KAUNO TECHNOLOGIJOS UNIVERSITETAS

FUNDAMENTALIŲJŲ MOKSLŲ FAKULTETAS

TAIKOMOSIOS MATEMATIKOS KATEDRA

Irma Zenkevičiūtė

Skaitmeninių vandens ženklų naudojimas paveikslėliuose

Magistro darlas

Vadovas
prof. Dr. E. Sakalauskas

KAUNAS, 2011

KAUNO TECHNOLOGIJOS UNIVERSITETAS

FUNDAMENTALIŲJŲ MOKSLŲ FAKULTETAS

TAIKOMOSIOS MATEMATIKOS KATEDRA

TVIRTINU
Katedros vedėjas
doc. dr. N. Listopadskis
2011 06 02

Skaitmeninių vandens ženklų naudojimas paveikslėliuose

Taikomosios matematikos magistro baigiamasis darlas

Vadovas
prof. dr. E. Sakalauskas
2011 06 01

Recenzentas
doc. B. Tamulynas
2011 06 01

Atliko
FMMM 9 gr. stud.
I. Zenkevičiūtė
2011 05 30

KAUNAS, 2011

KVALIFIKACINĖ KOMISIJA

Pirmininkas: Leonas Saulis, profesorius (VGTU)

Sekretorius: Eimutis Valakevičius, docentas (KTU)

Nariai: Algimantas Jonas Aksomaitis, profesorius (KTU)

Vytautas Janilionis, docentas (KTU)

Vidmantas Povilas Pekarskas, profesorius (KTU)

Rimantas Rudzkis, habil. dr., vyriausiasis analitikas (DnB NORD Bankas)

Zenonas Navickas, profesorius (KTU)

Arūnas Barauskas, dr., vice-prezidentas projektams (UAB „Baltic Amadeus“)

Zenkevičiūtė I. Skaitmeninių vandens ženklų naudojimas paveikslėliuose, Taikomosios matematikos magistro darbas / vadovas doc. dr. E. Sakalauskas; Taikomosios matematikos katedra, Fundamentaliųjų mokslų fakultetas, Kauno technologijos universitetas. – Kaunas, 2011. -42p

SANTRAUKA

Būtinybė apsaugoti autorinių teisių savininkus nuo neteisėto intelektinės nuosavybės naudojimosi ir platinimo vis didėja. Tam puikiai tinka skaitmeniniai vandens ženklai, kurie ne tik apsaugo nuo neleistino intelektinės nuosavybės naudojimosi, bet pasinaudojus vandens ženklais galima susekti neteisėtą vartotoją.

Šiame darbe aptarta diskrečioji kosinuso transformacija (angl. *Discrete Cosine Transform (DCT)*) ir išplėsto spektro (angl. *Spread-Spectrum*) ženklinimo vandens ženklais metodai, plačiau išnagrinėtas DCT metodas ir patikrinta keletas paprastų vaizdo atakų, kaip antai: karpymas, suspaudimas, pasukimas ir pan.

Dalies vaizdo iškirpimas, pasukimas gali neatpažįstamai pakeisti vandens ženklą. Taip nutinka, nes iš pakeisto paveikslėlio ištraukiant vandens ženklą priešingu įterpimui metodu pasikeičia vaizdo taškų koordinatės, o iškirpus dalies koordinačių trūksta. Priklausomai nuo posūkio kampo ar iškirptos dalies dydžio sugadinamas ir vandens ženklas, kuris nepasikeičia keičiant spalvą ar kontrastą.

Zenkevičiūtė I. Digital watermarking for image: Master's work in applied mathematics / supervisor doc. dr. E. Sakalauskas; Departament of Applied mathematics, Faculty of Fundamental Sciences, Kaunas University of Technology. – Kaunas, 2011. -42p.

SUMMARY

The necessity to protect copyright owners from using and sharing illegal intellectual property still grows. Digital water marks fits perfectly for this matter. They not only prevent using illegal intellectual property, but they can also detect illegal user.

In this paper the discrete cosine transform (DCT) and spread-spectrum water-marking methods were discussed, and DCT method was analysed, and several image attacks were tested, such as: trimming, compression, rotation and etc.

The trimming a part of an image, rotation of an image can change water mark beyond recognition. It happens because taking water mark out from changed image using inverse method of insertion image pixel coordinates change, and trimming causes a missing of part of coordinates. Depending on the angle of rotation or the size of a trimmed part a water mark is corrupted, but it does not change when a colour or a contrast is being changed.

TURINYS

LENTELIŲ SĄRAŠAS

PAVEIKSLĖLIŲ SĄRAŠAS

ĮVADAS

IT (informacinės technologijos) labiausia vystoma ir perspektyviausia veiklos sritis, kurios taikymo spektras yra labai platus ir susijęs su greitu ir efektyviu skaitmeninės informacijos perdavimu ir apdorojimu. Išskiriamos dvi pagrindinės tendencijos:

- Skaitmeninė informacija persiunčiama privačiais tinklais (įmonių intranetas);
- Laisvai prieinama ir platinama „Internete“.

Įvairių tipų tinklai vis dažniau sujungiami, todėl mokama informacinė medžiaga gali būti perduodama bendrojo naudojimo tinklais. Taigi kyla klausimas: kaip tokią medžiagą reiktų apsaugoti nuo jos nelegalaus naudojimo ir kopijavimo? Daugiaterpės informacijos apsaugai naudojamos dviejų pagrindinių rūšių priemonės:

- Technologijoms informacijos savininkai gali riboti ir kontroliuoti, kas patenka į tas tinklo sritis, kuriose yra jiems priklausantys skaitmeniniai objektai (norint apsilankyti šiuo būdu saugomoje svetainėje, privalu turėti vartotojo vardą ir slaptažodį).
- Autorių teisės saugomos „vandens ženklais“. Iš esmės skaitmeninis vandens ženklas yra tam tikras vaizdo elementų derinys, kuris įmontuojamas naudojant slaptą raktą į failą. Jis nepakeičia kokybės; negalima aptikti vizualiai. Ženklai turi tenkinti tam tikrus reikalavimus: nedingti archyvuojant failą, keičiant formatą arba po daugkartinių vertimų iš analogo į kodą ir atvirkščiai. Be to, vandens ženklo signalas turi būti suderintas su vaizdo signalu, nes kitaip išnyks apdorojant vaizdą. Vandens ženklą gali sudaryti įvairios rūšies informacija: tekstas, dvejetainis kodas, televizijos programos, užsakovo ar gamintojo firminis ženklas. Jį kuriant reikalingas sudėtingas matematinis aparatas.

Šiame darbe aptariama keletas gerai žinomų ir dažniausia taikomų vandens ženklų įterpimo į vaizdinius failus ir ištraukimo metodų. Taip pat sukurta elementari programėlė MATLAB paketu, kurios pagalba galime įterpti vandens ženklą į vaizdinį failą, taip pat atvirkštinė operacija vandens ženklo ištraukimas. Atliekama vaizdo su įterptu vandens ženklu transformacijų: apkarpymas, suspaudimas, paveikimas baltuoju triukšmu ir pan. Tam, kad išsiaiškintume, vandens ženklo atsparumą vaizdo apdorojimui elementariomis priemonėmis.

1. BENDROJI DALIS

1.1. VANDENS ŽENKLAI

Vandens ženklas – tai atpažįstamas vaizdas ar šablonas popieriuje, atrodantis kaip įvairių atspalvių šviesesnis/tamsesnis žiūrint prieš šviesą (ar žiūrint iš atsispindėjusios šviesos ant tamsaus fono), kurį sukelia popieriaus storis ar tankio pokyčiai [2]. Yra du pagrindiniai vandens ženklų gamybos popieriuje būdai; (*dandy roll process)* ir sudėtingesnis cilindro formos procesas (*cylinder mould process)*.

Vieni vandens ženklai yra akivaizdūs atsitiktiniame patikrinime, kiti reikalauja tyrimų. Jiems išskirti sukurta keletas pagalbinių priemonių, kaip vandens ženklų skystis. Vandens ženklai dažnai naudojami kaip apsaugos požymis banknotuose, pasuose, pašto ženkluose ir kituose dokumentuose, kad būtų užkirstas kelias padirbinėjimui. Taip pat jie labai naudingi, popieriaus tyrime, nes jis gali būti naudojamas pažinimui, nurodant dydį, gamyklų prekių ženklus ir vietą, ir popieriaus kokybę.

1.2. SKAITMENINIAI VANDENS ŽENKLAI

Ženklinimas skaitmeniniais vandens ženklais – tai procesas įtvirtinantis informaciją į skaitmeninį signalą taip, kad būtų sunku pašalinti. Terminas kilęs iš proceso naudojamo nuo 1282 popieriuje matomų vandens ženklų gamyboje. Skaitmeniniuose vandens ženkluose, signalas gali būti garso, vaizdo įrašas ar nuotrauka. Jei signalas kopijuojamas, tai informacija taip pat perduodama kopijai. Signalas gali gabenti keletą skirtingų vandens ženklų tuo pačiu metu.

Vandens ženklai skirstomi į:

- Matomus. Nuotraukoje ar vaizdo įraše yra matomas skaitmeninis vandens ženklas. Paprastai tai būna tekstas ar logotipas, kuris indentifikuoja savininką. Kai televizijos transliuotojas priduria savo logotipą perduodamo vaizdo kampe, tai taip pat yra matomas vandens ženklas.
- Nematomus. Nematomuose skaitmeniniuose vandens ženkluose informacija pridedama kaip skaitmeniniai garso, vaizdo ar vaizdo įrašo duomenys, tačiau jis nesuvokiamas kaip toks (nors įmanoma nustatyti, kad yra paslėpta informacija signale). Vandens ženklas gali būti skirtas plačiam vartojimui, todėl lengva susigražinti kaip iš steganografijos, kai perduodamas slaptas pranešimas įterpiant į skaitmeninį signalą.

Matomo vandens ženklo tikslas yra susieti nuosavybę ar kitokią aprašomojo pobūdžio informaciją, kad signalą būtų sunku pašalinti. Taip pat galima naudoti paslėptą informaciją kaip slaptą asmeninio bendravimo priemonę.

