000	.000
		N	91	91	91	91	91	91	91	91	91	91	91

Rezultatų išklotinėje (2.27 lent.) matyti, kad pagal Gauso skirstinį pasiskirsčiusių paveikslų (8 priedas) atpažinimų vidurkis tarp asmenų, kurie dėvi akinius ar kontaktinius lęšius ir tų, kurie jų nedėvi, labai panašus. Tą patvirtina ir nepriklausomų imčių t-kriterijaus reikšmės ($p>0,05$) (2.27 lent.). Vadinasi, negalime patvirtinti H_0 hipotezės apie vaizdo atpažinimo dažnio ir regos sąryšį.

2. 27 lentelė Vidurkių tarp regos grupių palyginimas

	Rega	N	Mean	Std. Deviation	Std. Error Mean
pav_1	0*	61	15.6557	3.20617	.41051
	1**	30	16.2167	3.99285	.72899
pav_4	0*	61	12.3607	1.97933	.25343
	1**	30	12.5500	2.50637	.45760
pav_6	0*	61	11.7623	2.00334	.25650
	1**	30	12.0667	2.59221	.47327
pav_7	0*	61	10.7623	2.04452	.26177
	1**	30	10.4667	2.22809	.40679
pav_8	0*	61	11.4754	2.21628	.28377
	1**	30	11.7000	2.07863	.37950
	0* -asmuo nedėvi akinių ar kontaktinių lęšių, 1**- asmuo dėvi akinius ar kontaktinius lęšius				

2. 28 lentelė. Nepriklausomų imčių t-kriterijus regos grupėms

		Levene's Test for Equality of Variances		t-test for Equality of Means				
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference
pav_1	Equal variances assumed	1.965	.164	-.722	89	.472	-.56093	.77649
pav_4	Equal variances assumed	3.896	.051	-.392	89	.696	-.18934	.48283
pav_6	Equal variances assumed	1.732	.192	-.617	89	.539	-.30437	.49338
pav_7	Equal variances assumed	.274	.602	.629	89	.531	.29563	.46965
pav_8	Equal variances assumed	.276	.601	-.464	89	.644	-.22459	.48443

Iš 2.29 lentelės matyti, kad vyrų paveikslų atpažinimo dažnio vidurkiai yra mažesni nei moterų, tačiau pagal populiacijos statistikos reikšmės tarp lyties ir paveikslo informacijos atpažinimo dažnio, galime teigti, kad informacijos dekodavimo dažnio bei lyties nesieja statistinis ryšys (2.30 lent), p reikšmė >0,005.

2. 29 lentelė. Pagal Gauso skirstinį pasiskirsčiusių paveikslų atpažinimo ir lyties grupių vidurkių palyginimas

	Lytis	N	Mean	Std. Deviation	Std. Error Mean
pav_1	Vyrai	38	15.4079	3.73054	.60517
	Moterys	53	16.1509	3.27664	.45008
pav_4	Vyrai	38	12.1842	2.23129	.36196
	Moterys	53	12.5943	2.10324	.28890
pav_6	Vyrai	38	11.5526	2.22635	.36116
	Moterys	53	12.0849	2.18328	.29990
pav_7	Vyrai	38	10.4474	2.45717	.39861
	Moterys	53	10.8208	1.80835	.24840
pav_8	Vyrai	38	11.1974	2.28254	.37028
	Moterys	53	11.8019	2.05768	.28264

2.30 lentelė. Nepriklausomų imčių t-kriterijus lyties grupėms

		Levene's Test for Equality of Variances		t-test for Equality of Means				
		F	Sig.	T	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference
pav_1	Equal variances assumed	1.965	.164	-.722	89	.472	-.56093	.77649
pav_4	Equal variances assumed	3.896	.051	-.392	89	.696	-.18934	.48283
pav_6	Equal variances assumed	1.732	.192	-.617	89	.539	-.30437	.49338
pav_7	Equal variances assumed	.274	.602	.629	89	.531	.29563	.46965
pav_8	Equal variances assumed	.276	.601	-.464	89	.644	-.22459	.48443

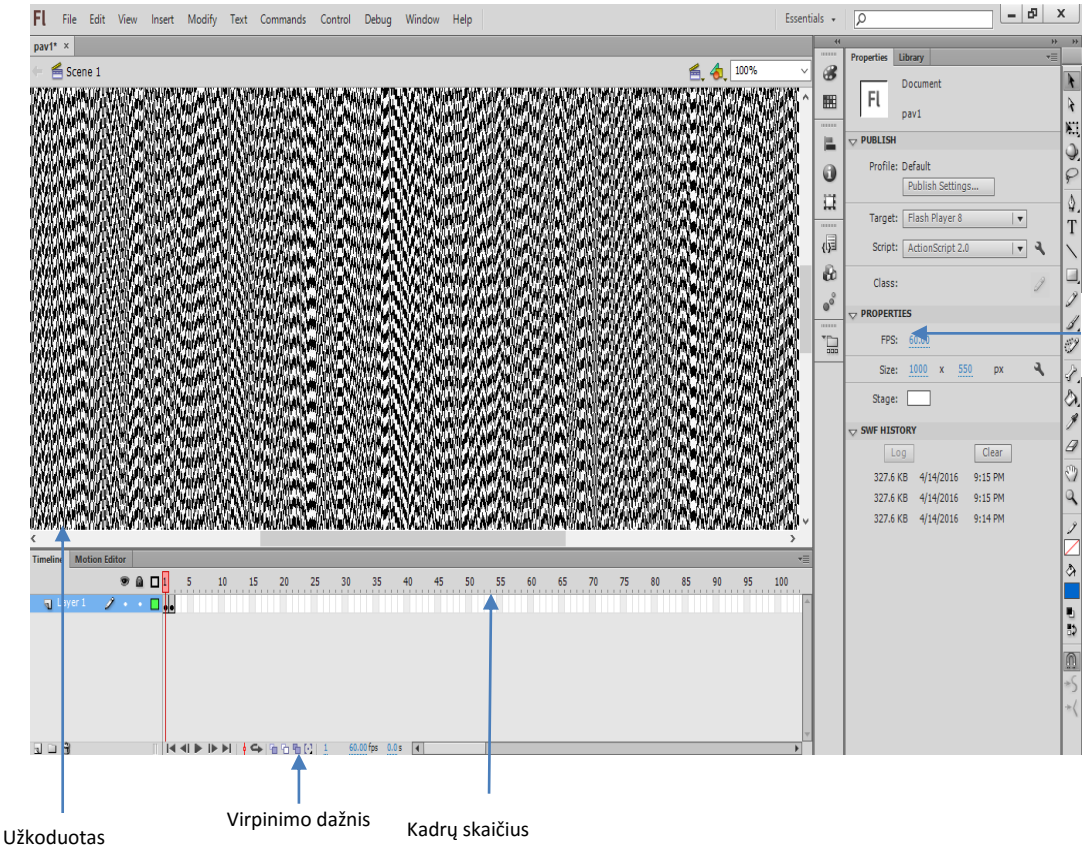
Empirinio Spirmano koreliacijos koeficiento reikšmės rodo, kad nors amžių ir paveikslo atpažinimą sieja silpnas teigiamas koreliacinis ryšys, negalime atmesti hipotezės H_0: „ Populiacijos koeficientas lygus 0“. Pateiktoje (2.31 lent.) matyti, kad p reikšmė žymiai didesnė nei 0,05.

9 -10 priede pateiktas pagal neparametrinį modelį pasiskirsčiusių paveikslo raidžių atpažinimo dažnio sąryšis tarp lyties ir regos. Ir jame matyti, kad lyties bei regos įtaka nėra ryški, nors jau įrodėme, kas atskiros raidės atpažinimui šie veiksniai turi įtakos.

2. 31 lentelė. Spirmano koreliacijos koeficiento reikšmės tarp paveikslo atpažinimo ir laiko

			Laikas	pav_1	pav_2	pav_3	pav_4	pav_5	pav_6	pav_7	pav_8	pav_9	pav_10
Spearman's rho	Amzius	Correlation Coefficient	.042	.175	.085	.196	.207	.346	.215	.229	.196	.213	.166
		Sig. (2-tailed)	.696	.097	.424	.063	.049	.001	.041	.029	.063	.043	.116
		N	91	91	91	91	91	91	91	91	91	91	91

3. DEKODAVIMO PROCEDŪRA: PROGRAMINĖ REALIZACIJA IR INSTRUKCIJA VARTOTOJUI



3.1 pav. Dekodavimo algoritmo programinės įrangos langas

DISKUSIJA

Informacijos kodavimas literatūros apžvalgoje išnagrinėtu metodu yra iki šiol menkai ištirta tema. Virpinimo dažnio parinkimas sudėtingas procesas, kurį hipotetiškai įtakoja laikas, lytis, amžius bei rega.

Darbe tirtų abėcėlės raidžių koreliacinė analizė parodė, kad skirtingų raidžių atpažinimą lemia įvairūs veiksniai. Vienų raidžių atpažinimą lytis, amžius bei fizinė būsena įtakoja stipriau, kitų silpniau. Galime teigti, kad virpinamo simbolio atpažinimui įtaką daro ir greta esančios raidės. Pastebėta, kad jei asmuo pastebi raidę H, tai šalia jos esančią h mažąją atpažįsta virpinant ją lygiai tokiu pat dažniu. Lygiai tas pats pasakytina ir apie tris iš eilės tame pačiame paveiksle esančias raides A, B, C (jų atpažinimo dažnis absoliučiai identiškas). Kitas vertus, patvirtinti galime tik abėcėlės raidžių W, E, S, x, z, ,w sąryšį su amžiumi, lytimi bei rega. Raidžių x, z, S sąryšis labai ryškus ne tik su lytimi, amžiumi bei rega, bet ir su fizine asmens būsena; virpinimo atpažinimo dažnio kreivė smarkiai kyla į viršų, jei asmuo pavargęs (skirtumas tarp jaučia pirmus nuovargio požymius ir yra labai pavargęs nėra toks ryškus).

Labai įdomūs ir skirtingi rezultatai gaunami, kai dekodavimo algoritmas yra atliekamas iki tol, kol asmuo atpažįsta visą užšifruotą informaciją. Tokiu atveju gauname, kad atpažinimo dažnis labiausiai sietinas su laiku. Amžiaus, regos bei lyties įtaką mūsų nagrinėjamų paveikslų atpažinimo dažniui (8 priedas) įtakos neįrodėme.

Darbe pateikta analizė patvirtina, kad yra tam tikras statistinis ryšys tarp raidžių atpažinimo pasiskirstymo bei asmens charakteristikų; analogiškai patvirtinome, kad egzistuoja monotoninis neparametrinis ryšys tarp visos užkoduotos slaptos informacijos ir laiko. Iš pateikto paveikslų atpažinimo (2.23 lent.) matyti, kad kuo respondentas labiau įgunda sekti besikeičiančius vaizdus, tuo didesnę įtaką jo atpažinimui daro tyrimo laikas; Spirmano koreliacijos koeficiento reikšmės, tarp stebėjimo laiko ir atpažinimo dažnio, didėja. Siūloma pirmus du paveikslus pateikti apmokymui.

Matyti, kad yra tam tikras sąryšis tarp nagrinėjamų charakteristikų ir dekodavimo algoritmo, tačiau reikalingos išsamesnės studijos, leidžiančios patvirtinti dėsningumus.

IŠVADOS

- Dinaminės vizualinės kriptografijos metodu užkoduotos slaptos informacijos dekodavimo procedūra yra individuali. Skirtingų abėcėlės raidžių atpažinimas priklauso ne tik nuo dekodavimo procese dalyvaujančio asmens charakteristikų, bet ir nuo dekoduojamo simbolio.
- Daugumos abėcėlės raidžių (daugiau nei pusės) atpažinimo pasiskirstymas normalusis.
- Užkoduotos slaptos informacijos – atsitiktinai parinktų abėcėlės raidžių dekodavimo dažnio parinkimą individualiam asmeniui bei laiką sieja silpnas neigiamas neparametrinis ryšys. Laiko bei dekodavimo algoritmo sąryšis neįrodytas.
- Gauti rezultatai parodė, kad kintamieji: lytis, amžius, rega bei fizinė būsena įtakoja ne visas abėcėlės raides. Didžiausią įtaką minėti veiksniai turi raidžių S, x, z, atpažinimui.
- Lyginant viso paveikslo raidžių atpažinimo dažnio sąryšį su lytimi, laiku bei amžiumi, matyti, kad didžiausią įtaką raidžių atpažinimui turi laiko kintamasis; atpažinimo dažnio sąryšis su laiku stiprėja tuomet, kai įgundama atlikti dekodavimo algoritmą - pirmųjų paveikslų atpažinimo dažnio sąryšis su amžiumi mažiausias, paskutiniojo stipriausias.