Viena iš vandens ženklų taikymo sričių yra autorių teisių apsaugos sistema, kuri skirta užkirsti kelią ar atgrasyti nuo neteisėto kopijavimo. Šiuo atveju, kopijavimo prietaisas nuskaito nuo signalo vandens ženklą prieš priimant kopiją; prietaisas priima sprendimą kopijuoti ar ne, priklausomai nuo vandens ženklo turinio. Kitas taikymas yra pirminis kopijavimas. Jei darbo kopija randama vėliau, tai vandens ženklas gali būti išgautas iš kopijos ir platinimo šaltinį galima nustatyti. Šis metodas naudojamas siekiant aptikti nelegaliai nukopijuotų filmų šaltinį.

Rūpindamosi garso signalo apsauga “IBM”, “NEC”, “Hitachi”, “Pioneer” ir “Sony” 1999 metų vasario 17 dieną sujungė jėgas ir sukūrė “Galaxy Group”. Principas buvo pasirinktas “Watermarking” (vandens ženklai). Vandens ženklai visam laikui pažymi kiekvieną garso ar vaizdo kadrą garsu (triukšmu), kuris teoriškai nėra girdimas ar matomas žmogui. Vandens ženklai gali būti atpažinti grotuvų ar kopijavimo įrenginių, net kai signalas yra paverčiamas iš skaitmeninio į analoginį ar kai jis tik papildo vaizdo takelį. Vandens ženklai tai ne užkodavimas, o greičiau būdas identifikuoti ar vaizdo (garso) kopija ar gabalas gali būti kopijuojamas ar grojamas.

Šios apsaugos sistemos yra taikomos tik tam, kad nebūtų piktnaudžiaujama kopijavimo galimybėmis (tai kasmet padaro milijardus dolerių nuostolių filmų ir programų gamintojams). DVD apsaugos sistemų pradininkai pripažįsta, kad tokiu būdu neužkirs kelio “piratams”.

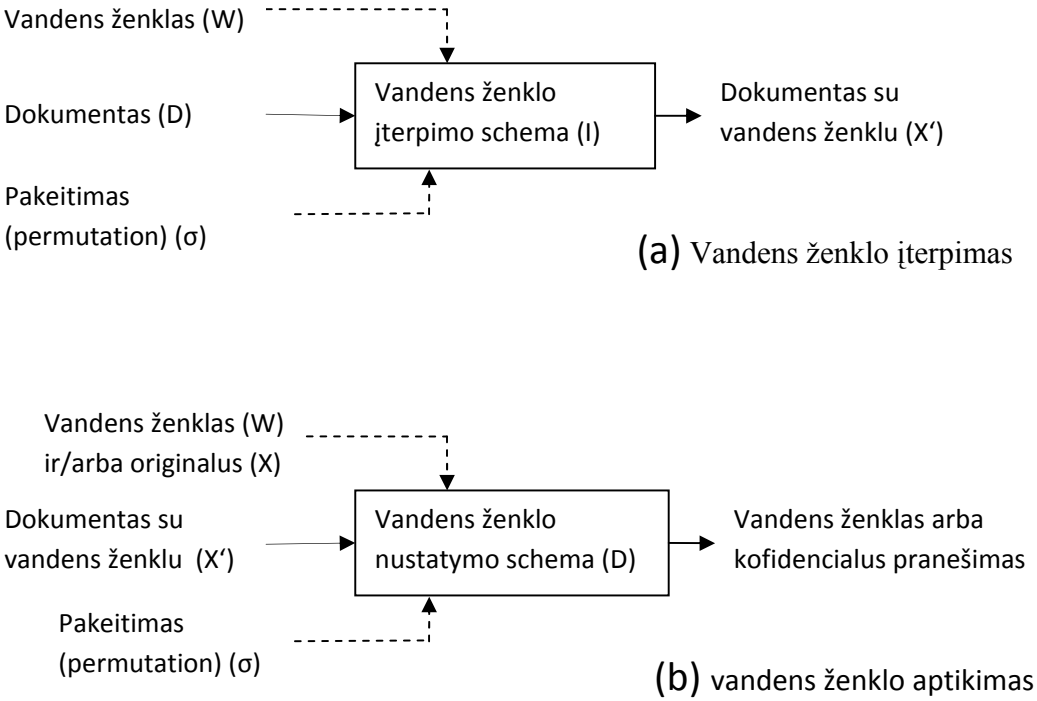
Dar vienas nematomų ženklų taikymas yra skaitmeninės fotografijos su aprašomojo pobūdžio informacija. Nors kai kurių failų formatai skaitmeninėje medijoje gali būti papildomos informacijos vadinamas metaduomenims, skaitmeninių vandens ženklų yra skiriamasis požymis, kad duomenys tvarkomi teisingai signale.

Vandens ženklai taip pat gali būti naudojami slaptam bendravimui, į kokį nors failą įterpiamas pranešimas, kaip vandens ženklas, kurį gali aptikti tik žinantys, kokiu būdu jis buvo įterptas.

Taigi skaitmeniniai vandens ženklai dažniausia taikomi:

- Autorių teisių apsaugai
- Šaltinių sekimui (skirtingi gavėjau gauna vandens ženklus su skirtingu turiniu)
- Transliacijos stebėjimas (televizijos naujienų vaizdo įrašai dažnai yra su tarptautinių agentūrų vandens ženkliais)
- Slaptam bendravimui.

1.3. ŽENKLINIMO VANDENS ŽENKLAIS SCHEMOS PRINCIPAS



1.1. pav. Vandens ženklo įterpimo (a) ir aptikimo (b) procesų schema

Nagrinėjama vandens ženklų schema naudoja signalo apdorojimo technologiją apdirbti vandens ženklo signalą skaitmeninio dokumento dalyje. Esama ženklinimo schema paprastai apima dvi stadijas: vandens ženklo įterpimas ir jo nustatymas, kaip parodyta 1.1. paveikslėlyje. Tarkime turime skaitmeninį dokumentą X, vandens ženklą W ir pakeitimo funkciją σ. Vandens ženklo įterpimo schema I įterpia vandens ženklą W į dokumentą X, kur:

$$X' = I(X, W, \sigma)$$

Aiškinant pagrindinį įterpimo schemos principą, iliustravimui dažnai naudojama praplėsto spektro (spreed spectrum) ženklinimo technika, aprašyta Cox [11]. Praplėsto spektro technikoje (i) dokumento „savybė“ yra vektorius t.y. $X = \{x_1, x_2, \dots, x_n\}$ ir (ii) vandens ženklo signalas yra „vandens ženklo elemento“ vektorius t.y. $W = \{w_1, w_2, \dots, w_m\}$, kai $n \geq m$. Užrašas, kad savybių skaičius dokumente turi būti daug didesnis, nei komponenčių skaičius vandens ženklo signale, taigi signalas yra nepastebimas paženklintame dokumente X'. Pakeitimo funkcija σ yra bijekcija, kad vandens ženklo elementas būtų įtraukiamas į dokumentą X. Tarkime išmaišytas vandens ženklas yra vektorius $\sigma(W) = \{w_1', w_2', \dots, w_m'\}$,

kur $w_i^{'} = \sigma(w_j), i,j \leq m$. Pakeitimo funkcija naudojama apsaugoti vandens ženklo paslaptį įtraukiant į dokumentą X. Sumaišyti vandens ženklo elementai yra įtraukiami į dokumentą X vidutinių linijų įterpimo operacija $\oplus$, kaip X‘ įterpimo schemoje (I) yra duota:

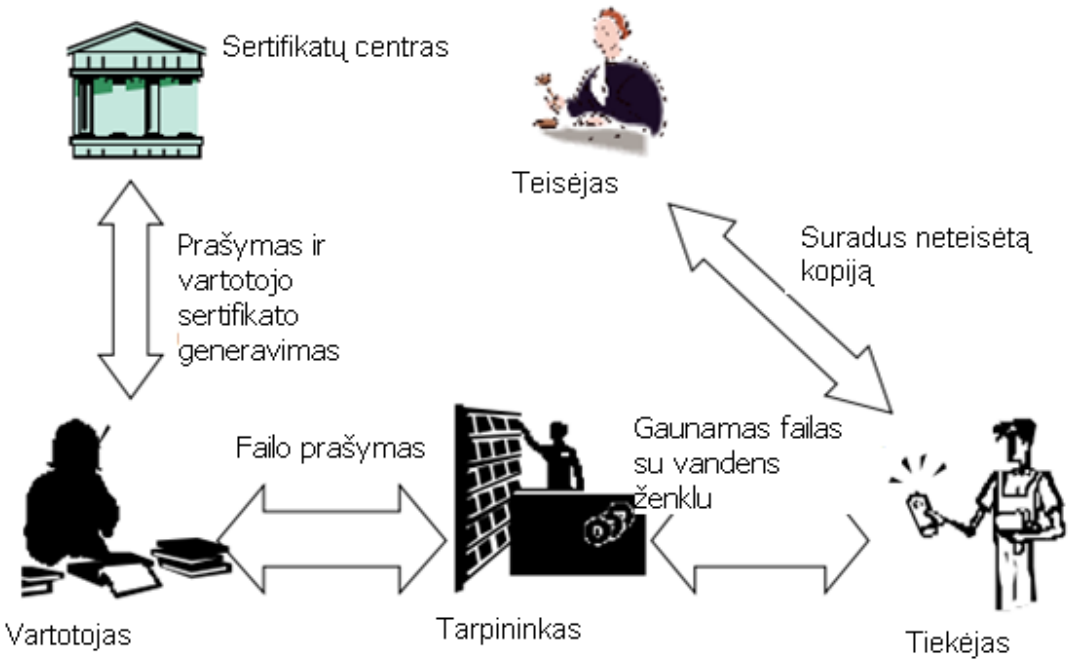
$$X \oplus \sigma(W) = \{x_1 \oplus w_1^{'}, x_2 \oplus w_2^{'}, \dots, x_n \oplus w_n^{'}\}$$

Vandens ženklo įterpimo schema I, vandens ženklo aptikimo schema D, kuri sugražina konfidencialų pranešimą iš egzistuojančio vandens ženklo W dokumento X’ dalyje. Ženklinimo vandens ženklais technologija yra ne aklas ženklinimas. Norint aptikti vandens ženklą schemoje D pareikalaujame žinomo originalaus dokumento X, t.y.

$$\begin{cases} D(X, X^{'}, W, \sigma) = true \quad jei\ W \in X' \\ D(X, X^{'}, W, \sigma) = false \quad jei\ W \notin X' \end{cases}$$

Jei X nepareikalautas originalus dokumentas, D schema vadinama užmirštančiu (oblivious) ženklinimu vandens ženklais. Yra du pagrindiniai scenarijai, kuriame ženklinimo technologijai naudojama teisėta nuosavybė (rightful ownerships). Pirmajame scenarijuje, tiekėjas įtraukia unikalų vandens ženklą į dokumentą. Jei kopija randama vėliau, tiekėjas gali įrodyti nuosavybę nustatydamas unikalų vandens ženklą dokumente. Sekančiame scenarijuje nuo tiekėjo galima įtraukti skirtingus vandens ženklus originaliame dokumente ir identifikuoti kiekvieną vartotoją. Kiekviena kopija gali būti pažymėta ir todėl palikti pėdsaką.

Naudojant antrąjį scenarijų nustatomi penki pagrindiniai vaidmenys informacinio dokumento infrastruktūroje, dokumento naudotojas, tiekėjas, autorinės informacijos kontrolės sertifikatas, teisėjas ir tarpininkas 1.2 pav. Dokumento naudotojas yra vienas, kuris nori įsigyti keletą informacinių dokumentų. Kiekviena informacinio dokumento kopija gali būti atskirai paženklinta vandens ženklu nustatyti naudotoją.



1.2. pav. Intelektualių dokumentų paskirstymo infrastruktūra

1.4. VANDENS ŽENKLŲ KŪRIMUI NAUDOJAMI MATEMATINIAI METODAI

1.4.1. LIEKANŲ TEOREMA (CRT)

Kinų liekanų teorema (The Chinese remainder theorem (CRT)) pirmą kartą suformuota trečiajame amžiuje Kinų matematiko Sun Zi knygoje *Sun Zi Suanjing* arba paprasčiau Sun‘s Arithmetical Manual (Ding, Pei, & Salomaa, 1996, p.2). CRT naudojama kriptologijoje, duomenų apdorojime ir kodavimo teorijoje.

Teorema. Tarkime $n_1, n_2, \dots, n_k$ yra teigiami sveikieji poromis pirminiai skaičiai. Tada, iš kiekvienos duotos sveikųjų skaičių sekos $a_1, a_2, \dots, a_k$ egzistuoja sveikasis skaičius x randamas iš atitinkamos egzistuojančios sistemos

$$\begin{aligned} x &\equiv a_1 (\mathrm{mod}\, n_1) \\ x &\equiv a_2 (\mathrm{mod}\, n_2) \\ &\vdots \\ x &\equiv a_k (\mathrm{mod}\, n_k) \end{aligned} \qquad \textbf{(1.1)}$$

Be to, visi *x* sprendimai iš šios sistemos yra kongruentiniai (sutampantys) modulio $N = n_1 n_2 \dots n_k$ reikšmės.

Taigi $x \equiv y \pmod{n_i},\ \forall\ 1 \le i \le k$, tad ir tik tada, jei $x \equiv y \pmod{N}$.

Kartais vienu metu kongruentūs gali būti apskaičiuojami, net jeigu n_i nėra poromis pirminiai. Sprendinys *x* egzistuoja tada ir tik tada, jei:

$$a_i \equiv a_j \left(\mathrm{mod}\ \gcd\left(n_i, n_j\right)\right), \forall\ i\ ir\ j. \tag{1.2}$$

Visi sprendiniai *x* yra kongruentūs modulio mažiausiams bendrams kartotinis n_i.

Alternatyvūs panašių lygybių sistemų metodai buvo aprašyti Aryabhata (VI a., Kak 1986). Specialus CRT atvejis žinomas kaip Brahmagupta (VII a.), ir pasirodė Fibinacci Liber Abaci (1202).

Modernus teorijos pakartojimas algebrine kalba yra toks iš sveikųjų teigiamų skaičių n su pirminiu suskaidymu $p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$ turime izomorfizmą tarp apskritimų ir tiesioginę sandaugą iš jo pirminių laipsnių dalių:

$$\frac{\mathbb{Z}}{n\mathbb{Z}} \cong \frac{\mathbb{Z}}{p_1^{r_1}\mathbb{Z}} \times \frac{\mathbb{Z}}{p_2^{r_2}\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{p_k^{r_k}\mathbb{Z}} \tag{1.3}$$

Egzistavimas. Egzistavimas gali būti suvokiamas iš detalios x konstrukcijos. Naudosime žymėjimą $[a^{-1}]_b$ nurodyti atvirkštinei $a(mod\ b)$ funkcijai, ji apibrėžiama tiksliai kai a ir b yra tarpusavyje pirminiai.

Dviejų lygčių atvejis.

Duota sistema ($k = 2$)

$$\begin{aligned} x &\equiv a_1 (mod\ n_1) \\ x &\equiv a_2 (mod\ n_2) \end{aligned} \tag{1.4}$$

Apsibrėžiame reikšmę

$$x := a_1 n_2 [n_2^{-1}]_{n_1} + a_2 n_1 [n_1^{-1}]_{n_2} \tag{1.5}$$

Jis atitinka abu kongruentumus. Pavyzdžiui

$$a_1 n_2 [n_2^{-1}]_{n_1} + a_2 n_1 [n_1^{-1}]_{n_2} \equiv a_1 1 + a_2 0 [n_1^{-1}]_{n_2} \equiv a_1 (mod\ n_1) \tag{1.6}$$

Bendru atveju.

Bendru atvejų k kongruenčių lygčių. Tegu $N = n_1 n_2 \cdots n_k$ apibrėžiama visų modulių sandauga.

$$x := \sum_i a_i \frac{N}{n_i} \left[\left(\frac{N}{n_i} \right)^{-1} \right]_{n_i} \quad \textbf{(1.7)}$$

1.4.2. ARITMETINIS PERTEKLINIŲ LIEKANŲ KODAS

Daugelis klaidų taisymo algoritmų naudoja liekanas skaitmeninėje ženklinimo schemoje, kurios pagrindas yra perteklinių liekanų kodas.

Nustatome n poromis tarpusavyje pirminių teigiamų sveikųjų skaičių $m_1, m_2, \dots, m_i, m_{i+1}, \dots, m_n$. Modulis m_i pasirenkamas, kaip didžiausias bendras daliklis

$\gcd(m_i, m_j) = 1, \forall\, i, j, kai\ i \neq j\ ir\ m_1 < m_2 < \cdots < m_i < m_{i+1} < \cdots < m_n$ nuo n modulių sekos, pirmi k yra neperteklinai modeliai,$r = n - k$ perteklinių liekanų modulis. Šių modulių sekos apibrėžimui naudojamos tokios formulės:

$$M_K = \prod_{i=1}^{k} m_i \quad \textbf{(1.8)}$$

$$M = \prod_{i=1}^{n} m_i = M_K \cdot M_R \quad \textbf{(1.9)}$$

$i = 1,2, \dots, k, k+1, \dots, n.$ pastebima, kad M_K mažiausia sandauga iš k skirtingų m_i elementų. Sveikasis skaičius $X \in [0, M)$, kur M apibrėžiamas (1.9) lygybe, gali vienareikšmiškai atspindėti liekanų vektorių $x = \{x_1, x_2, \dots, x_n\}$ naudojant

$$X \equiv x_i (mod\ m_i), \qquad i = 1,2, \dots, k, k+1, \dots, n \quad \textbf{(1.10)}$$

Pagal (1.10) lygtį kiekviena liekana x_i atspindi X modulį m_i taip, kad $0 \leq x_i \leq m_i$. Tačiau, klaidos ištaisymui, X turi būti pasirinktas iš $[0, M_K)$, kur M_K iš (1.8) lygties. Tada liekanų vektorius x gali būti padalintas į dvi dalis, pirmosios k liekanos vadinamos informacinėmis liekanomis, likusios r – perteklinėmis.

Kai liekanų vektorius *x* pateiktas atitinkantis sveikąjį skaičių *X* galima vienareikšmiškai išspręsti visas *n* tiesinių kongruenčių lygčių (1.10). Vienu metu sprendžiamos sekos tiesinių atitikčių problemos supaprastinimui naudojama CRT (1.11).

$$X = \sum_{i=1}^{n} x_i M_i a_i \ mod\ M \tag{1.11}$$

Kur $M_i = \frac{M}{m_i}, a_i = M_i^{-1} mod\ m_i,\ i = \overline{1,n}$, jei $X \in [0, M)$, *k* iš *n* liekanų iš vektoriaus *r*, kur $n > k$ turi būti pakankamas, kad susigražintų originalų skaičių *X*.