LITERATŪRA

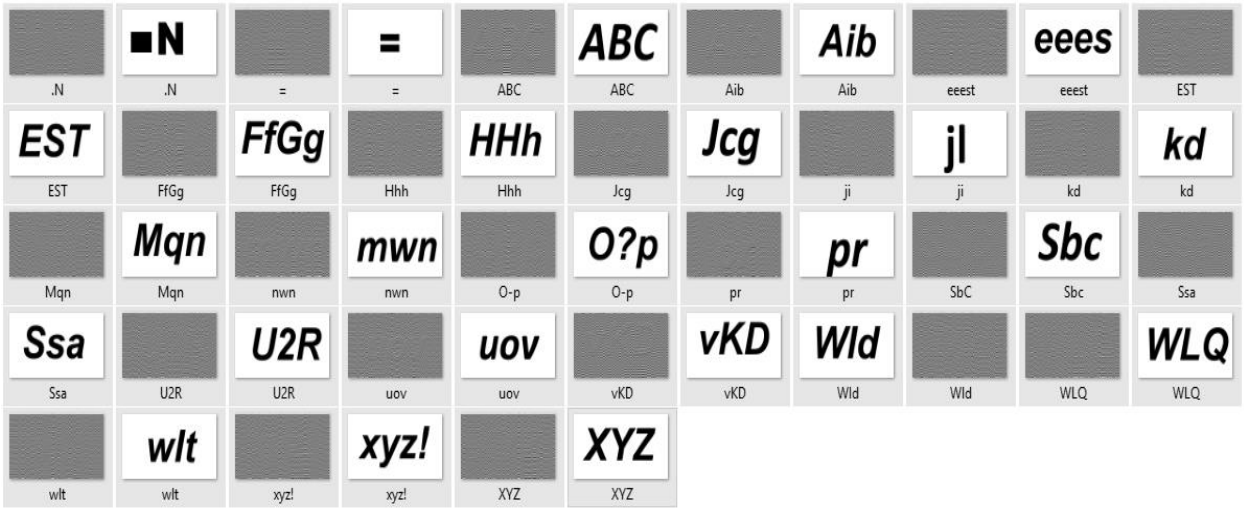
1. CHANG-CHOU, L., and T. WEN-HSIANG. Visual cryptography for gray- level mages by dithering techniques. *Pattern Recognition Letters.* 2003, 24, 349-358.ISBN 978-3-540-92238-4
2. CLOUD, G. Optical Methods in Experimental Mechanics. *Society in experimental mechanics.* 2006, 30(2), 13-69. Prieiga per doi: 10.1111/j.1747-1567.2006.00032.x
3. CIMATO, S., DE PRISCO S., and A. DE SANTIS. Colored visual cryptography without color darkening. *Theoretical Computer science*. 2007, 304 (1-3), 261-267.
4. DIFFIE W. and M. HELLMAN. New Direction in Cryptography. *Transaction of information theory.* 1976, 22. ISNN 15579654.
5. DUO J., Y.WEI-QI, and M.S. KANKANHALLI. Progressive color visual cryptography. *Journal of Electronic Imaging. 2005*. [žiūrėta 2016-05-05] Prieiga per: *https://pdfs.semanticscholar.org/*
6. ENGINEERING statistics handbook [interaktyvus] Žiūrėta [2016-05-05, 11:43]. Prieiga per :https:// www.statsref.com/HTML/introduction.html
7. GABRIELAN, E. The basic of line moire pattern and optical speedup. [žiūrėta 2016-05-05] Prieiga per : https://docs.switzernet/
8. HE, Z., C., and A. BOUMAN. AM/FM halftoning: Digital halftoning through simultaneous modulation of dot size and dot density. *Journal of Electronic Imaging.* 2004, 13(2), 286-302.
9. RAGULSKIS M., and Z.Navickas. Time- Average Geometric Moire. Back to Basics. *Experimental Mechanics.* [interaktyvus], 2009, 439-457. Prieiga per doi: 10.1007/s11340-008-9167-8.
10. KLEIN, A., and M. WESSLER. Extended visual cryptography schemes. *Information and Computation*. [interaktyvus] *2007, 205, 716-732. Prieiga per* doi:10.1016/j.ic.2006.12.005.
11. LEUNG, B., and Y. FELIX, and DUNCAN S. WONG. On the Security of a Visual Cryptography Scheme for Color Images. 2008 [žiūrėta 2016-05-05] Prieiga per https://eprint.iacr.org/
12. LEBANON G. and L. BRUCKSTEIN. Variation Approach to Moire pattern Synthesis. *Journal of the Optical Society of America.* 2001, 18(6),1371-1382
13. NAOR, M. and A. SHAMIR. Visual cryptography. *Lecture Notes in Computer Science* 950. 1994, 1–12.
14. PALEVIČIUS P. Optical interferometry based methods for investigation of dynamical processes in microsystem. Doctoral Dissertation. Kaunas, 2015. ISBN 978-609-02-1140-3.
15. PALIVONAITĖ, R. et al. Image hiding in time-averaged deformable moire gratings. J. Opt. 2014, 16(2), 025401. ISSN: 2040-8986.
16. PALIVONAITĖ R. Chaotic Visual cryptography. Summary of Doctoral Dissertation, Kaunas 2015.
17. PETRAUSKIENĖ, V. Dynamic Visual Cryptograhy Based On Nonlinear Oscilliations. Summary of Doctoral Dissertation, Kaunas, 2015.
18. PETRAUSKIENĖ, V., R. PALIVONAITĖ et al. Dynamic visual cryptography based on chaotic oscillations. *Communications in Nonlinear Science and Numerical Simulation*. 2014, 19(1), 112–120. ISSN: 1007-5704.
19. PUKĖNAS, Kazimieras. Kokybinių duomenų analizė SPSS programa. Kaunas: LKKA, 2009. SBN 9955-622-18-0.
20. RAGULSKIS M., L.SAUNORIENĖ and R. MASKELIUNAS. The structure of moire grating lines and influence to time averaged fringes. *Experimental techniques.* 2009, march/april, 60-64. ISSN 0732-8818.
21. RAGULSKIS M. Time-averaged pattern produced by stochastic moire gratings. *Computer and graphics.* 2009, 33(2), 147-150. ISSN 0097-8493.

22. RAGULSKIS M. and A. ALEKSA. Image hiding based on time-averaging moire. *Optics Communications.* 2009, 282, 2752-2759. ISSN 0030-4018.
23. RAGULSKIS M., A. ALEKSA and Z. NAVICKAS. Image hiding based on time-averaged fringes produced by non-harmonic oscillations. *Journal of Optics A: Pure and Applied Optics*. 2009, 11(12). ISSN 1464-4258.
24. STATISTICAL analysis handbook [interaktyvus] 2015 Žiūrėta [2016-05-05, 11:43]. Prieiga per://https//www. statsref.com/HTML/introduction.html
25. ŠAKYTĖ E et. all. Image hiding based on near optimal moire gratings. *Optics Communications.* 2011, 48. ISNN 3954-3964.
26. WAN, R. Z. Incrementing Visual Cryptography. *SP Letters*. 2009, 16 (8), 659-662.
27. WEIR, Jonathan and Weiqi YAN. *Visual Cryptography and Its Application.* 2012. ISBN 978- 87-403-0126-7.
28. VENCLOVIENĖ, Jonė. *Statistiniai metodai medicinoje*. Kaunas, 2010. ISBN 978-9955-12-558-7.

PRIEDAI

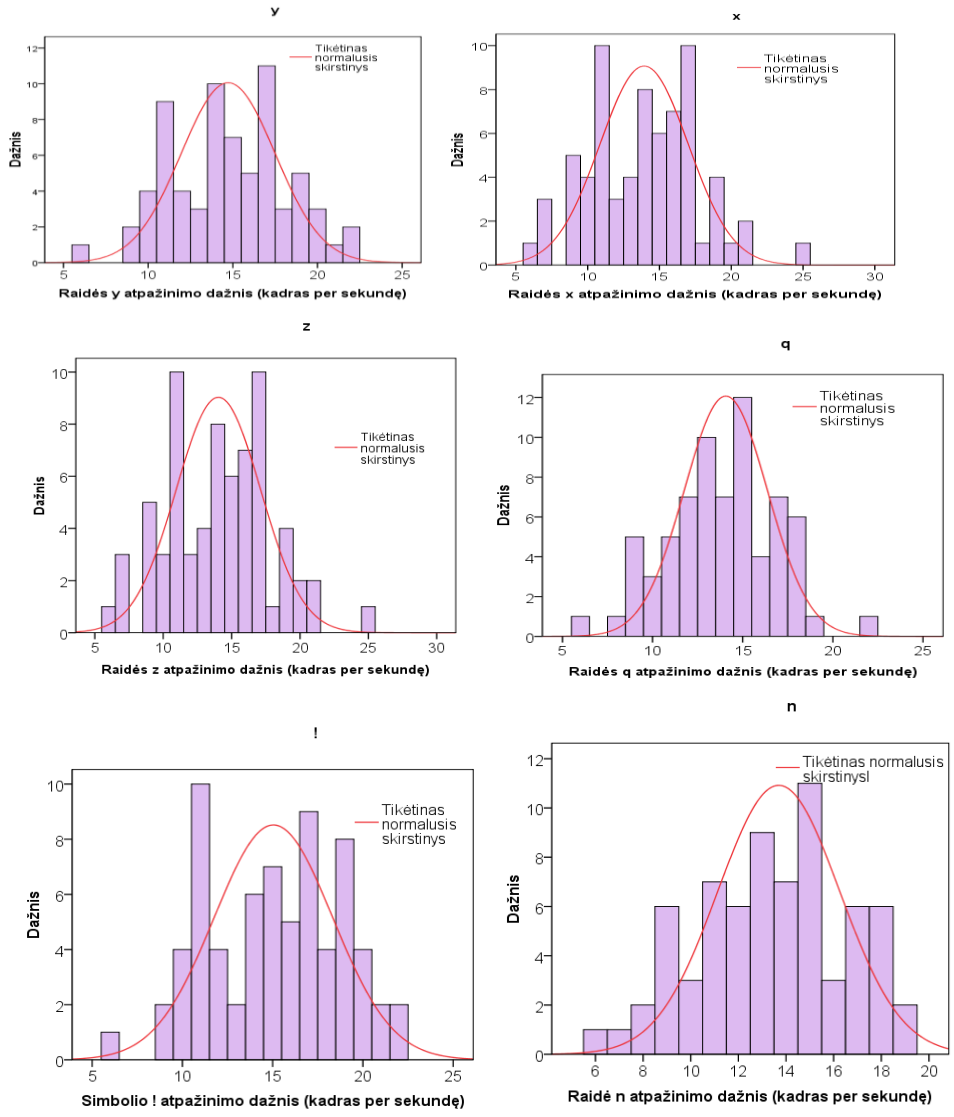
1 priedas

1.1 pav. Slaptų ir užkoduotų vaizdų biblioteka

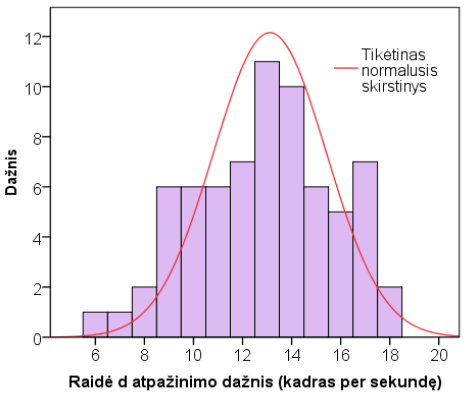


2 priedas

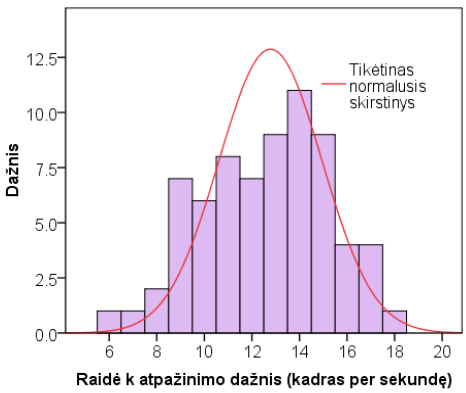
2.1 pav. Dekodavimo procedūros atskirų raidžių atpažinimo pasiskirstymas



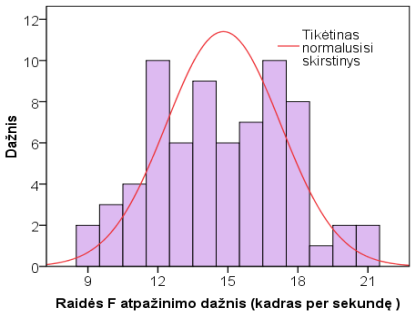
d


Tikėtinas normalusis skirstinys
Dažnis
Raidė d atpažinimo dažnis (kadras per sekundę)

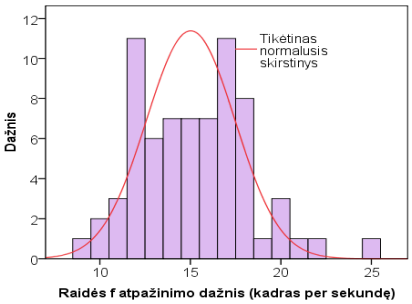
k


Tikėtinas normalusis skirstinys
Dažnis
Raidė k atpažinimo dažnis (kadras per sekundę)

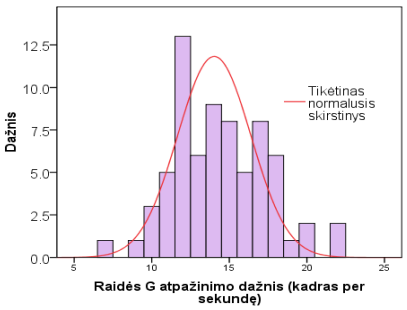
F


Tikėtinas normalusisi skirstinys
Dažnis
Raidės F atpažinimo dažnis (kadras per sekundę)

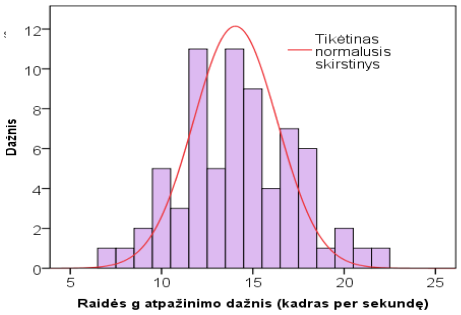
f


Tikėtinas normalusis skirstinys
Dažnis
Raidės f atpažinimo dažnis (kadras per sekundę)

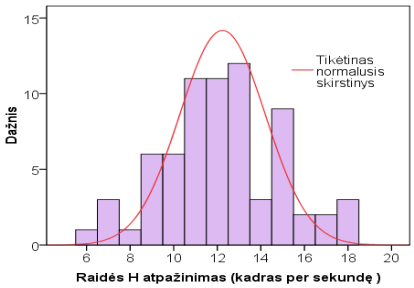
G


Tikėtinas normalusis skirstinys
Dažnis
Raidės G atpažinimo dažnis (kadras per sekundę)

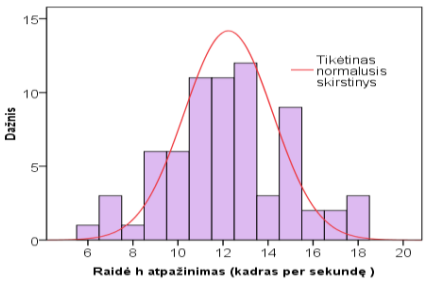
g


Tikėtinas normalusis skirstinys
Dažnis
Raidės g atpažinimo dažnis (kadras per sekundę)

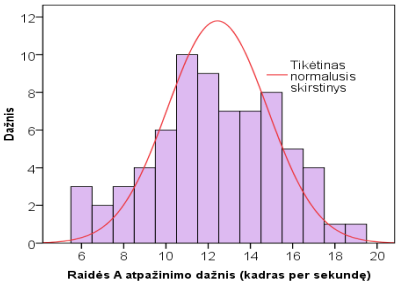
H


Tikėtinas normalusis skirstinys
Dažnis
Raidės H atpažinimas (kadras per sekundę)

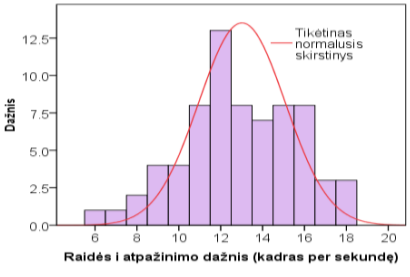
h


Tikėtinas normalusis skirstinys
Dažnis
Raidė h atpažinimas (kadras per sekundę)

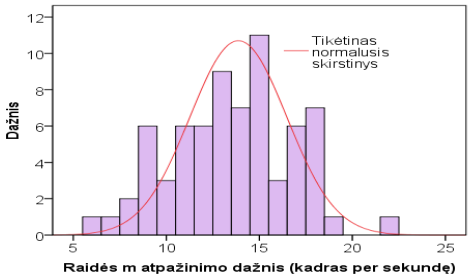
A


Tikėtinas normalusis skirstinys
Dažnis
Raidės A atpažinimo dažnis (kadras per sekundę)

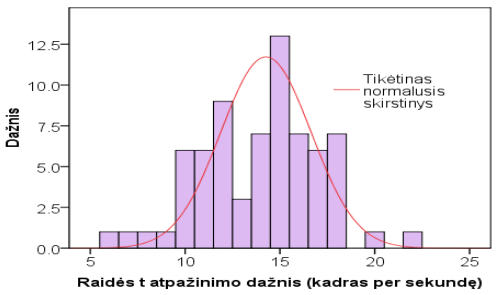
i


Tikėtinas normalusis skirstinys
Dažnis
Raidės i atpažinimo dažnis (kadras per sekundę)

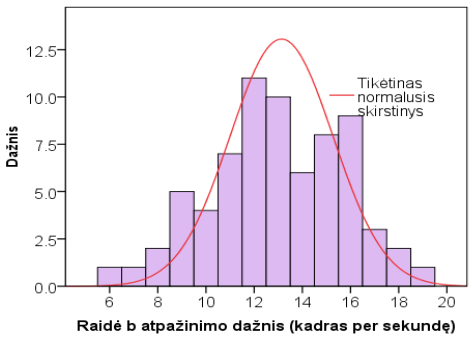
m


Tikėtinas normalusis skirstinys
Dažnis
Raidės m atpažinimo dažnis (kadras per sekundę)

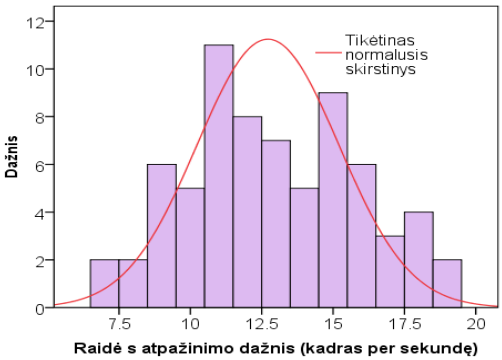
t


Tikėtinas normalusis skirstinys
Dažnis
Raidės t atpažinimo dažnis (kadras per sekundę)

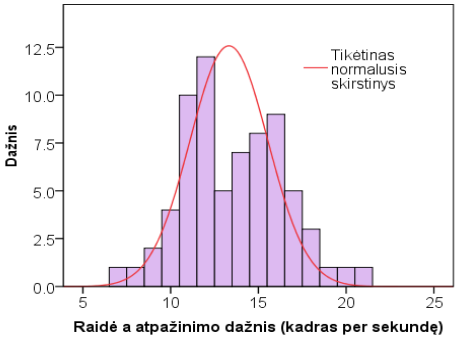
b


Tikėtinas normalusis skirstinys
Dažnis
Raidė b atpažinimo dažnis (kadras per sekundę)

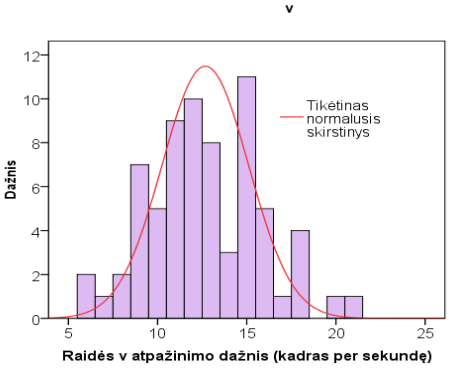
s


Tikėtinas normalusis skirstinys
Dažnis
Raidė s atpažinimo dažnis (kadras per sekundę)

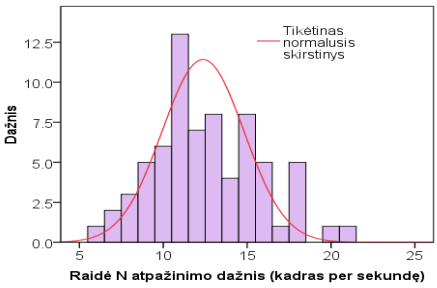
a


Tikėtinas normalusis skirstinys
Dažnis
Raidė a atpažinimo dažnis (kadras per sekundę)

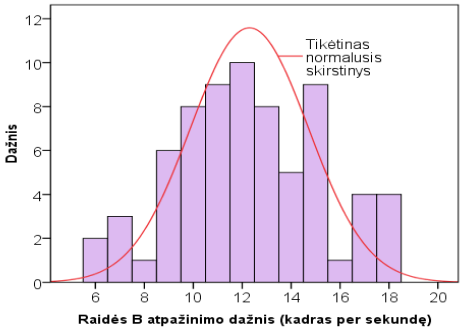
v


Tikėtinas normalusis skirstinys
Dažnis
Raidės v atpažinimo dažnis (kadras per sekundę)

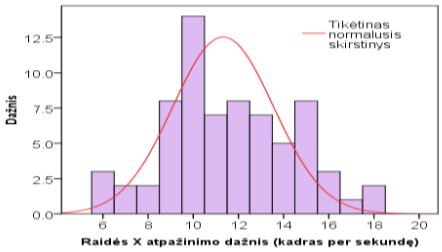
N


Tikėtinas normalusis skirstinys
Dažnis
Raidė N atpažinimo dažnis (kadras per sekundę)

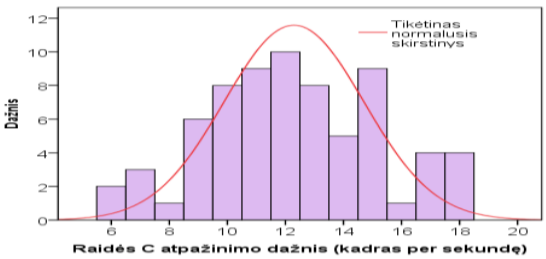
B

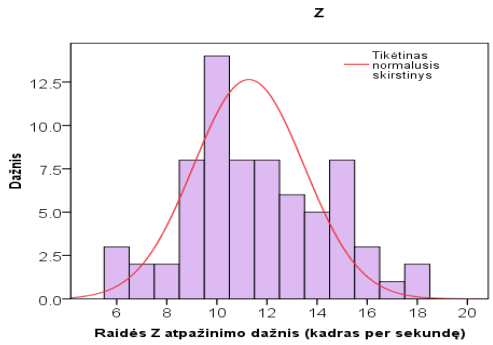

Tikėtinas normalusis skirstinys
Dažnis
Raidės B atpažinimo dažnis (kadras per sekundę)

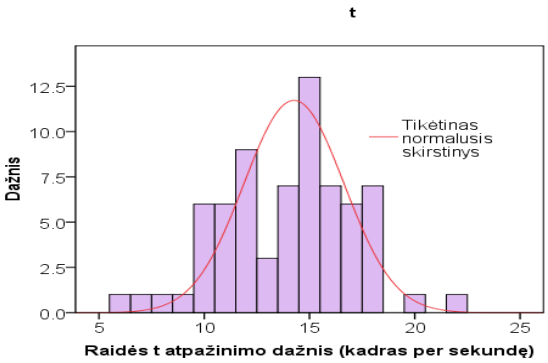
x


Tikėtinas normalusis skirstinys
Dažnis
Raidės X atpažinimo dažnis (kadras per sekundę)

c


Tikėtinas normalusis skirstinys
Dažnis
Raidės C atpažinimo dažnis (kadras per sekundę)





3 priedas

***3.1* lentelė.** Empirinio koreliacijos koeficiento reikšmės

		N	Correlation	Sig.
Pair 1	Amžius & x	70	.733	.000
Pair 2	Amžius & y	70	.554	.000
Pair 3	Amžius & z	70	.763	.000
Pair 4	Amžius & !	70	.484	.000
Pair 5	Amžius & q	70	.574	.000
Pair 6	Amžius & n	70	.602	.000
Pair 7	Amžius & A	70	.646	.000
Pair 8	Amžius & B	70	.646	.000
Pair 9	Amžius & C	70	.646	.000
Pair 10	Amžius & H	70	.634	.000
Pair 11	Amžius & h	70	.634	.000
Pair 12	Amžius & i	70	.652	.000
Pair 13	Amžius & b	70	.662	.000
Pair 14	Amžius & v	70	.400	.001
Pair 15	Amžius & u	70	.348	.003
Pair 16	Amžius & o	70	.434	.000
Pair 17	Amžius & Z	70	.377	.001
Pair 18	Amžius & X	70	.384	.001
Pair 19	Amžius & Y	70	.409	.000
Pair 20	Amžius & S	70	.628	.000
Pair 21	Amžius & s	70	.652	.000
Pair 22	Amžius & a	70	.602	.000