Kai $X \in [0, M_K)$, gauname perteklinės liekanos kodas gali būti laikomas tiesiniu. Be to, kodas Ω pagrindinis perteklinių liekanų skaičius sistemoje turi minimizuoti nenulinį Hamming svorį $wt_{min} \geq r + 1$ ir minimalų atstumas $d_{min} \geq r + 1$. Kai Hamming svoris ir atstumas reiškia, kad perteklinių liekanų kodas taiso *t* klaidas, kur:

$$t \leq \left\lfloor \frac{d_{min} - 1}{2} \right\rfloor$$

$\lfloor * \rfloor$ apvalinimas į didesniąją pusę. Kodas su $d_{min} = r + 1$ vadinamas didžiausio atstumo atskyrimu (MDS), jis yra optimalus ir gali koreguoti didžiausią skaičių klaidų t, su mažiausiu skaičiavimų dubliavimu. MDS maksimalios taisomos klaidos:

$$t \leq \left\lfloor \frac{r}{2} \right\rfloor \tag{1.12}$$

Dėl daugelio klaidų taisymo, sistema pirmiausia apsvarsto perteklinių liekanų kodą nustatydama modulį m_i. Sveikasis skaičius *X* yra pasirinkamas iš intervalo $[0,M_K)$ ir liekanų vektorius yra $x=\{x_1,x_2,\ldots, x_n\}$. Tegul intervalą $[0,M_K)$ galima pavadinti teisėtu diapazone, o jo kopija, iš intervalo $[M_k, M)$, gali būti apibūdinta kaip neteisėtą intervalasą. Tarkime, kad *t* klaidos buvo įtrauktos į vektorių *x*, kai jis eina per potencialiai triukšmingą sistemą. Gautas vektorius *y*:

$$y = x + e$$

$$\{y_1, K, y_n\} = \{x_1, K, x_n\} + \{e_{u_1}, K, 0, e_{u_2}, K, e_{u_t}\}, 0 \leq e_{u_j} \leq m_{u_j}, 1 \leq j \leq t.$$

Klaidų reikšmės $e_{u_1}, e_{u_2}, \ldots, e_{u_j}, e_{u_{j+1}}, \ldots, e_{u_t}$, patiniai indeksai $u_1, u_2, \ldots, u_j, u_{j+1}, \ldots, u_t$, yra klaidų y pozicijos. Gavus vektorių *y*, klaidų aptikimo pradžioje atliekamas nustatymas, ar *y* yra svarbus vektorius. Tai galima atlikti apskaičiuojant Y, kuri yra pagrįstą lygtimi (1.11):

$$Y = \sum_{i=1}^{n} y_i M_i \, a_i \mathrm{mod} M \, , i = \overline{1,n} \quad \textbf{(1.13)}$$

Jeigu išieškotos *Y* per teisėtą diapazoną, tada *y* yra svarbus vektorius ir jokių tolimesnių žingsnių neatliekame. Kita vertus, jei *Y* yra neteisėto diapazono, tada galima daryti išvadą, kad *y* yra klaidingų liekanų. Daugelio klaidų korekcijos schema gali būti apibendrinta kaip teorema.

Teorema. Dėl perteklinių liekanų skaičiaus sistemos kodas atsižvelgdamas tinkamo dydžio pertekliaus r, tokio, kad $t \geq \left[\frac{r}{2}\right]$ klaidos įvyko gavo vektorių *y*, originalų sveikąjį skaičių *X* galima rasti atliekant šią operacija:

$$YX = Y \mathrm{mod}\ \mathrm{Z_c} \quad \textbf{(1.14)}$$

Kur $Z_c = \frac{M}{\prod_{\alpha=u_1}^{u_t} m_\alpha}$ ir $u_1, u_2, \dots, u_j, u_{j+1}, \dots, u_t$ yra *t* klaidos pozicija *y*. Apatinis *c* indeksas $p = {}^{n}C_t$ galimos kombinacijos iš u_j.

Kadangi nėra nustatyta, kaip a priori klaidų pozicija, visi galimi deriniai turi būti atsižvelgiami į Z_c skaičiavimą. Tokia, lygtis (1.14) turės būti pakartota bent *p* kartų, kad būtų ištaisytos klaidos.

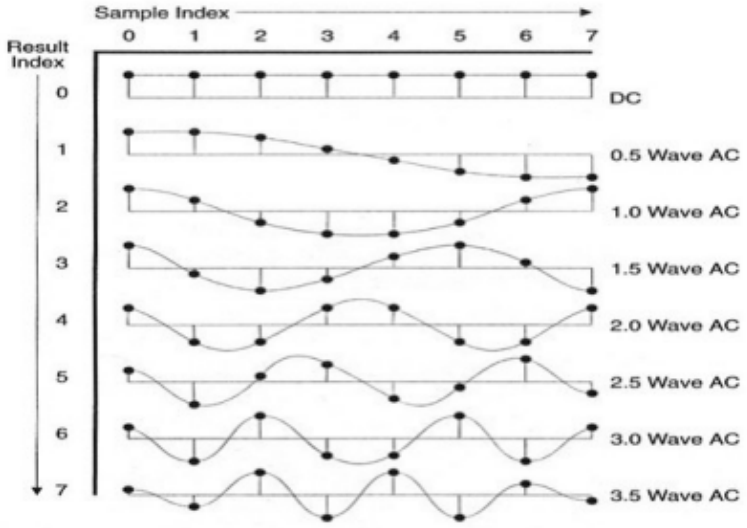
1.4.3. DISKREČIOJI KOSINUSO TRANSFORMACIJA (DCT)

Diskrečioji kosinusų transformacija (angl. – discrete cosine transform(DCT)) yra matematinė operacija, kuri transformuoja duomenis, gautus diskretizuojant tam tikru dažniu, į jų dažnio komponentes. Vienas iš jos privalumų yra tas, kad koeficientai labiau koncentruoti ties žemesniais indeksais. Dėl to signalą galima aproksimuoti panaudojant mažiau koeficientų.

Formaliai DCT yra tiesinė, atvirkštinė funkcija $F: \boldsymbol{R}^N \rightarrow \boldsymbol{R}^N$ (kur **R** realiųjų skaičių aibė), arba ekvivalenti atvirkštiniai $N \times N$ kvadratiniai matricai. N realieji skaičiai $x_0, \dots, x_{N-1}$yra transformuojami į N realųjį skaičių $X_0, \dots, X_{N-1}$ priklausomai nuo formulių.

Vienos demencijos DCT konvertuoja skaičių masyvą, kuris atitinka skirtingais laiko momentais užfiksuotas signalo amplitudes, į kitą skaičių masyvą, iš kurių kiekvienas atitinka konkrečią pradinio masyvo dažnio dedamųjų amplitudę. Gautas masyvas turi tiek pat reikšmių, kiek ir pradinis masyvas. Pirmoji gautojo masyvo reikšmė yra visų pradinio masyvo reikšmių aritmetinis vidurkis ir yra nuolatinės dedamosios atitikmuo. Kiekvienas iš likusių elementų atitinka pradinio masyvo dažnio dedamųjų

amplitudes. Dažnio dedamosios randamos apskaičiuojant viso masyvo reikšmių su svorio koeficientais vidurkį. Svorio koeficientai yra tarsi kosinusinė banga, kurios dažnis yra proporcingas masyvo indeksui.

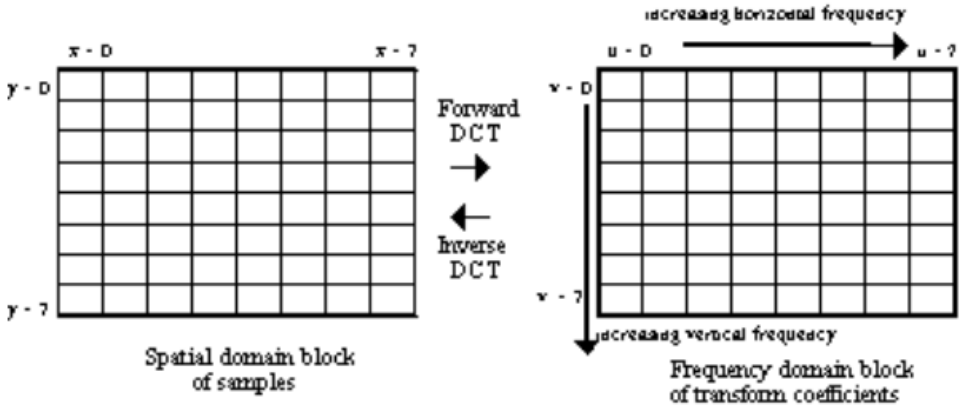


1.3. pav. Kosinusų transformacija

Vienos demencijos DCT skaičiuojamas pagal tokią formulę:

$$f_j = \frac{1}{2}\left(x_0 + (-1)^j x_{n-1}\right) + \sum_{k=1}^{n-2} x_k \cos\left[\frac{\pi}{n-1} jk\right] \qquad \textbf{(1.15)}$$

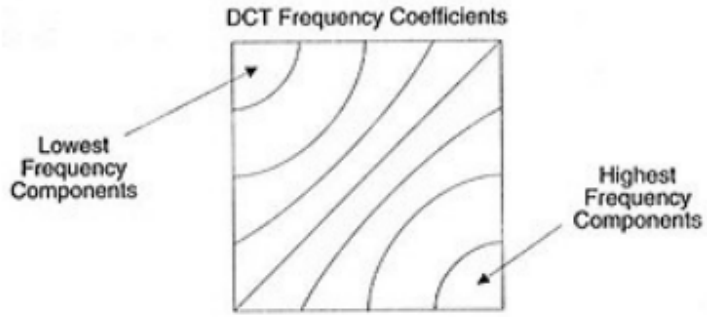
Dviejų dimensijų DCT keičia dviejų dimensijų erdvės sritį į dviejų demencijų DCT sritį.



1.4. pav. 2D laiko srities masyvo keitimas 2D DCT sritimi

Dviejų dimensijų DCT naudoja fundamentalius vienos dimensijos DCT veiksmus. Galima įsivaizduoti, kad 8×8 taškų masyvas yra aštuonios eilutės po aštuonis taškus. Taigi, vienos dimensijos DCT pritaikoma atskirai kiekvienai eilutei po aštuonis taškus. Atsakymas – aštuonios eilutės dažnio

koeficientų. Dabar imami aštuoni koeficientų stulpeliai. Visi pirmo stulpelio koeficientai atitiks nuolatines dedamąsias, antrame stulpelyje bus pirmi kintamos dedamosios elementai ir t.t. Nors horizontalia kryptimi koeficientai atitinka dažnio dedamąsias, vertikaliai vis dar išreiškiama erdvinė informacija, todėl vienos demencijos DCT turi būti prataikoma dar kartą kiekvienam stulpeliui. Dažnių pasiskirstymas pavaizduotas paveiksle.