Empirinio koreliacijos koeficiciento sig. <0,05 reikšmė patvirtina hipotezę, kad $\rho > 0$

3.2 lentelė. Populiacijos statistika tarp amžiaus ir raidės atpažinimo

		Paired Differences					t	Df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference				
					Lower	Upper			
Pair 1	Amžius - x	20.557	6.894	.824	18.913	22.201	24.949	69	.000
Pair 2	Amžius - y	19.686	7.816	.934	17.822	21.549	21.073	69	.000
Pair 3	Amžius - z	20.414	6.721	.803	18.812	22.017	25.412	69	.000
Pair 4	Amžius - !	19.343	8.068	.964	17.419	21.267	20.058	69	.000
Pair 5	Amžius - q	20.657	7.846	.938	18.786	22.528	22.027	69	.000
Pair 6	Amžius - n	21.086	7.712	.922	19.247	22.925	22.876	69	.000
Pair 7	Amžius - A	22.214	7.597	.908	20.403	24.026	24.466	69	.000
Pair 8	Amžius - B	22.214	7.597	.908	20.403	24.026	24.466	69	.000
Pair 9	Amžius - C	22.214	7.597	.908	20.403	24.026	24.466	69	.000
Pair 10	Amžius - H	22.271	7.751	.926	20.423	24.120	24.039	69	.000
Pair 11	Amžius - h	22.271	7.751	.926	20.423	24.120	24.039	69	.000
Pair 12	Amžius - i	21.571	7.687	.919	19.739	23.404	23.479	69	.000
Pair 13	Amžius - b	21.529	7.619	.911	19.712	23.345	23.641	69	.000
Pair 14	Amžius - v	21.800	8.426	1.007	19.791	23.809	21.645	69	.000
Pair 15	Amžius - u	21.786	8.606	1.029	19.734	23.838	21.181	69	.000
Pair 16	Amžius - o	21.757	8.310	.993	19.776	23.739	21.905	69	.000
Pair 17	Amžius - Z	22.871	8.524	1.019	20.839	24.904	22.448	69	.000
Pair 18	Amžius - X	22.843	8.503	1.016	20.815	24.870	22.475	69	.000
Pair 19	Amžius - Y	22.657	8.416	1.006	20.650	24.664	22.523	69	.000
Pair 20	Amžius - S	21.686	7.645	.914	19.863	23.509	23.732	69	.000
Pair 21	Amžius - s	21.571	7.565	.904	19.768	23.375	23.856	69	.000
Pair 22	Amžius - a	20.871	7.787	.931	19.015	22.728	22.425	69	.000

Kadangi sig.=0,000<0,01 , tai galime teigti pasikliovimo lygmeniu $\alpha = 0{,}01$ raidžių atpažinimo ir amžiaus koreliacija statistiškai reikšminga.

4 priedas

4.1 lentelė Raidės atpažinimo vidurkių rangų palyginimas pagal lytį

	Lytis	N	Mean Rank	Sum of Ranks		Lytis	N	Mean Rank	Sum of Ranks
x	Vyrai	33	23.68	781.50	A	Vyrai	33	27.86	919.50
	Moterys	37	46.04	1703.50		Moterys	37	42.31	1565.50
	Total	70				Total	70		
y	Vyrai	33	27.68	913.50	B	Vyrai	33	27.86	919.50
	Moterys	37	42.47	1571.50		Moterys	37	42.31	1565.50
	Total	70				Total	70		
!	Vyrai	33	26.65	879.50	C	Vyrai	33	27.86	919.50
	Moterys	37	43.39	1605.50		Moterys	37	42.31	1565.50
	Total	70				Total	70		
z	Vyrai	33	22.53	743.50	F	Vyrai	33	26.08	860.50
	Moterys	37	47.07	1741.50		Moterys	37	43.91	1624.50
	Total	70				Total	70		
q	Vyrai	33	26.45	873.00	f	Vyrai	33	26.80	884.50
	Moterys	37	43.57	1612.00		Moterys	37	43.26	1600.50
	Total	70				Total	70		
n	Vyrai	33	28.15	929.00	G	Vyrai	33	27.39	904.00
	Moterys	37	42.05	1556.00		Moterys	37	42.73	1581.00
	Total	70				Total	70		
k	Vyrai	33	24.09	795.00	g	Vyrai	33	26.77	883.50
	Moterys	37	45.68	1690.00		Moterys	37	43.28	1601.50
	Total	70				Total	70		
d	Vyrai	33	24.95	823.50	H	Vyrai	33	27.55	909.00
	Moterys	37	44.91	1661.50		Moterys	37	42.59	1576.00
	Total	70				Total	70		
h	Vyrai	33	27.55	909.00	m	Vyrai	33	27.41	904.50
	Moterys	37	42.59	1576.00		Moterys	37	42.72	1580.50
	Total	70				Total	70		
A	Vyrai	33	25.74	849.50	t	Vyrai	33	28.82	951.00
	Moterys	37	44.20	1635.50		Moterys	37	41.46	1534.00
	Total	70				Total	70		
i	Vyrai	33	25.06	827.00	X	Vyrai	33	28.71	947.50
	Moterys	37	44.81	1658.00		Moterys	37	41.55	1537.50
	Total	70				Total	70		

b	Vyrai	33	24.95	823.50	Y	Vyrai	33	27.61	911.00
	Moterys	37	44.91	1661.50		Moterys	37	42.54	1574.00
	Total	70				Total	70		
S	Vyrai	33	26.27	867.00	Z	Vyrai	33	28.91	954.00
	Moterys	37	43.73	1618.00		Moterys	37	41.38	1531.00
	Total	70				Total	70		
Z	Vyrai	33	28.91	954.00	u	Vyrai	33	29.45	972.00
	Moterys	37	41.38	1531.00		Moterys	37	40.89	1513.00
	Total	70				Total	70		
a	Vyrai	33	26.44	872.50	o	Vyrai	33	28.15	929.00
	Moterys	37	43.58	1612.50		Moterys	37	42.05	1556.00
	Total	70				Total	70		
N	Vyrai	33	30.21	997.00	v	Vyrai	33	29.35	968.50
	Moterys	37	40.22	1488.00		Moterys	37	40.99	1516.50
	Total	70				Total	70		

4.2 lentelė. Raidės atpažinimo pagal lytį statistikos reikšmingumas. Mann Whithney kriterijus

Pateiktoje lentelėje matyti, kad raidžių atpažinimo asimp.sig. <0.05. Vadinasi galime teigti, kad raidžių atpažinimo vidurkių rangai reikųmingai skiriasi.

	x	y	!	z	q	n	k	d	A	B	C	G
Mann-Whitney U	220.500	352.500	318.500	182.500	312.000	368.000	234.000	262.500	358.500	358.500	358.500	343.000
Wilcoxon W	781.500	913.500	879.500	743.500	873.000	929.000	795.000	823.500	919.500	919.500	919.500	904.000
Z	-4.611	-3.052	-3.451	-5.060	-3.534	-2.868	-4.457	-4.118	-2.982	-2.982	-2.982	-3.169
Asymp. Sig. (2-tailed)	.000	.002	.001	.000	.000	.004	.000	.000	.003	.003	.003	.002
	X	Y	Z	u	O	v	N	g	H	h	A	i
Mann-Whitney U	386.500	350.000	393.000	411.000	368.000	407.500	436.000	322.500	348.000	348.000	288.500	266.000
Wilcoxon W	947.500	911.000	954.000	972.000	929.000	968.500	997.000	883.500	909.000	909.000	849.500	827.000
Z	-2.655	-3.088	-2.578	-2.360	-2.870	-2.403	-2.066	-3.410	-3.114	-3.114	-3.807	-4.081
Asymp. Sig. (2-tailed)	.008	.002	.010	.018	.004	.016	.039	.001	.002	.002	.000	.000
	b	S	s	a	m	t						
Mann-Whitney U	262.500	306.000	293.000	311.500	343.500	390.000						

Wilcoxon W	823.500	867.000	854.000	872.500	904.500	951.000
Z	-4.120	-3.602	-3.755	-3.542	-3.158	-2.612
Asymp. Sig. (2-tailed)	.000	.000	.000	.000	.002	.009

5 priedas

5.1 lentelė. Kendalo tau koeficiento reikšmių lentelė tarp laiko ir raidžių atpažinimo

Raidė		Q	l	t	X	Y	Z	u	o	v	kvadr.	N
Kendall's tau_b Stebėjimo laikas	Correlation Coefficient	-.225**	-.184*	-.118	-.092	-.083	-.101	-.092	-.101	-.131	-.103	-.123
	Sig. (2-tailed)	.009	.032	.171	.287	.334	.241	.284	.240	.127	.232	.151
		x	y	z	!	E	S	T	M	n	k	w
	Correlation Coefficient	-.292**	-.328**	-.267**	-.250**	-.200*	-.200*	-.200*	-.277**	-.244**	-.230**	-.227
	Sig. (2-tailed)	.001	.000	.002	.003	.019	.019	.019	.001	.004	.008	.008
		U	2	R	v	K	D	W	I	m	l	p
	Correlation Coefficient	-.280	-.187	-.187	-.212	-.089	-.097	-.227	-.017	-.237	-.178	-.131
	Sig. (2-tailed)	.001	.031	.031	.013	.310	.270	.008	.846	.006	.037	.128
		d	A	C	F	G	H	r	?	O	p	I
	Correlation Coefficient	-.148	-.225**	-.225**	-.294**	-.291**	-.246**	-.186*	-.156	-.141	-.131	.000
	Sig. (2-tailed)	.084	.009	.009	.001	.001	.004	.031	.070	.103	.128	1.000
		f	g	J	j	b	i	b	S	s	a	
	Correlation Coefficient	-.323	-.269	-.142	-.161	-.205*	-.209*	-.188*	-.163	-.187*	-.261	
	Sig. (2-tailed)	.000	.002	.099	.065	.017	.015	.029	.057	.029	.002	

6 priedas

6.1 lentelė. Vidurkių rangu sumos palyginimas pagal lytį

	Lytis	N	Mean Rank	Sum of Ranks		Lytis	N	Mean Rank	Sum of Ranks
p	Vyrai	33	25.39	838.00	e	Vyrai	33	30.95	1021.50
	Moterys	37	44.51	1647.00		Moterys	37	39.55	1463.50
	Total	70				Total	70		
R	Vyrai	33	25.39	838.00	c	Vyrai	33	25.14	829.50
	Moterys	37	44.51	1647.00		Moterys	37	44.74	1655.50
	Total	70				Total	70		
J	Vyrai	33	28.86	952.50	kvadratas	Vyrai	33	30.26	998.50
	Moterys	37	41.42	1532.50		Moterys	37	40.18	1486.50

	Total	70				Total	70		
C	Vyrai	33	28.62	944.50	I	Vyrai	33	25.59	844.50
	Moterys	37	41.64	1540.50		Moterys	37	44.34	1640.50
	Total	70				Total	70		
O	Vyrai	33	29.41	970.50	w	Vyrai	33	24.29	801.50
	Moterys	37	40.93	1514.50		Moterys	37	45.50	1683.50
	Total	70				Total	70		
?	Vyrai	33	28.45	939.00	Q	Vyrai	33	24.06	794.00
	Moterys	37	41.78	1546.00		Moterys	37	45.70	1691.00
	Total	70				Total	70		
J	Vyrai	33	29.79	983.00	L	Vyrai	33	24.06	794.00
	Moterys	37	40.59	1502.00		Moterys	37	45.70	1691.00
	Total	70				Total	70		
l	Vyrai	33	30.55	1008.00	s	Vyrai	33	30.95	1021.50
	Moterys	37	39.92	1477.00		Moterys	37	39.55	1463.50
	Total	70				Total	70		
E	Vyrai	33	30.95	1021.50					
	Moterys	37	39.55	1463.50					
	Total	70							

6.2 lentelė. Mann – Whitney U kriterijus pagal lytį

	p	r	J	c	O	?	j	l	e	c	kvadratas	L	W	Q	L
Mann-Whitney U	277.000	277.000	391.500	383.500	409.500	378.000	422.000	447.000	460.500	268.500	437.500	283.500	240.500	233.000	233.000
Wilcoxon W	838.000	838.000	952.500	944.500	970.500	939.000	983.000	1008.000	1021.500	829.500	998.500	844.500	801.500	794.000	794.000
Z	-3.951	-3.951	-2.593	-2.694	-2.383	-2.751	-2.244	-1.935	-1.787	-4.045	-2.049	-3.873	-4.373	-4.463	-4.463
Asymp. Sig. (2-tailed)	.000	.000	.010	.007	.017	.006	.025	.053	.074	.000	.040	.000	.000	.000	.000

Lentelėje matyti, kad pagal Mann-Whitney kriterijų asymp.sig < 0,05, vadinasi raidės atpažinimo rangų vidurkiai reikšmingai skiriasi pagal lytį.

7 priedas

```
%Brėžiama harmoninė muaro gardelė
clc
clear all
close all
IMG=imread('O_p.tif');  % 0 - juoda, 1 - balta
```

```
figure(1);
imshow(IMG);
[m,n]=size(IMG);
%fono ir teksto kodavimas
f= [0 0 0 0 0 0 0 0 0  1 1 1 1 1 1 1 1 1 ];
t=[ 0 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1 1 ] ;

[mf,nf]=size(f);
[mt,nt]=size(t);

Random(1:n)=0;
for I= 1:n
   Randomas(I)=mod(round(10000*rand),nf)+1;
end
%++++++++++++++++++++++++++++++++++++++++++++++++
%Koduojama blokais. Koduojama kai keičiasi fonas; kai keičiasi tekstas
IMG_mod(1:m+nf,1:n)=1;
for I=1:n     %stulpeliai
   J=1;
   JJ=1;
   while J<= m  %eilutės
      if IMG(J,I)==1 & JJ==1
         IMG_mod(1:nf-Randomas(I),J)=f(Randomas(I)+1:nf);
         J=nf-Randomas(I)+1;
         JJ=2;
      elseif IMG(J,I)==1
         IMG_mod(J:J+nf-1,I)=f(1:nf);
         I=J+nf;
      else
         IMG_mod(J:J+nt-1,I)=t(1:nt);
         J=J+nt;
      end
   end
end
IMG_mod1(1:m,1:n)=IMG_mod(1:m,1:n);
figure(3); imshow(IMG_mod1);
[mm,nn]=size(IMG_mod1);
IMG2(1:550,1:1000)=1;
IMG2(1:550,1:1000)=IMG_mod1(1:550,1:1000);
mm=im2uint8(IMG2);
imwrite(mm,'.O-p.jpg');
```

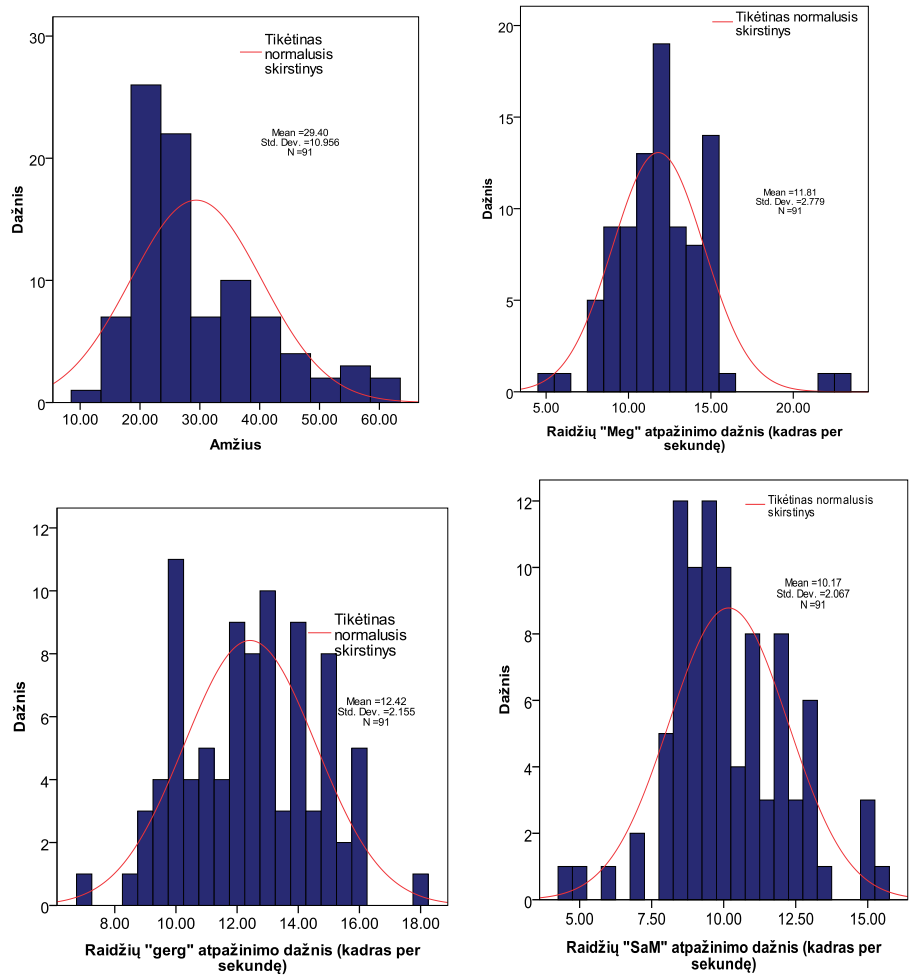
8 priedas

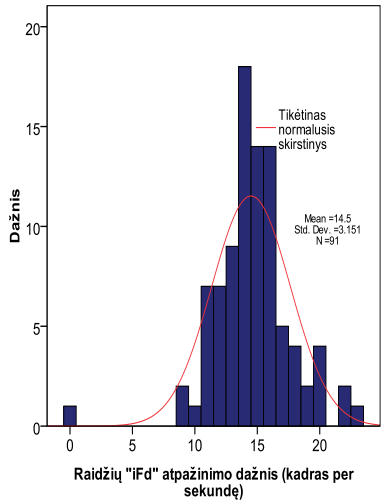
```
%Laike vidukintu gardeliu formavimasis
%nulines eiles pirmos rusies Beselio saknis
clc
clear all
close all
dlam = 0:0.01:10;
x = 2*pi*dlam;
y = besselj(0,x)
figure;
plot(x,y, 'k');
hold on;
% Draw X axis
plot([0 60], [0 0], 'k-');
set(gca,'fontsize',14)
xlabel('x')
ylabel('J_0')
% ++++++++++++++++++++++++++++++++++++++++
%Pilkio lygi nusakanti funkcija
clear all;
```

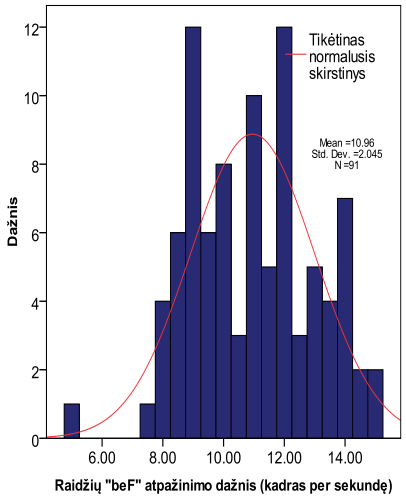
```
close all;
x = [0:0.1:10];
g = 1/2+1/2*cos(2*pi/0.25*x)
plot(x, g,'k');
set(gca,'fontsize',14)
xlabel('x')
ylabel('G(x)')
```

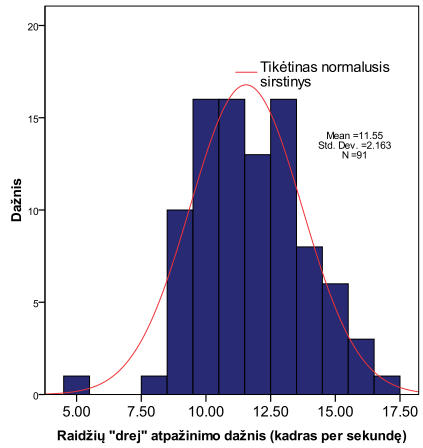
9 priedas

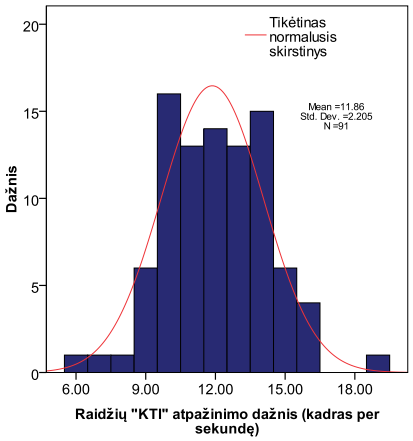
9.1 pav. Dekodavimo procedūros paveikslų atpažinimo dažnio pasiskirstymas

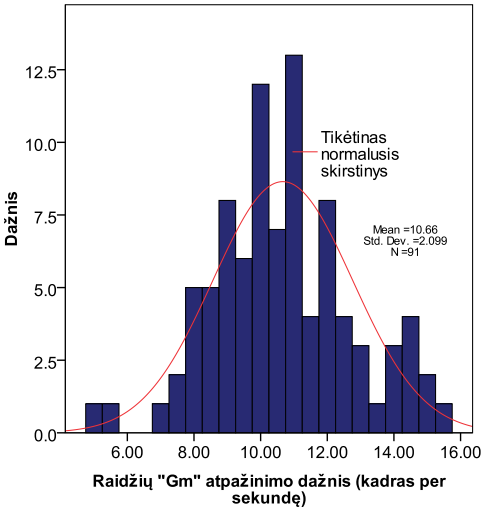


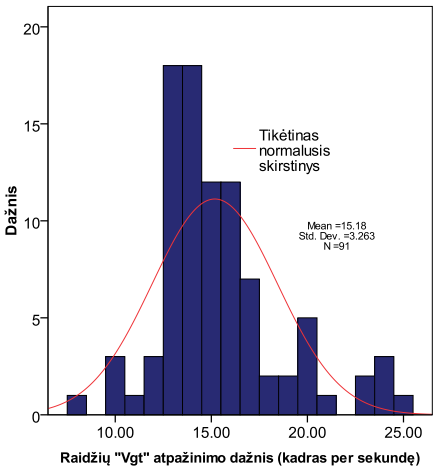

Tikėtinas normalusis skirstinys
Mean =14.5
Std. Dev. =3.151
N =91
Dažnis
Raidžių "iFd" atpažinimo dažnis (kadras per sekundę)

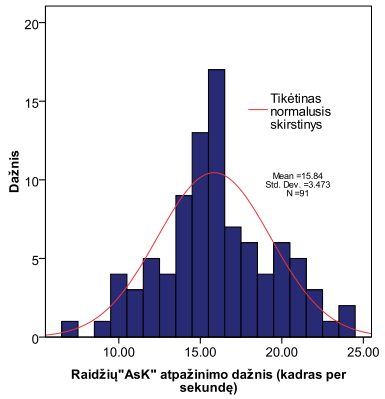

Tikėtinas normalusis skirstinys
Mean =10.96
Std. Dev. =2.045
N =91
Dažnis
Raidžių "beF" atpažinimo dažnis (kadras per sekundę)


Tikėtinas normalusis sirstinys
Mean =11.55
Std. Dev. =2.163
N =91
Dažnis
Raidžių "drej" atpažinimo dažnis (kadras per sekundę)


Tikėtinas normalusis skirstinys
Mean =11.86
Std. Dev. =2.205
N =91
Dažnis
Raidžių "KTI" atpažinimo dažnis (kadras per sekundę)


Tikėtinas normalusis skirstinys
Mean =10.66
Std. Dev. =2.099
N =91
Dažnis
Raidžių "Gm" atpažinimo dažnis (kadras per sekundę)


Tikėtinas normalusis skirstinys
Mean =15.18
Std. Dev. =3.263
N =91
Dažnis
Raidžių "Vgt" atpažinimo dažnis (kadras per sekundę)



10 priedas

10.1 lentelė. Neparametrinis sąryšis tarp lyties grupių ir visos paveiksle užkoduotos slaptos informacijos atpažinimo. Vidurkių rangų reikšmių palyginimas

	Lytis	N	Mean Rank	Sum of Ranks
pav_2	Vyrai	38	41.41	1573.50
	Moterys	53	49.29	2612.50
	Total	91		
pav_3	Vyrai	38	39.66	1507.00
	Moterys	53	50.55	2679.00
	Total	91		
pav_5	Vyrai	38	41.96	1594.50
	Moterys	53	48.90	2591.50
	Total	91		
pav_9	Vyrai	38	41.24	1567.00
	Moterys	53	49.42	2619.00
	Total	91		
pav_10	Vyrai	38	41.07	1560.50
	Moterys	53	49.54	2625.50
	Total	91		

10.2 lentelė. Neparametrinis sąryšis tarp lyties grupių ir visos paveiksle užkoduotos slaptos informacijos atpažinimo statistika. Mann-Withney kriterijus.

	pav_2	pav_3	pav_5	pav_9	pav_10
Mann-Whitney U	832.500	766.000	853.500	826.000	819.500
Wilcoxon W	1573.500	1507.000	1594.500	1567.000	1560.500
Z	-1.409	-1.947	-1.239	-1.463	-1.516
Asymp. Sig. (2-tailed)	.159	.052	.215	.144	.130

	pav_2	pav_3	pav_5	pav_9	pav_10
Mann-Whitney U	832.500	766.000	853.500	826.000	819.500
Wilcoxon W	1573.500	1507.000	1594.500	1567.000	1560.500
Z	-1.409	-1.947	-1.239	-1.463	-1.516
Asymp. Sig. (2-tailed)	.159	.052	.215	.144	.130
a. Grouping Variable: Lytis					