1.5. pav. Dažnių pasiskirstymas DCT srityje

Galiausia kiekvienas masyvo elementas reikš dvimatį dažnio komponentą. Kairiajame viršutiniame kampe esantis komponentas yra viso dvimačio masyvo nuolatinės dedamosios elementas, o visi likę koeficientai parodo dažninę informaciją.

Dviejų dimensijų DCT koeficientai randami pagal tokią formulę:

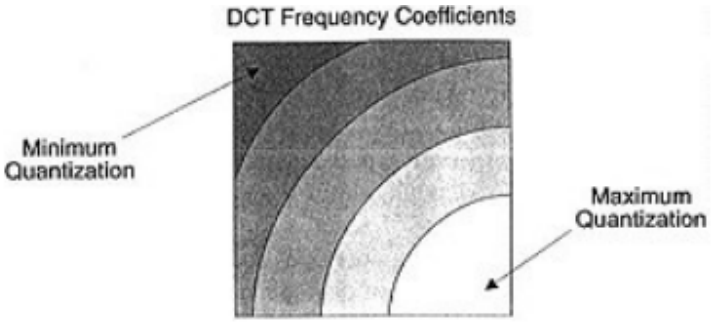
$$f_j = \sum_{k=0}^{n-ą} x_k \cos\left[\frac{\pi}{n} j \left(k + \frac{1}{2}\right)\right] \quad \textbf{(1.16)}$$

DCT naudojamas JPEG vaizdų, MJPEG, MPEG, DV ir Theora video failų suspaudimui. Tai dviejų demencijų DCT blokų skaičiavimas ir rezultatas yra kvantas ir entropijos kodas (coded). Šiuo atveju, N dažniausia yra 8 ir dviejų demencijų DCT formulė taikoma kiekvienoje eilutėje ir stulpelyje blokais. Rezultatas yra 8×8 transformuotų koeficientų masyvas, kuriame (0,0) elementas (iš viršaus kairėje) yra DCT (nulinio dažnio) sudedamųjų dalių ir įrašų su vertikaliu ir horizontaliu indeksu reikšmės užimančios didesnius vertikalius ir horizontalius erdvės dažnius.

Kvantavimas

Po pradinio 8 x 8 taškų bloko transformavimo į 8 x 8 DCT koeficientus pritaikomas kvantavimas. Žemesnio dažnio sritis reikalauja mažiau kvantavimo resursų, o aukštesnio – daugiau. Kvantuojant DCT

koeficientų tikslumas sumažėja, todėl kvantavimo laipsnis ir forma yra pritaikoma skirtingiem vaizdų tipams (vidiniams arba ne vidiniams), kad būtų išvengta matomų rekonstruoto vaizdo iškraipymų



1.6. pav. DCT sritys pagal kvantavimo sudėtingumą

MPEG algoritmas leidžia naudoti skirtingų svorių matricas vidiniams ir ne vidiniams vaizdams, kad atitiktų kiekvieno vaizdo dažnines charakteristikas.

1.5. VANDENS ŽENKLO GENERAVIMO ALGORITMAS DCT METODU

Naudojamas prototipas naudoja praplėsto spektro (Spread-Spectrum) ženklinimo vandens ženklais schemą. [11]. Kita tiesinė ženklinimo schema gali būti naudojama protokole taip ilgai kol vandensženklis įterpiamas į šifruotą sritį, kur skaitmeninis dokumentas yra užšifruotas viešuoju raktu. Vandens ženklas susideda iš 1000 nepriklausomų realiųjų skaičių sekos $W = \{w_1, w_2, \dots, w_{1000}\}$. Pasirenkama reikšmės iš 1000 yra sutartinė; galima naudoti mažiausią skaičių vandens ženklo generavimui. Kiekvienas iš šių skaičių yra iš Gauso skirstinio ($m = 0, \sigma = 1$).

Vandens ženklas įterpiamas į didžiausią iš 1000 diskrečiojo kosinuso transformacijos (DCT) koeficientą iš skaitmeninio dokumento. Pavyzdžiui, jei skaitmeninis dokumentas X su didžiausiu 1000 DCT $\{x_1, x_2, \dots, x_{1000}\}$ įterpiamas su vandens ženklu $W = \{w_1, w_2, \dots, w_{1000}\}$, tada didžiausias 1000 DCT koeficientai iš paženklinto dokumento X‘ yra $\{x'_1, x'_2, \dots, x'_{1000}\}$, kur

$$x'_i = x_i(1 + \alpha w_i), \qquad 0 \le i \le 1000 \tag{1.17}$$

α yra mažiausia konstanta (0,1). Po įterpimo naudojamas atvirkštinis DCT operatorius išgauti vandens ženklą dokumente X‘. Taip užbaigiamas vandens ženklo įterpimo procesas. Siekiant aptikti vandens ženklą skaitmeniniame dokumente Y, pirmiausia naudojama DCT aptikti 1000 didžiausių DCT koeficientų $Y = \{y_1, y_2, \dots, y_{1000}\}$. Tada atimamas kiekvienas koeficientas x_i stebima seka T= $\{t_1, t_2, \dots, t_{1000}\}$, kur

$$t_i = \frac{y_i - x_i}{\alpha x_i} \quad \textbf{(1.18)}$$

Jei $W = \{w_1, w_2, \dots, w_{1000}\}$ iš tiesų yra Y, tada turi būti aukšta koreliacija tarp T ir W. Koreliacija apskaičiuojama taip:

$$Corr(T, Y) = \frac{T \cdot Y}{\sqrt{T \cdot T * W \cdot W}} \quad \textbf{(1.19)}$$

Kur $\cdot$ sandaugos operatorius,$*$ realiųjų skaičių daugybos operatorius.

Sekantis, pateikiamas taikymas RSA kriptosistemos šifravimui protokole. Šifravimo procese, iš charakteristikos x ir viešojo rakto a, šifruotas dydis y apskaičiuojamas taip:

$$y = E_a(x) = x^a \bmod n \quad \textbf{(1.20)}$$

Kur n yra sandauga dviejų didelių pirminių skaičių p ir q. Iššifravimo procese naudojamas privatus raktas b ir skaičiuojama:

$$x = D_b(y) = y^b \bmod n \quad \textbf{(1.21)}$$

Jei turimas $W = \{(1+\propto w_1), (1 + \alpha w_2), \dots, (1 + w_{1000})\}$, tada procesas $X \oplus W$ gali būti laikomas vandens ženklo įterpimo operatoriumi, nes:

$$X \oplus W = \{x_1(1 + \alpha w_1), x_2(1 + \alpha w_2), \dots, x_m(1 + \alpha w_{1000})\} \quad \textbf{(1.22)}$$

Naudojant RSA kriptosistemos savybes $\big(E(x) \oplus E(y)\big) = E(x \oplus y)$ vandens ženklas gali būti įterptas į šifruotą sritį. Pavyzdžiui, pasiūlytame protokole turime X' kaip X su vandens ženklas W šifruotame dokumente.

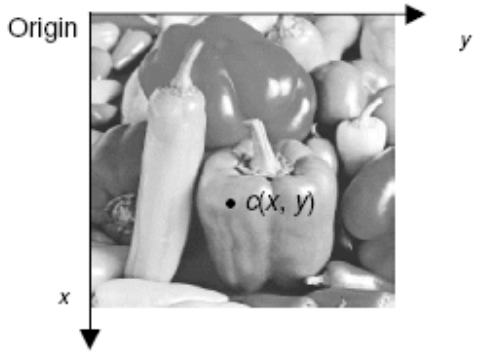
1.6. VANDENS ŽENKLO ĮTERPIMO SCHEMA

Tegul C yra nespalvotas $P_1 \times P_2$ dydžio vaizdas, kuris bus paženklintas. Be to, W vandens ženklo seka, kurio ilgis N, yra įterpiamas į C. Nespalvotus vaizdus aprašomas taip:

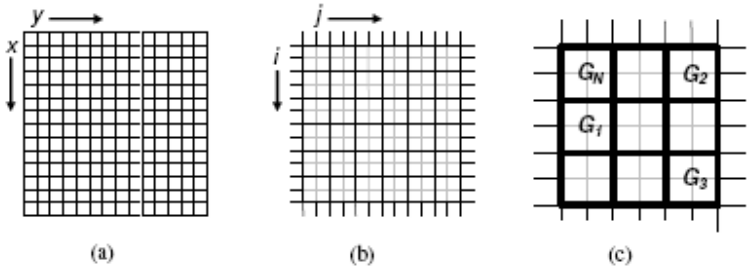
$$C = \{c(x, y) | x = 1,2, K, P_1, y = 1,2, K, P_2\} ir\ c(x, y) \in \{0,1, K, 255\}$$

Kur c(x,y) yra pikselių intensyvumas erdvės koordinatėse *x* ir *y*. 1.7. paveikslėlyje pavaizduota, kaip erdvės koordinatės yra nustatomos duotame vaizde. Vandens ženklo seka yra vienintelė binari seka:

$$W = \{w_h | x = 1,2,K,N\}, w_h \in \{0,1\}$$



1.7. pav. Bendrosios ašies paprastumas naudojant skaitmeninį vaizdą



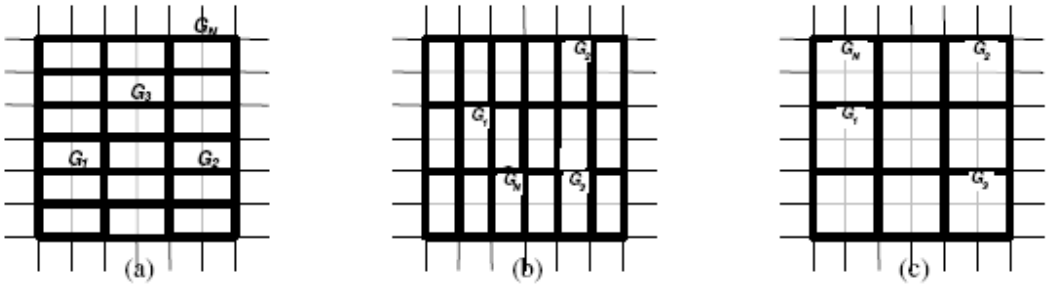
1.8. pav. Skirtingų lygių vaizdo suskirstymas; a) vaizdo taškų; b) po blokų formavimo; c) po formavimo

Tai reiškia, kad vandens ženklo seka W yra binari bitų seka reprezentuojanti ID ar paprasta vizualiai prasmingas vaizdas kaip logotipas, kuris nustato unikalumą, kopijos savininką.