Pagal Mann – Whitney kriterijų vidurkių rangų asymp.sign.>0,05, vadinasi galime atmesti hipotezę, kad kuri nors lytis užkoduotą informaciją atpažįsta virpinant paveikslą

10.3 lentelė. Neparametrinis sąryšis tarp regos grupių ir visos paveiksle užkoduotos informacijos atpažinimo

	Rega	N	Mean Rank	Sum of Ranks
pav_2	0	61	45.26	2761.00
	1	30	47.50	1425.00
	Total	91		
pav_3	0	61	42.89	2616.00
	1	30	52.33	1570.00
	Total	91		
pav_5	0	61	44.88	2737.50
	1	30	48.28	1448.50
	Total	91		
pav_9	0	61	47.79	2915.00
	1	30	42.37	1271.00
	Total	91		
pav_10	0	61	48.92	2984.00
	1	30	40.07	1202.00
	Total	91		
0* -asmuo nedėvi akinių ar kontaktinių lęšių, 1**- asmuo dėvi akinius ar kontaktinius lęšius				

10.4 lentelė. Neparametrinio sąryšio tarp regos ir paveikslo atpažinimo statistikos tikrinimas Mann - Whitney kriterijus

Pagal šiuos duomenis matyti, kad asymp.sig. >0,05, vadinasi galime atmesti hipotezę, kad vyrai dekoduojamą informaciją atpažįsta virpinant paveikslą prie mažesnio virpinimo dažnio nei moterys.

	pav_2		pav_3	pav_5	pav_9	pav_10
Mann-Whitney U	870.000		725.000	846.500	806.000	737.000
Wilcoxon W	2761.000		2616.000	2737.500	1271.000	1202.000
Z	-.381		-1.610	-.580	-.924	-1.510

Asymp. Sig. (2-tailed)	.703		.107	.562	.355	.131
a. Grouping Variable: Rega						

11 priedas

11.1 lentelė duomenys

Eil.nr.	Amžius	Stebėjimo laikas	Rega	Lytis	Fizinė būsena	x	y	z	!	E	S	T	M	q	n	k
1	18	17:00	0	1	1	7	9	7	15	7	7	7	7	12	7	7
2	21	17:25	0	1	1	9	11	9	11	9	9	9	15	15	15	10
3	29	17:50	1	1	1	9	9	9	9	9	9	9	9	9	9	9
4	34	17:50	0	2	1	11	11	11	11	10	10	10	13	13	11	10
5	36	18:25	0	2	1	11	11	11	11	11	11	11	11	15	11	11
6	21	18:50	0	2	1	10	10	10	10	10	10	10	10	13	10	10
7	28	19:25	0	1	2	11	11	11	11	11	11	11	10	10	10	11
8	33	19:50	1	2	2	13	13	13	22	12	12	12	13	13	13	13
9	34	20:25	0	1	2	13	14	13	18	13	13	13	14	14	14	12
10	28	20:25	1	1	2	13	17	13	17	12	12	12	12	12	12	12
11	25	20:50	1	1	2	14	14	14	14	14	14	14	14	14	14	14
12	31	12:00	0	1	1	14	13	14	13	14	14	14	13	13	13	13
13	33	12:25	1	2	1	14	14	14	18	14	14	14	18	13	13	13
14	37	12:50	0	2	1	15	15	15	15	15	15	15	13	13	13	14
15	34	13:15	1	1	1	16	16	16	16	16	16	16	17	16	15	16
16	49	13:40	0	2	1	16	19	16	19	16	16	16	15	15	14	14
17	45	14:05	0	2	1	16	16	16	16	15	15	15	16	13	13	13
18	40	13:30	0	2	1	17	19	17	19	15	15	15	17	17	17	17
19	49	13:55	0	2	1	17	17	17	22	17	17	17	17	17	17	16
20	41	14:20PM	1	2	3	17	17	17	17	17	17	17	15	15	15	15
21	42	12:10	0	2	1	17	17	17	17	17	17	17	18	17	17	15
22	43	12:35	1	2	2	17	17	17	17	17	17	17	18	18	18	14
23	22	13:00	0	1	1	9	19	9	19	9	9	9	15	12	12	10
24	29	12:00	0	1	2	9	19	9	19	8	8	8	11	11	11	9
25	32	12:25	0	2	2	19	22	19	19	19	19	19	18	18	18	17
26	29	12:50	1	2	3	16	18	18	18	18	18	18	14	14	14	15
27	27	13:15	0	1	1	11	17	11	20	9	9	9	12	12	12	9
28	22	13:40	0	1	1	11	20	11	20	11	11	11	11	11	11	12
29	46	14:05	0	2	3	10	20	20	20	18	18	18	11	9	9	18
30	37	14:30	1	2	3	25	14	25	19	18	18	18	19	19	19	17
31	51	14:45	1	2	3	21	21	21	21	16	16	16	18	18	18	15
32	53	12:00	0	2	3	21	22	21	21	19	19	19	17	17	17	17
33	45	12:25	1	1	1	15	15	15	11	15	15	15	13	13	13	14
34	27	12:50	0	1	1	15	15	15	15	12	12	12	16	16	16	13
35	44	13:15	0	2	1	19	19	19	20	9	9	9	19	22	19	12
36	20	13:40	0	1	1	7	12	7	10	7	7	7	10	10	8	8
37	22	14:05	0	2	1	9	10	9	12	9	9	9	9	9	9	9
38	27	14:30	0	1	1	6	6	6	6	6	6	6	10	6	6	6
39	29	17:30	0	1	2	11	11	11	11	11	11	11	11	11	11	10
40	24	17:55	1	1	1	11	11	11	11	11	11	11	11	11	11	9
41	28	18:20	0	1	1	10	10	10	10	10	10	10	10	10	10	11
42	24	18:45	1	1	1	11	11	11	11	11	11	11	9	9	9	10
43	34	19:10	0	1	2	12	12	12	12	14	14	14	18	18	18	8
44	41	19:35	0	1	2	12	12	12	12	12	12	12	12	12	12	13
45	34	18:05	0	2	2	12	12	12	12	12	12	12	14	12	12	12
46	33	18:30	0	2	2	14	14	14	14	14	14	14	13	13	13	11
47	31	18:55	0	1	1	14	14	14	14	14	14	14	16	14	14	14
48	29	19:20	0	2	1	14	14	14	15	14	14	14	15	15	15	15
49	40	19:45	1	2	3	15	15	15	15	15	15	15	17	15	15	14
50	44	12:10	1	2	2	16	16	16	16	12	12	12	14	12	12	12
51	41	12:35	1	2	1	16	16	16	16	16	16	16	15	15	15	14
52	43	13:00	0	2	1	16	16	16	16	16	16	16	16	16	16	15
53	44	13:25	0	2	1	17	17	17	17	13	13	13	17	17	15	13
54	45	13:50	1	2	2	17	17	17	17	17	17	17	14	14	13	14
55	47	14:15	1	2	1	17	17	17	17	16	16	16	14	17	17	15
56	31	14:40	1	2	2	17	17	17	17	17	17	17	17	14	14	13
57	31	15:05	0	2	1	17	17	17	17	17	17	17	15	15	9	15
58	29	15:30	0	2	1	14	14	14	14	12	12	12	15	15	15	12
59	27	19:00	0	1	2	13	13	13	13	12	12	12	14	14	14	11
60	17	19:25	0	1	1	7	15	7	9	8	8	8	8	8	8	9
61	33	19:50	0	1	1	10	10	10	10	10	10	10	10	9	9	9
62	31	20:15	0	1	1	11	11	11	11	12	12	12	11	11	11	11
63	22	10:30	0	1	1	11	11	11	11	11	11	11	13	13	13	11
64	41	12:00	0	1	1	18	18	16	19	11	11	11	17	17	17	14
65	44	12:25	0	1	1	19	18	19	18	17	17	17	18	18	18	16
66	57	12:50	0	2	1	20	20	20	14	18	18	18	18	18	18	15
67	36	13:15	1	1	1	14	14	14	14	12	12	12	15	15	15	11
68	34	13:40	0	1	1	15	15	15	15	15	15	15	16	16	16	13
69	42	14:05	0	2	1	15	15	15	15	15	15	15	15	15	15	14
70	44	14:30	1	2	2	19	14	19	19	18	18	18	15	15	15	16

d	A	B	C	F	f	G	g	H	H	h	p	r	J	c	g	O	?	p
7	6	6	6	11	11	11	7	7	7	7	11	11	11	9	9	6	10	6
10	9	9	9	9	12	9	9	9	9	9	13	13	10	10	10	8	11	8
9	9	9	9	9	9	7	9	9	9	9	9	9	9	9	9	8	9	9
10	10	10	10	13	13	10	10	10	10	10	12	12	12	9	9	8	10	10
11	11	11	11	16	16	12	12	11	11	11	11	11	13	12	11	9	9	11
10	11	11	11	12	12	11	10	12	12	12	20	20	11	11	11	11	10	11
11	10	10	10	11	11	11	11	10	10	10	12	12	10	10	10	10	17	10
13	11	11	11	13	13	13	13	11	11	11	15	15	18	11	11	11	16	11
12	12	12	12	15	15	12	12	12	12	12	12	12	12	12	12	10	12	12
12	11	11	11	11	13	11	11	11	11	11	15	15	11	11	11	11	13	11
14	14	14	14	14	14	14	14	13	13	13	13	13	15	14	14	12	14	14
13	13	13	13	13	20	13	15	12	12	12	12	12	14	12	12	12	12	13
13	13	13	13	15	15	15	15	13	13	13	22	22	13	13	13	11	13	13
14	12	12	12	12	12	12	12	12	12	12	14	14	12	12	12	12	12	12
16	9	9	9	16	16	16	16	9	9	9	19	19	10	10	10	9	12	9
14	13	13	13	14	14	14	14	13	13	13	18	18	13	11	13	13	14	13
13	12	12	12	16	16	16	16	12	12	12	16	16	12	12	12	12	16	12
17	9	9	9	17	17	17	17	11	11	11	16	16	11	16	9	9	16	9
16	10	10	10	17	17	17	17	10	10	10	13	13	10	10	10	10	16	10
15	12	12	12	18	20	18	18	12	12	12	16	16	13	13	13	12	12	12
15	15	15	15	19	19	19	19	15	15	15	22	22	15	15	15	13	17	13
14	14	14	14	21	21	22	22	13	13	13	20	20	16	13	14	11	11	11
10	9	9	9	17	17	17	17	10	10	10	10	10	17	9	9	9	17	9
9	15	15	15	12	12	12	12	15	15	15	12	12	13	8	13	9	9	9
17	9	9	9	18	18	18	18	9	9	9	17	17	10	13	10	9	16	9
15	17	17	17	14	12	12	12	15	15	15	12	12	12	12	17	10	10	10
9	10	10	10	17	17	17	17	11	11	11	10	10	13	12	10	10	13	10
12	11	11	11	18	18	18	18	11	11	11	11	11	11	13	11	11	11	11
18	15	15	15	20	20	20	20	15	15	15	18	18	19	19	19	15	18	15
17	18	18	18	20	25	20	20	18	18	18	22	22	20	17	18	17	17	18
15	17	17	17	21	22	22	21	16	16	16	20	20	17	17	17	17	20	17
17	18	18	18	17	17	17	17	18	18	18	17	17	16	16	16	10	11	10
14	15	15	15	12	12	12	12	13	13	13	12	12	13	13	12	9	9	11
13	14	14	14	15	15	15	15	14	14	14	13	13	15	15	14	13	15	13
12	18	18	18	17	17	17	17	13	13	13	13	13	17	17	18	18	17	18
8	7	7	7	15	15	11	11	8	8	8	9	9	15	13	13	18	18	18
9	7	7	7	12	17	12	12	9	9	9	7	7	10	10	10	7	14	14
6	8	8	8	16	16	16	8	7	7	7	8	8	16	9	9	8	8	8
10	6	6	6	10	12	12	10	6	6	6	7	7	10	10	10	6	9	9
9	10	10	10	12	15	15	15	9	9	9	10	10	12	12	12	10	10	10
11	10	10	10	12	12	12	12	10	10	10	9	9	11	11	11	10	10	10
10	10	10	10	10	10	10	10	11	11	11	10	10	13	13	13	11	13	11
8	11	11	11	11	11	13	13	11	11	11	9	9	13	10	11	11	11	11
13	13	13	13	12	12	12	14	13	13	13	13	13	13	13	13	13	13	13
12	11	11	11	14	14	14	14	11	11	11	11	11	14	11	11	11	11	11
11	13	13	13	18	18	15	15	13	13	13	12	12	18	15	13	13	13	13
17	14	14	14	15	15	15	15	14	14	14	14	14	12	16	14	12	12	12
17	15	15	15	14	14	14	14	15	15	15	15	15	20	15	15	15	15	15
17	13	13	13	12	12	12	12	13	13	13	12	12	14	11	13	13	13	13
12	12	12	12	16	16	16	16	12	12	12	12	12	16	12	12	12	12	12
16	15	15	15	18	18	18	18	15	15	15	13	13	16	13	11	15	15	15
18	15	15	15	17	17	15	15	15	15	15	15	15	18	14	18	15	15	15
13	15	15	15	14	14	14	14	15	15	15	13	13	16	13	13	13	13	13
14	13	13	13	16	16	17	17	13	13	13	10	10	18	10	10	11	11	11
15	14	14	14	18	18	18	18	14	14	14	12	12	12	12	14	14	14	14
13	12	12	12	16	16	16	16	12	12	12	11	11	15	16	11	12	12	12
15	12	12	12	15	15	15	15	12	12	12	12	12	17	11	11	12	15	15
14	13	13	13	13	13	13	13	13	13	13	15	15	22	14	14	12	16	12
13	11	11	11	14	14	14	14	11	11	11	11	11	13	10	10	10	10	10
9	7	7	7	10	10	10	10	7	7	7	8	8	15	9	9	7	10	7
12	10	10	10	13	13	13	13	10	10	10	10	10	12	9	9	10	10	10
14	12	12	12	12	12	12	12	12	12	12	12	12	15	15	12	9	9	12
11	11	11	11	13	13	13	13	11	11	11	10	10	13	13	13	11	11	11
14	17	17	17	17	17	17	14	17	17	17	17	17	16	13	13	16	16	16
16	17	17	17	18	18	18	18	17	17	17	14	14	19	14	14	16	16	16
13	18	18	18	17	17	14	14	18	18	18	13	13	17	15	13	16	18	18
11	12	12	12	14	14	12	12	13	13	13	11	11	14	11	11	13	13	13
13	15	15	15	17	17	14	14	15	15	15	13	13	15	12	15	15	15	15
14	12	12	12	14	18	14	14	12	12	12	12	12	14	11	11	10	12	12
16	16	16	16	18	18	15	15	16	16	16	18	18	16	16	16	10	15	18