Blokų vandens ženklų schemoje, vaizdas pirma padalinamas į mažesnius neužeinančius vienas ant kito blokelius, kurių dydis $O_1 \times O_2$, kaip parodyta 1.8 b) paveikslėlyje. Tegul šie blokai žymimi $b(i,j)$ kur i ir j erdvės koordinatės, nurodančios blokelių vietą. Tai gali būti vertinama, kaip $0 \le i < P_1/O_1$, $0 \le j < P_2/O_2$.

Vaizdas iš esmės yra taškų rinkinys, kurių kiekvienas turi savo intensyvumo lygį. Šie pikseliai yra sugrupuoti fiksavimo metodu, lyginant su kiekvienu kitu, formuojant didesnius vaizdus. Priešingai, izoliuotas taškas perteikia mažiau regimą informaciją. Todėl vizualiai turtingas paveikslėlis taškais, kurie yra labai priklausomi nuo kaimyninių taškų perteikiamo vaizdo turinio. Šie taškai susiję tam tikru būdu,

kad negalėtų būti daug įvairių žeminančio vaizdo kokybę nepriimtinų būdų. Tai yra būtent tokia nuosavybė, kuri yra naudojama kaip priemonė įtvirtinti vandens ženklą.



1.9. pav. Diagrama parodo keletą galimų gretimų blokų grupavimų palyginimų: a) kairė ir dešinė; b) viršuje ir apačioje; c) stačiakampio

Taip, vietoj kiekvieno pikselio su kitu koreliacijos matavimo, imama koreliacija tarp grupės pikselių su kita grupe. Kiekvienai pikselių grupei atstovauja jų vidurkis, nes nedideli daliniai vaizdo pakeitimai, pvz. pridedant atsitiktinio triukšmo, nesukelia reikšmingų pokyčių, vidutiniam taškų intensyvume. Jei atliekama daugiau pakitimų, galima daryti prielaidą, kad gretimos grupės taškai, taip pat paveikti, panašiu būdu. Rezultate, bendri santykiai tarp grupių yra išlaikomi ir pakitimai minimalūs.

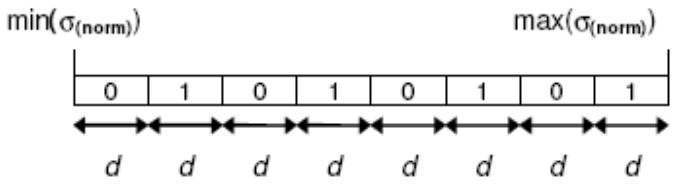
Tegu taškų grupė $O_1 \times O_2$ blokas padalintas. Vidutinė kiekvieno bloko $b(i,j)$ vertė žymima $\mu_{b(i,j)}$. Apskaičiuojamas taip:

$$\mu_{b(i,j)} = \frac{\sum_{(x,y)\in b(i,j)} c(x,y)}{O_1 \times O_2} \quad \textbf{(1.23)}$$

Kur x ir y – taškų erdvės koordinatės, taip sudaro kvadratėlį $b(i,j)$. Be to, tarp blokų koreliacija gali būti apskaičiuota naudojant bet kurią funkciją, kuri suteikia informacijos, kaip jie yra susiję vieni su kitu. Šioje vandens ženklų sistemoje funkcija, naudojama apskaičiuoti šių blokų koreliacijai yra standartinis nuokrypis.

Siekdami gauti koreliaciją, naudojame gretimus blokus. Visi $O_1 \times O_2$ blokai yra sugrupuoti kaip paveiksle 1.8 (c). Grupės iš tikrųjų gali būti bet kokių formų ir dydžių, keletas pavyzdžių parodyta 1.9. pav. Nepriklausomai nuo to, kaip šie blokai yra sugrupuoti, reikia pažymėti, kad vienos grupė q blokai bus naudojami įterpti vieną vandens ženklo bitą. Todėl iš N grupės pseudoatsitiktinai atrenkamas iš skirtingų dalių vaizdas naudojant įterpimo raktą m. Tai užtikrina, kad vandens ženklas yra pasklidę po visą vaizdą, mažintantis regimo vaizdo iškraipymą, atsiradus vandens ženklui sistemoje. Tegul pseudoatsitiktinai parinktos grupės $\Gamma = \{\Gamma_1, \Gamma_2, \dots, \Gamma_h, \Gamma_{h+1}, \dots, \Gamma_N\}$. Tai galima matyti 1.9. pav.

Jei nesusiekiantys blokai grupuojami kartu, tarp šių blokų atitikimas sunkiau išlaikomas. Taip yra dėl to, kad skirtingo dydžio pakeitimas gali būti taikomi skirtingoms vaizdo dalims, bei žeminančios vaizdo kokybę.



1.10. pav. Skaidymo ašis naudojama vandensženklio įterpimo procese

Deja, pasikeičia nesusiekiančių blokų tarpusavio ryšys pašalinimo procese. Kita vertus, pakeitimai paprastai yra gana vienodi, leidžiantys tiksliau išieškoti vandens ženklo.

Bloko dydis $O_1 \times O_2$ taip pat ir gretimų blokų skaičiaus q nustatymai turi būti atidžiai parenkami tokie, kad:

$$N \leq \frac{1}{\propto q}\left(\frac{P_1}{O_1} \cdot \frac{P_2}{O_2}\right), \alpha \geq 1. \tag{1.24}$$

Tai užtikrina, kad yra pakankamai erdvės palaikykite vandens ženklą paveikslėlyje. Parametras naudojamas įsitikinti, kad ne visi vaizdo taškai yra pakeisti, įtvirtinus vandenženklį. Tokiu būdu pašalinama galimybė sumažinti ir iškraipyti vandens ženklą iki minimumo.

Vidutinio intensyvumo grupėje Γ_h standartinis nuokrypis apibrėžiamas taip σ_h:

$$\sigma_h = \left\{\frac{1}{q}\sum_{b(i,j)\in G_h}\left[A_h - \mu_{b(i,j)}\right]^2\right\}^{\frac{1}{2}} \tag{1.25}$$

$$A_h = \frac{1}{q}\sum_{b(i,j)\in G_h}\mu_{b(i,j)} \tag{1.26}$$

Tegu $\sigma = \{\sigma_1, \sigma_2, \ldots, \sigma_h, \sigma_{h+1}, \ldots, \sigma_N\}$ ir normalizuotas $\sigma_{(norm)} = \{\sigma_{1(norm)}, \sigma_{2(norm)}, \ldots, \sigma_{h(norm)}, \sigma_{h+1(norm)}, \ldots, \sigma_{N(norm)}\}$, kur vidurkis nulis, o standartinis nuokrypis 1. Standartinį nuokrypį σ_h $h = 1,2,\ldots,N$ reikia pakeisti, įterpiant vandens ženklo bitus. Apibrėžti apimčių kitimą, ašyse naudojamas $\max(\sigma_{(norm)})$ (1.7. pav).

Ašis yra nustatoma pagal mažiausią ir didžiausią $\sigma_{(norm)}$. Taip pat suskirsto į ε nesusikertančių dalių vienodų dydžių, kiekvienas intervalas turi svorius

$$d = \frac{\max\left(\sigma_{(norm)}\right) - \min(\sigma_{(norm)})}{\varepsilon} \quad \textbf{(1.27)}$$

Kintanti seka nuliukų ir vienetukų atstovauja binarius skaitmeninis priskiriama kiekvienai daliai. Vandens ženklo bitas *kth* įterpiamas pridedant nedidelį nuokrypį $\Delta s_{k(norm)}$į $\sigma_{k(norm)}$. Jei $\sigma_{k(norm)}$ patenka į dalį, tada yra dvejetainis skaitmuo, kuris atitinka *kth* vandens ženklo bitus, tik mažas nukrypimas, kad $\sigma_{k(norm)}$ juda į bloko centrą yra reikalinga. Kita vertus, jei bloko vandens ženklo bitai neatitinka *htk* vandens ženklo bitų, iš $\Delta\sigma_{k(norm)}$reikia judėti į $\sigma_{k(norm)}$ artimiausios dalies centrą.

Persikėlimas $\sigma_{k(norm)}$ į ląstelės centrą užtikrina, kad didžiausia vandens ženklo tvirtumas yra pasiektas. Taip yra todėl, kad atstumas iki kito elemento, bet kuria kryptimi yra toliausiai į centrą. Jame bus atsižvelgiama į $d\ /\ 2$ iškraipymo vandens ženklo bitus, todėl klaida gavybos vandens ženklas (Wong et al., 2003). Kaip tokia, didesnių vertę d geriau į siekiant išlaikyti vandens ženklo tvirtumą. Deja, didelis d gali sukelti matomus artefaktus.

Kai nuokrypis $\Delta\sigma_h, h = 1,2,\ldots,N$ buvo nustatytas, senas standartinis nuokrypis σ_h turi būti pakeista į s_h^*. Laikykimes (1.30) lygties, kad s_h yra priklausomas nuo $\mu_{b\,(i,j)}$. Todėl siekiant gauti σ_h^*, vidutinės vertės $\mu_{b\,(i,j)}, b\,(i,j) \in G_h$ turi būti pakeista. Leisti $\Delta\mu_{b\,(i,j)}$ yra vertė, kuri turi būti įtraukta į $\mu_{b\,(i,j)}$, suteikiant naują vidurkį $\mu^*_{b\,(i,j)}$.Matematiškai:

$$\mu^*_{b\,(i,j)} = \mu_{b\,(i,j)} + \Delta\mu_{b\,(i,j)},\ \ b\,(i,j) \in G_h, h = 1,2,\ldots,N \quad \textbf{(1.28)}$$

$\mu^*_{b\,(i,j)}$ryšys tarp $\Delta\sigma_h$ ir σ_h pateikiamas taip:

$$|(\sigma_h^*)^2 = \sigma_h^2 + \Delta\sigma_h \quad \textbf{(1.29)}$$

$$\Delta\sigma_h\ = \frac{1}{q}\sum_{b(i,j)\in G_h}\left[2\left(A_h - \mu_{b\,(i,j)}\right)\left(\delta - \Delta\mu_{b\,(i,j)}\right) + \left(\delta - \Delta\mu_{b\,(i,j)}\right)^2\right] \quad \textbf{(1.30)}$$

Kur vidutinė $\Delta\mu_{b\,(i,j)}, b(i,j) \in G_h$ reikšmė :

$$\delta = \frac{1}{q}\sum_{b(i,j)\in G_h}\Delta\mu_{b\,(i,j)} \quad \textbf{(1.31)}$$

(1.31) lygties parametras $\Delta\mu_{b\,(i,j)}, b(i,j) \in G_h$ reikalingas kintamųjų stebėjimas, kad gautume artimesnį pageidaujamo nuokrypio įvertinimą $|\Delta\sigma_h$. $\Delta\mu_{b\,(i,j)}$ reikšmių deapazonas sukelia naują reiškmiųū intensyvumą turį negaliojančių pustonių:

$$\left(0 - \mu_{b\,(i,j)}\right) \leq \Delta\mu_{b\,(i,j)} \leq \left(255 - \mu_{b\,(i,j)}\right) \quad \textbf{(1.32)}$$

Nors ekstremalios reikšmės $\Delta\mu_{b\,(i,j)}$gali būti naudojama siekiant gauti geriau įvertintą norimą nuokrypį $\Delta\sigma_h$, vaizdo iškraipymai tampa matomi. Kaip tokia, $\Delta\mu_{b\,(i,j)}$ yra tik įvairių $[-t, t]$. t – paprastai vienas skaitmuo sveikasis skaičius. Norėdami surasti tinkamiausią vertę $\Delta\mu_{b\,(i,j)}$, $b(i,j) \in G_h$ imamas visų įmanomų derinių iš $\Delta\mu_{b\,(i,j)}$ patikrinimas. Kiekvieną skirtingų derinių rinkinį, atsižvelgiant į q reikšmes išbandoma pakeičiant ją į (1.30) lygtį. Apskaičiuoti rezultatai palyginami su norimu nuokrypiu $\Delta\sigma_h$ kartu yra mažiausių klaidų naudojimas. Nustačius geriausią derinį $\Delta\mu_{b\,(i,j)}$, vidutinis intensyvumas kiekvieno bloko grupės $\Gamma_h, h = 1, 2, \ldots, N$, turi būti pakeisti. Paprasčiausias būdas įvykdyti tai, vienodai pridedant sumą $\Delta\mu_{b\,(i,j)}$ prie kiekvieno pikselių intensyvumo $bloke\ b\ (i,j) \in \mathrm{G}_h$.

$$c^*(x,y) = c(x,y) + \Delta\mu_{b\,(i,j)} \quad \textbf{(1.33)}$$

Kur $c^*(x,y)$ vandens ženklo pikselis $(x,y) \in b(i,j)$. Įterpimo proceso rezultatas yra paženklintas vaizdas C^*.

1.7. **VANDENS ŽENKLO IŠTRAUKIMO SCHEMA**

Kadangi paženklinto vandens ženklu vaizdo C* vientisumas negali būti nustatytas prieš gaunant vandens ženklą C`. Potencialiai sugadinto paženklinto vandens ženklu vaizdas aprašomas taip:

$$C' = \{c'(x,y) | 0 \leq x \leq P_1, 0 \leq y \leq P_2\}\ ir\ c'(x,y) = \{0,1,K,255\} \quad \textbf{(1.34)}$$

Kopijavimo informacija, vis dar gali būti randama iš C‘ su raktu y. Surasti vandens ženklą naudojami tie patys algoritmai, kaip sukuriant. Pirmiausia, vaizdas C‘ padalinamas į mažesnius nesusikertančius $O_1 \times O_2$ blokus. Tada sugrupuojami į nesusikertančias grupes. Tada, su raktu y, grupės su įterptais vandensženklio bitais yra atrenkamos iš sekos $\Gamma = \{\Gamma_1, \Gamma_2, \ldots, \Gamma_h, \Gamma_{h+1}, \ldots, \Gamma_N\}$. Visas procesas matomas 1,8pav.

Tęsiant ištraukimo algoritmą, iš standartinio nuokrypio sekos $\sigma = \{\sigma_1, \sigma_2, \ldots, \sigma_h, \sigma_{h+1}, \ldots, \sigma_N\}$ ir normalizuotos $\sigma_{(norm)}$. Ašys panašios 1.10. pav. yra generuojamos ir naudojamos išgauti vandens ženklo

bitus. Vandens ženklo ištraukimas yra atliekamas priešingomis taisyklėmis, nei naudojama įterpime. Jei $\sigma_{h(norm)}$ klaidingas celeje, bitas atstovauja langelį hth vandens ženklo bitas. Tas pats procesas kartojamas kol visi vandens ženklo bitai w_h yra ištraukiami $h = 1,2, \dots, N$. Su vandens ženklo bitu w_h' išgaunama seka W'.

2. TIRIAMOJI DALIS

2.1. PERTEKLINIŲ LIEKANŲ KODO SKAIČIAVIMAS

Pademonstruosime keletą klaidų ištaisymo algoritmo galimybių, naudojant perteklinių liekanų kodą.

Tarsime, kad $(n = 6, k = 2)$ kodas naudoja $m_i \in \{11, 13, 17, 19, 23, 29\}$. Pagal (1.12) lygtį šis kodas taisomas iki $t = 2$ klaidos. Leistinas intervalas [0, 143], neleistinas [143, 30808063]. Tegu $X = 73$ ir ekvivalentus liekanų vektoriui $x = \{7,8,5,16,4,15\}$. Tarkime, kad dvi klaidos $(t = 2)$ atsikleidžia x perdavimo metu $u_1 = 3, u_2 = 6$. Todėl, išsaugotas vektorius $y = \{7,8,11,16,4,2\}$. Nuo y, skaičiuojant sveikąjį skaičių Y naudojama (1.13) lygtis:

$$Y = \sum_{i=1}^{6} y_i M_i a_i \bmod M = 25121455$$

Atitinkamai M_i ir atvirkštinės daugyba a_i yra:

$$M_i = \{2800733, 2369851, 1812239, 1621477, 1062347\}$$

$$a_i = \{1,9,7,9,10,26\}$$

Kadangi, apskaičiuotos vertės Y yra neteisėtame intervale galima daryti išvadą, kad yra klaidų. Taigi, algoritmas ir toliau atliekamas pagal (1.14) lygtį keletą kartų. Visi Z_c deriniai – apskaičiuojami. Rezultatai yra pateikti 2.1 lentelėje.

Vienintelis teisingas rezultatas iš 2.1 lentelės, kur leistinas intervalas [0, 143) yra $X = 73$. Su šiuo rezultatu, klaidų pozicija yra nustatoma $u_1 = 3, u_2 = 6$. Algoritmas teisingai nustatė pradinį sveikąjį skaičių.

2.1. lentelė

Daugelio klaidų taisymo algoritmo, kai iteracijų skaičius p=15 rezultatas

c	Y	Klaidos pozicija		Z_c	$X = Y \bmod Z_c$
		u_1	u_2		
1	25121455	1	2	215441	130299
2	25121455	1	3	164749	79607
3	25121455	1	4	147407	62265
4	25121455	1	5	121771	36629
5	25121455	1	6	96577	11435
6	25121455	2	3	139403	28915
7	25121455	2	4	124729	50926
8	25121455	2	5	103037	83464
9	25121455	2	6	81719	33722
10	25121455	3	4	95381	36281
11	25121455	3	5	78793	65281
12	25121455	3	6	62491	73
13	25121455	4	5	70499	23811
14	25121455	4	6	55913	16518
15	25121455	5	6	46189	40828

2.2. ŽENKLINIMAS DCT METODU

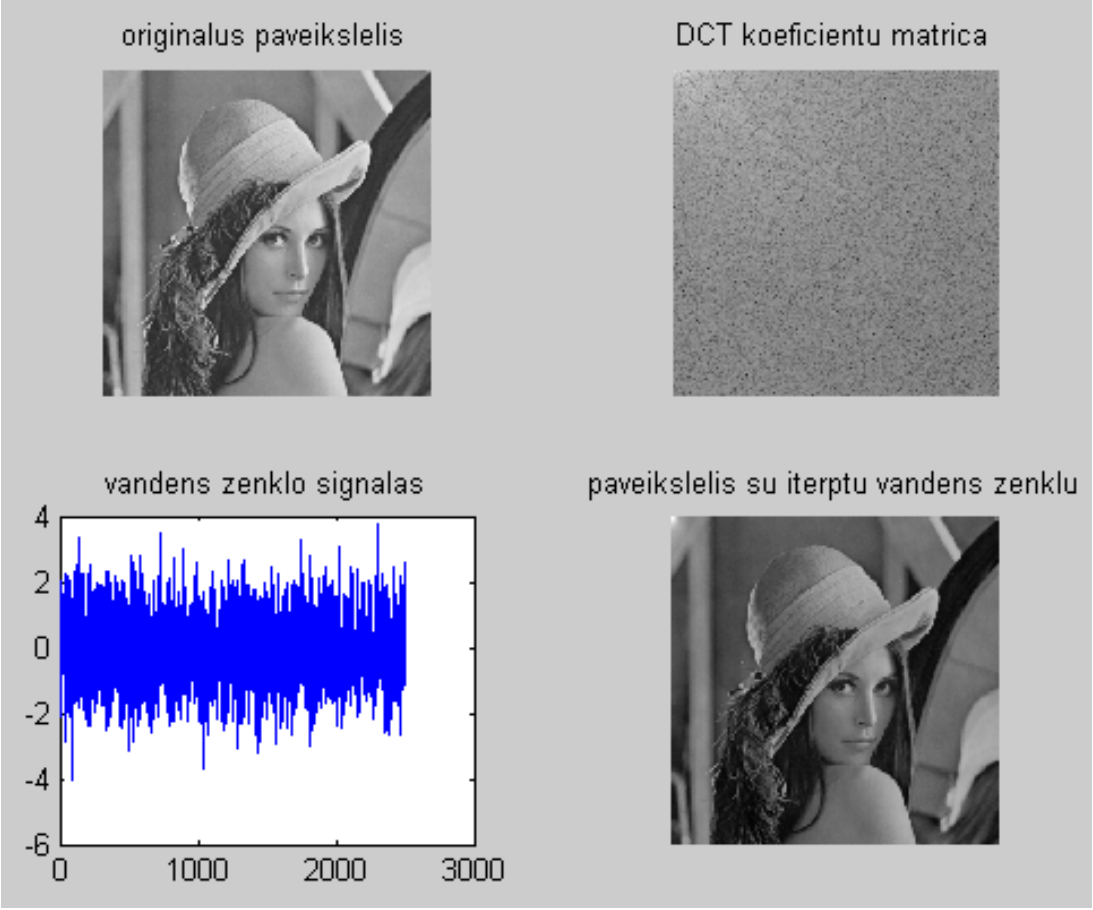
DCT pagrindu sukurtas ženklinimo algoritmas: atsitiktinė seka, kaip vandens ženklo signalas įterpiamas į DCT svarbias vaizdo komponenčių amplitudes (n koeficientai didesnės amplitudės, kaip svarbi komponentė). Nustačius panašias funkcijas kaip ir bandant išgauti vandens ženklą pastebime, kad algoritmas yra nematomas dėl įprastinio vaizdo apdorojimo, kaip filtravimas, suspaudimas, kirpimas ir t.t.