j	l	e	e	e	s	S	b	c	A	i	b	S	s	a	U	2
7	7	7	7	7	7	7	9	9	6	12	9	7	7	12	6	6
10	10	10	10	10	10	9	15	9	8	12	12	9	9	11	10	9
9	9	9	9	9	9	8	11	9	9	9	9	9	9	12	9	9
11	14	10	10	10	10	10	10	10	10	12	12	10	10	12	12	9
11	11	9	9	9	9	11	11	11	11	13	13	11	11	14	11	11
11	18	11	11	11	11	10	10	10	11	12	12	11	11	11	10	10
12	17	10	10	10	10	10	10	10	10	11	13	10	10	10	10	10
10	10	11	11	11	11	12	12	12	11	12	13	12	12	12	11	11
12	12	10	10	10	10	13	13	13	12	12	12	13	15	15	10	10
12	12	11	11	11	11	11	11	11	11	11	11	11	11	11	10	10
14	14	12	12	12	12	14	16	14	14	14	14	14	14	14	9	9
13	13	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12
13	13	13	13	13	13	14	14	14	13	13	13	14	14	14	13	13
12	12	12	12	12	12	9	9	9	9	9	9	9	9	12	15	9
16	16	10	10	10	10	16	16	16	14	15	15	16	16	16	16	14
13	13	13	13	13	13	16	18	16	15	16	16	16	16	16	16	15
16	16	11	11	11	11	15	16	15	12	16	16	15	15	17	15	12
16	16	10	10	10	10	15	18	15	14	14	14	15	15	18	15	15
18	18	11	11	11	11	17	17	17	14	14	14	16	16	16	16	16
17	22	12	12	12	12	17	17	17	16	16	16	17	16	16	17	14
19	19	11	11	11	11	17	17	17	15	15	15	15	15	15	15	15
13	13	11	11	11	11	17	17	17	14	16	16	14	14	14	16	13
9	9	8	8	8	8	9	12	9	9	9	9	9	9	12	16	10
12	12	10	10	10	10	8	8	8	8	8	8	8	8	15	12	8
10	10	9	9	9	9	19	19	19	19	18	18	19	19	19	17	12
10	10	10	10	10	10	18	18	18	16	16	16	19	18	16	16	16
11	11	11	11	11	11	9	17	9	9	9	9	9	11	17	11	9
12	16	12	12	12	12	11	11	11	11	11	11	11	12	14	11	11
17	17	9	9	9	9	18	18	19	16	16	16	17	17	17	17	15
17	17	17	17	17	17	18	18	17	17	17	17	18	18	18	17	16
17	20	18	18	18	18	16	16	16	16	16	16	16	18	16	18	16
13	13	11	11	11	11	19	19	19	17	18	18	17	17	17	17	12
11	11	9	9	9	9	15	15	15	15	15	15	15	15	15	18	15
17	17	11	11	11	11	12	12	12	12	12	12	12	12	12	12	10
17	17	18	18	18	18	12	12	12	12	12	12	12	12	12	11	11
12	12	18	18	18	18	12	7	14	7	7	7	7	7	7	10	7
9	9	7	7	7	7	9	9	10	8	8	8	9	9	9	8	8
9	12	8	8	8	8	6	6	6	6	6	6	6	8	8	11	6
11	11	6	6	6	6	11	11	11	6	10	10	11	11	11	10	10
12	17	10	10	10	10	11	11	11	10	10	10	11	11	11	10	9
10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10	10
13	13	10	10	10	10	12	12	12	10	11	11	11	11	11	10	10
9	12	9	9	9	9	15	15	15	11	11	11	15	11	11	16	10
13	18	12	12	12	12	14	14	14	13	13	13	13	13	13	14	12
12	19	11	11	11	11	13	13	13	11	11	11	11	11	11	11	11
12	16	13	13	13	13	14	14	14	13	13	13	13	13	13	13	13
13	16	13	13	13	13	15	18	15	14	14	14	14	14	14	14	14
14	19	14	14	14	14	16	16	16	15	15	15	15	15	15	14	14
12	12	11	11	11	11	13	13	13	13	13	13	13	13	13	12	12
14	14	12	12	12	12	12	12	12	11	12	12	11	11	11	12	12
13	13	12	12	12	12	16	16	16	15	15	15	16	19	21	15	13
13	18	15	15	15	15	16	16	16	15	15	15	16	15	15	15	15
12	14	11	11	11	11	13	13	13	15	13	13	13	13	17	14	11
10	12	9	9	9	9	17	17	16	13	13	13	13	13	13	9	9
11	11	11	11	11	11	17	17	17	14	14	14	14	14	14	11	11
11	14	10	10	10	10	16	16	16	13	14	16	13	13	13	12	10
13	16	12	12	12	12	12	12	12	12	12	12	12	12	12	14	12
12	12	12	12	12	12	15	15	15	13	14	14	13	13	16	12	12
11	11	10	10	10	10	10	11	11	11	11	11	15	10	10	10	10
10	11	7	7	7	7	11	11	11	7	12	12	10	10	10	12	8
10	10	9	9	9	9	10	10	10	10	10	10	9	9	9	9	9
12	15	9	9	9	9	15	15	15	12	13	13	12	12	12	10	10
9	12	12	12	12	12	10	10	10	11	11	11	10	12	12	13	10
13	13	16	16	16	16	16	16	16	17	17	17	16	18	18	15	15
14	18	16	16	16	16	17	17	17	17	17	17	17	16	16	15	15
13	13	16	16	16	16	18	18	18	18	18	19	17	17	20	17	17
11	12	14	14	14	14	12	12	12	12	12	12	11	11	11	15	12
12	15	12	12	12	12	15	15	15	15	15	15	13	15	15	14	12
11	11	9	9	9	9	15	15	15	12	15	15	11	15	15	15	9
10	10	10	10	10	10	17	17	17	16	16	16	17	16	16	16	16

R	v	K	D	m	l	w	W	L	Q	w	l	t	X	Y	Z	u	o	v	kvadratas	N
6	7	7	7	7	17	7	7	7	7	7	17	15	7	7	7	8	8	8	7	9
9	11	9	9	15	10	9	9	9	9	9	10	18	9	9	9	12	9	9	9	15
9	9	9	9	9	9	9	9	9	9	9	9	15	6	6	6	6	6	6	8	10
9	10	10	10	11	12	10	10	10	10	10	12	12	15	15	15	12	12	12	15	12
11	11	9	9	11	11	11	11	11	11	11	11	18	18	18	18	18	15	15	18	18
10	10	12	12	10	20	10	10	10	10	10	20	22	15	15	15	15	15	15	10	15
10	11	9	9	10	12	11	11	11	11	11	12	15	10	10	10	15	15	15	7	7
11	12	11	11	13	15	12	12	12	12	12	15	15	9	15	9	9	9	9	8	8
10	13	10	10	14	12	13	13	13	13	13	12	10	9	9	9	9	9	9	9	9
10	12	10	10	12	15	12	12	12	12	12	15	17	13	13	13	18	18	18	17	18
9	14	12	12	14	13	14	14	14	14	14	13	18	15	15	15	15	15	15	15	15
12	14	12	12	13	12	14	14	14	14	14	12	11	11	11	11	11	11	15	11	11
13	14	11	11	13	22	14	14	14	14	14	22	18	12	12	12	12	12	12	11	11
9	15	9	9	13	14	15	15	15	15	15	14	15	13	13	13	16	16	16	12	12
14	16	10	10	15	18	16	16	16	16	16	18	13	13	13	13	13	13	13	13	13
15	16	11	11	14	18	16	16	16	16	16	18	11	11	11	11	11	13	11	11	11
12	15	11	11	13	16	15	15	15	15	15	16	16	16	16	16	16	16	16	16	16
15	15	10	10	17	16	15	15	15	15	15	16	20	18	18	18	18	18	18	18	18
16	17	10	10	17	13	17	17	17	17	17	13	16	14	18	14	12	14	12	14	14
14	17	9	9	15	16	17	17	17	17	17	16	16	13	13	11	13	13	13	11	11
15	17	11	11	17	22	17	17	17	17	17	22	14	11	14	11	11	11	11	11	14
13	17	9	9	18	20	17	17	17	17	17	20	10	10	10	10	10	10	12	11	11
10	9	12	12	12	10	9	9	9	9	9	10	15	12	12	12	18	15	15	12	18
8	8	12	12	11	12	8	8	8	8	8	12	15	12	12	12	12	12	12	12	12
12	19	13	13	18	17	19	19	19	19	19	17	13	13	13	13	13	13	13	13	13
16	18	6	8	14	12	18	18	18	18	18	12	15	6	6	6	6	6	6	6	6
9	9	9	9	12	10	9	9	9	9	9	10	17	15	15	15	12	12	12	15	15
11	11	11	11	11	11	11	11	11	11	11	11	15	14	14	14	12	12	12	12	12
15	18	8	8	18	18	18	18	18	18	18	18	15	15	15	15	15	15	15	13	13
16	18	10	10	19	22	18	18	18	18	18	22	10	10	10	10	10	15	10	10	10
16	16	9	9	18	20	16	16	16	16	16	20	14	14	14	14	14	14	14	9	9
12	19	8	8	17	17	19	19	19	18	19	17	14	10	10	10	9	9	9	8	11
15	15	8	9	13	12	15	15	15	15	15	12	10	9	9	9	10	10	10	10	10
10	12	9	9	16	13	12	12	12	12	12	13	12	11	11	11	9	9	9	8	8
11	9	12	12	18	13	9	9	9	9	9	13	18	16	16	16	16	16	16	16	16
7	7	7	7	8	9	7	7	7	7	7	9	7	7	7	7	7	7	7	7	7
8	9	8	8	9	7	9	9	9	9	9	7	9	8	8	8	9	9	9	8	9
6	6	6	6	6	8	6	6	6	6	6	8	6	6	6	6	8	8	8	6	8
10	11	10	10	11	7	11	11	11	11	11	7	11	10	10	10	11	11	11	10	11
9	11	9	9	22	10	11	11	11	11	11	10	11	9	9	9	11	11	11	9	11
10	10	10	10	10	9	10	10	10	10	10	9	10	10	10	10	10	10	10	10	10
10	11	10	10	9	10	11	11	11	11	11	10	11	10	10	10	11	11	11	10	11
10	14	10	10	9	9	14	14	14	14	14	9	14	10	10	10	11	11	11	10	11
12	12	10	10	12	13	12	12	12	12	12	13	12	10	10	10	13	13	13	10	13
11	12	11	11	12	11	12	12	12	12	12	11	12	11	11	11	11	11	11	11	11
13	14	14	14	13	12	14	14	14	14	14	11	14	14	14	14	13	13	13	14	13
14	14	13	13	14	14	14	14	14	14	14	14	14	13	13	13	14	14	14	13	14
14	14	14	14	15	15	14	14	14	14	14	15	14	14	14	14	15	15	15	14	15
12	15	10	10	15	12	15	15	15	15	15	12	15	10	10	10	13	13	13	10	13
12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	11	11	11	12	11
13	16	13	13	15	13	16	16	16	16	16	13	16	13	13	13	21	21	21	13	21
15	16	15	15	16	15	16	16	16	16	13	15	16	15	15	15	15	15	15	15	15
11	13	11	11	15	13	13	13	13	13	13	13	13	11	11	11	17	17	17	11	17
9	17	9	9	13	10	17	17	17	17	17	10	17	9	9	9	13	13	13	9	13
11	16	11	11	17	12	16	16	16	16	16	12	16	11	11	11	14	14	14	11	14
10	17	10	10	14	11	17	17	17	17	17	11	17	10	10	10	13	13	13	10	13
12	17	12	12	9	12	17	17	17	17	17	12	17	12	12	12	12	12	12	12	12
12	12	12	12	15	15	12	12	12	12	12	15	12	12	12	12	16	16	16	12	16
10	12	10	10	14	11	12	12	12	12	12	11	12	10	10	10	10	10	10	10	10
8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	10	10	10	8	10
9	10	9	9	9	10	10	10	10	10	10	10	10	9	9	9	9	9	9	9	9
10	12	10	10	11	12	12	12	12	12	12	12	12	10	10	10	12	12	12	10	12
10	11	10	10	13	10	11	11	11	11	11	10	11	10	10	10	12	12	12	10	12
15	16	15	15	17	17	16	16	16	16	16	17	16	15	15	15	18	18	18	15	18
15	17	15	15	18	14	17	17	17	17	17	14	17	15	15	15	16	18	18	15	16
17	18	17	17	18	13	18	18	18	18	18	13	18	17	17	17	20	20	20	17	20
12	1	12	12	15	11	12	12	12	12	12	11	12	12	12	12	11	11	11	12	11
12	15	12	12	16	13	15	15	15	15	15	12	15	12	12	12	15	15	15	12	15
9	15	9	9	15	12	15	15	15	15	15	12	15	9	9	9	15	15	15	9	15
16	18	16	16	15	18	18	18	18	18	18	18	18	16	16	16	16	16	16	16	16

0 – dėvi akinius ar kontaktinius lęšius; 1 – nedėvi akinių ar kontaktinių lęšių. 1 – vyras, 2 – moteris

11.2 lentelė. Duomenys

					AsK	Vgt	iFd	gerg	Meg	KTI	Gm	drej	beF	SaM	
Nr.	**Lytis**	**Amžius**	**Akiniai**	**Valanda**	**1 pav.**	**2 pav.**	**3 pav.**	**4 pav.**	**5 pav.**	**6 pav.**	**7 pav.**	**8 pav.**	**9 pav.**	**10 pav.**	**Vidurkis**
9	V	14	ne	14.30	18	14	\	16	12	14	15.5	14	13	12.5	14.33333
21	V	15	ne	14.00	15.5	13.5	12.5	13	11	13	10	12	11	10	12.15
18	V	18	ne	10.00	10	9.5	8.5	7	6	6	5.5	5	5	4.5	6.7
19	M	18	ne	13.00	15.5	16.5	16.5	10	9	13	11	9	8	8.5	11.7
3	M	20	ne	15.00	20	15	13	13	13	10.5	11	11	12	13	13.15
15	M	20	ne	19.00	21	18	15	14	11.5	12.5	10	13	11.5	15	14.15
20	V	20	taip	13.30	16	13.5	13	10.5	14	11.5	11.5	11	8.5	8.5	11.8
40	M	20	ne	16.00	18.5	15.5	14	12.5	11	11.5	11	11	10	9.5	12.45
47	M	20	ne	15.35	20	15	14.5	13	10.5	11.5	11	12	10	10	12.75
56	M	20	ne	12.35	17	14	12	11	11.5	11	10.5	9.5	9	10	11.55
7	V	21	ne	20.00	15	15	14	13	15	14	13	12	14	12	13.7
24	V	21	ne	16.00	10.5	13	10	12.5	10.5	10	10	9.5	9.5	9	10.45
31	V	21	taip	10.00	14	12	11	9.5	10	9.5	9.5	8.5	8.5	9	10.15
58	M	21	ne	17.00	15.5	13.5	14	12	11.5	11.5	11	10.5	11	12	12.25
60	V	21	ne	11.35	15	14	13.5	13	11.5	10	9.5	8.5	9	8	11.2
25	M	22	ne	16.30	15	11.5	14	12	15	9.5	12.5	12	13	11	12.55
27	V	22	ne	15.00	18	12.5	11	14	11.5	12	10	9.5	10	10.5	11.9
32	M	22	ne	13.00	18	14	12.5	12.5	12	10	10.5	9.5	9	8.5	11.65
44	V	22	ne	17.15	21	16.5	15	15.5	14.5	13.5	12	12.5	11.5	11.5	14.35
46	V	22	taip	10.00	14.5	13	12	12	10.5	10.5	10	9	9	8	10.85
57	V	22	ne	13.15	16	14.5	13	12.5	12	10	10.5	10	10	9.5	11.8
33	M	23	taip	13.30	18.5	13.5	13.5	12	13	10	10	11.5	9.5	9.5	12.1
34	M	23	ne	14.00	16	15	14	11	14.5	10	9.5	9	9.5	10	11.85
41	V	23	taip	18.00	20	15.5	15.5	15	14.5	14	14.5	11.5	11	11	14.25
43	M	23	ne	11.00	15.5	14	15	12.5	11.5	10.5	11	9.5	9	9	11.75
54	V	23	ne	10.00	14.5	13	11	10	9.5	9	8	8.5	8.5	8	10
6	V	24	ne	12.00	10	9.5	12.5	11	13	8.5	8	9.5	7.5	8.5	9.8
30	M	24	taip	12.00	15	13	11.5	10	9.5	10.5	9.5	8	8.5	8.5	10.4
35	V	24	ne	12.00	17	14.5	13	11.5	11.5	11	11.5	9.5	9	8.5	11.7
53	V	24	ne	9.45	13.5	12.5	10.5	10	9	9	7.5	9	8.5	9.5	9.9
23	V	25	taip	21.00	24	16	15	12	12	12.5	14.5	15	13.5	15.5	15
29	V	25	ne	8.00	13.5	12.5	11	10	9	9.5	10	8.5	8	8.5	10.05
48	M	25	ne	19.00	23.5	15.5	15.5	15	14.5	14	12.5	13.5	10.5	15	14.95
14	V	27	ne	13.00	16	13.5	11	11	11.5	10.5	8	9.5	11	8.5	11.05
26	M	30	taip	16.00	20	14	14	12	12.5	13.5	11	11.5	12	12.5	13.3
51	M	30	ne	10.00	15	13	11.5	11.5	10	9.5	8.5	10	8	8.5	10.55
13	M	32	taip	14.00	15.5	13.5	12.5	13.5	14	16	13	13	14	13	13.8
10	M	33	taip	21.00	21	16	15	15.5	23	15.5	15	15	14	13	16.3
37	V	33	ne	10.00	16	12.5	13.5	10	11.5	11.5	11	10.5	9.5	9.5	11.55
28	V	34	ne	12.00	19.5	16	14	13	13.5	14	12.5	11	10	10.5	13.4
36	M	34	ne	9.00	15.5	13	12	10.5	10.5	9.5	9.5	10	9	8.5	10.8
2	V	35	ne	14.00	14	14	14	13.5	14	12	14	14.5	12	13	13.5
38	M	36	taip	10.35	16	13	14	10	12	11.5	11	10	10	9.5	11.7
45	V	36	taip	19.00	23	16.5	15.5	16	15	14	13	12	11	11.5	14.75
42	V	37	ne	16.45	21.5	16	15.5	15	14	14	12.5	12	11.5	10	14.2
52	M	37	ne	16.35	17.5	15	15.5	14	13	12.5	10.5	9.5	9.5	10	12.7
1	M	38	ne	13.15	21	13	12	14	11	10.5	11.5	11.5	11.5	13	12.9
49	V	38	ne	12.00	15	14.5	13.5	11.5	10.5	10	10.5	11	9	9.5	11.5
59	M	40	ne	18.00	19	16	14.5	14.5	13.5	12.5	14	11	12	11.5	13.85
50	M	41	ne	14.00	17	18	15.5	13.5	15	15.5	13.5	15	14.5	12.5	15
55	M	41	taip	12.00	15.5	14	11.5	11.5	10.5	10	8.5	9.5	9	9	10.9
17	M	43	taip	14.20	17	20	16	12.5	15	19	12	11	11	11	14.45
22	V	44	ne	15.00	15	15.5	16.5	13	14	15	14.5	14	12	12	14.15
39	M	45	taip	13.30	17.5	13	14	10.5	11.5	12	11.5	11	10.5	10	12.15
4	M	47	ne	13.15	16.5	15	16	15	15.5	14	14	13	13	12	14.4
5	V	50	ne	13.45	14	14	15	14	15	13	12	12.5	14	11	13.45
16	M	50	taip	9.00	14.5	9.5	9	9.5	8.5	9	8.5	9.5	8.5	8	9.45
8	M	55	ne	20.30	21.5	16.5	16	14	21.5	15.5	15	16	14	15	16.5
12	M	59	taip	10.00	15	13.5	12.5	12	11.5	11	10.5	9	9	9	11.3
11	M	60	ne	18.00	16	15	14	15	14	15	14.5	14.5	13	12	14.3

1	V	23	Taip	-	Taip	15.45	25	22	40	20	20	25	16	25	18	14	22.5
2	M	41	Ne	-	-	15.45	28	26	32	18	26	21	24	22	23	18	23.8
3	M	24	Ne	-	-	15.45	14	16	30	20	20	20	18	25	18	12	19.3
4	M	54	Ne	-	-	16.15	30	26	32	20	24	22	20	25	22	17	23.8
5	M	24	Ne	-	-	10.45	24	32	45	28	18	24	18	22	22	19	25.2
6	V	19	Ne	-	-	11.55	24	45	40	18	10	14	10	28	16	10	21.5
7	M	43	Ne	-	-	17.00	18	24	30	22	15	18	15	19	19	16	19.6
8	M	54	Taip	Taip	-	13.00	32	45	32	32	29	25	18	25	21	18	27.7
9	M	25	Ne	-	-	18.50	25	30	30	28	25	20	22	34	24	27	26.5
10	V	27	Ne	-	-	19.50	28	30	30	25	15	18	14	18	24	14	21.6
11	M	24	Taip	-	Taip	17.40	23	47	32	30	18	16	16	22	20	19	24.3
12	M	25	Ne	-	-	17.40	19	25	36	24	16	20	18	22	24	22	22.6
13	M	22	Ne	-	-	17.40	34	28	34	26	22	26	24	25	22	20	26.1
14	V	28	Ne	-	-	12.00	27	26	30	30	19	22	20	24	20	18	23.6
15	M	37	Ne	-	-	14.30	31	40	28	25	22	26	17	28	25	21	26.3
16	M	14	Ne	-	-	14.30	24	26	22	19	18	27	20	28	24	17	22.5
17	V	11	Ne	-	-	14.30	22	32	28	26	18	29	19	32	30	19	25.5
18	M	25	Taip	-	Taip	11.00	28	39	36	32	24	27	24	25	27	20	28.2
19	M	23	Ne	-	-	11.00	32	37	34	30	21	27	18	26	24	18	26.7
20	M	41	Taip	Taip	-	15.20	37	48	44	36	30	26	22	32	28	24	32.7
21	V	27	Taip	Taip	-	16.00	42	39	36	32	26	29	20	24	25	22	29.5
22	M	24	Ne	-	-	16.00	25	33	36	24	19	25	17	27	27	19	25.2
23	V	29	Ne	-	-	16.00	21	27	30	18	16	22	21	25	24	19	22.3
24	V	26	Ne	-	-	16.00	23	31	32	21	16	24	18	26	25	21	23.7
25	M	33	Taip	-	Taip	10.40	43	50	39	29	30	30	24	30	28	18	32.1
26	M	27	Ne	-	-	16.50	35	40	28	19	22	24	18	24	22	20	25.2
27	V	28	Taip	-	Taip	16.50	39	47	38	26	24	28	20	28	26	22	29.8
28	M	25	Ne	-	-	16.50	30	38	43	29	20	28	22	26	30	22	28.8
29	V	15	Ne	-	-	13.15	20	34	37	20	18	24	18	21	24	24	24
30	M	18	Ne	-	-	13.15	26	34	39	17	25	24	22	21	27	24	25.9
31	M	46	Ne	-	-	13.15	34	42	34	28	30	29	24	25	29	26	30.1