Bendrasis vandens ženklo įterpimo procesas:

1) DCT metodu transformuojamas originalus vaizdas.

2) Vandens ženklo generavimas. Vandens ženklo signalas W naudojamas kaip normaliojo skirstinio N (0,1), n atsitiktinė realiųjų skaičių seka (Gauso atsitiktinė seka). Būtent:. $W = \{X_i, 0 =< i <= n\}$

3) Vandens ženklo įterpimas. Pasirinktas vandens ženklo signalas veikia svarbiausias komponentės vizualiai, nes vaizdas svarbiausia komponentė. Vaizdo signaluose sutelkta daugiausia energijos. Tam tikri iškraipyti vaizdai gali išlaikyti pagrindinius komponentus. Būtent vaizde svarbiausias antitrukdžių pajėgumas. Vandens ženklo įterpimas į šiuos komponentus, leidžia gauti geresnį saugumą. Kai vandens ženklo signalas yra mažas palyginus su priimančiojo signalu galima garantuoti nematomumą. Tačiau, šis algoritmas bus taikomas N(0,1) atsitiktinėms sekoms. Dažniausia pasirenkami didelės amplitudės koeficientai, kaip svarbios komponentės. Įterpimo formulė $v' = v(1 + aX_k)$.

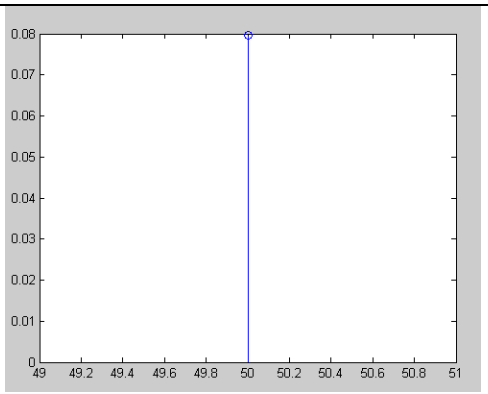
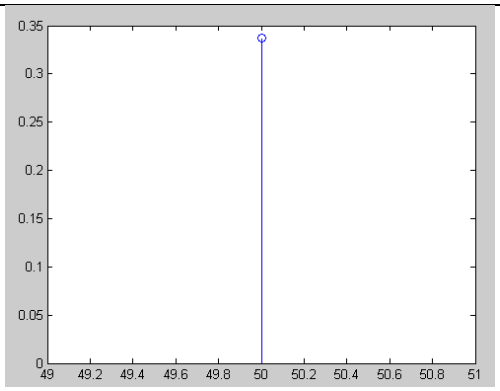


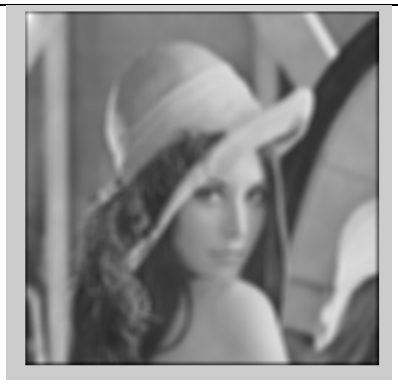
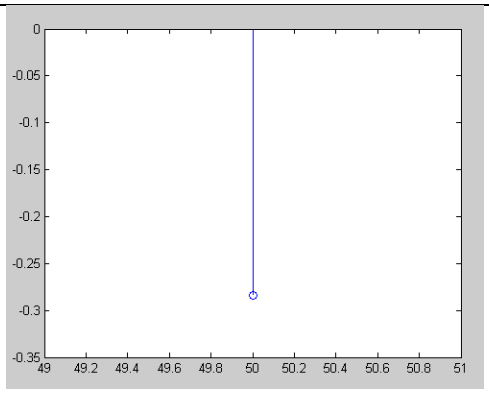
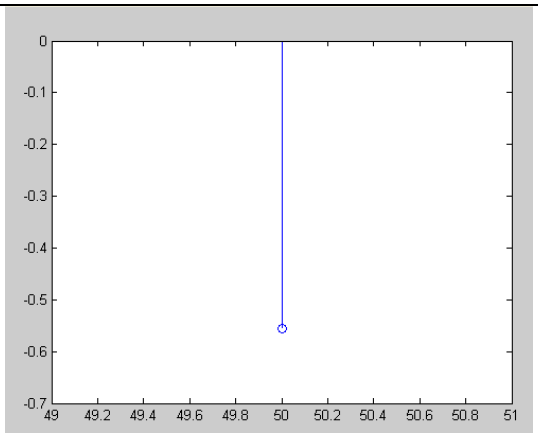
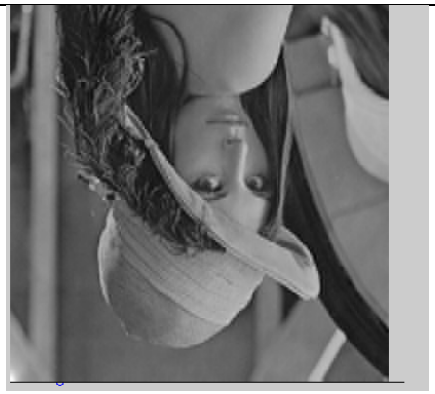
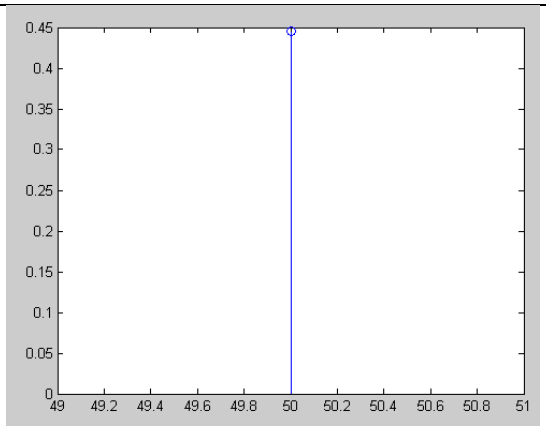
2.1. pav. ***DCT metodu paženklintas paveikslėlis***

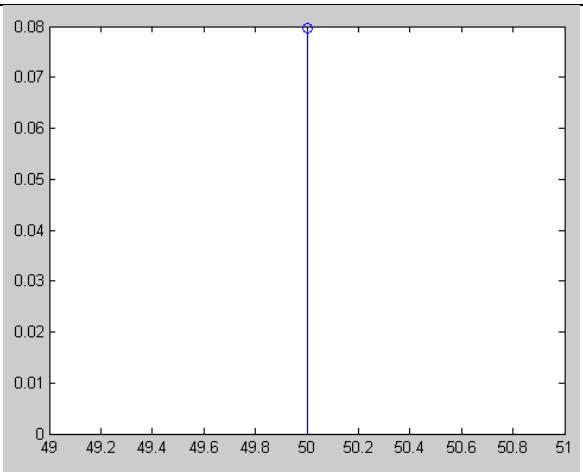
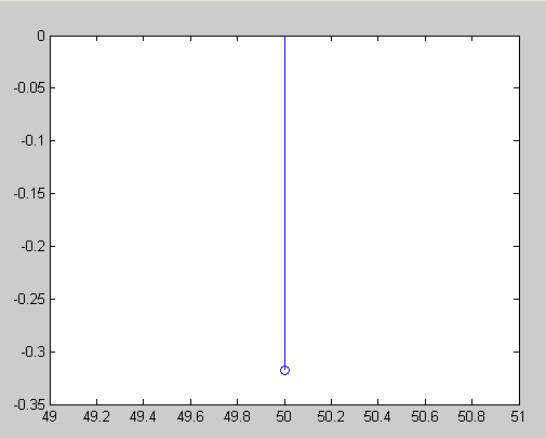
Naudojanti diskrečiojo kosinuso transformacija, originalus vaizdas, buvo paveiktas DCT koeficientų matrica, sugeneruotas vandens ženklo signalas (2,1 pav.), kurioje yra visos DCT koeficientų svarbiausių komponenčių amplitudės. Įterpus vandens ženklą svarbiausia vandens ženklo amplitudė yra 0,8 (2,2 lentelė). Ši vaizdą su vandens ženklu keičiant įvairiomis modifikacijomis keičiasi ir svarbiausia amplitudė. Mažiausią poveikį applitudės kitimui turi pasukimas iki 15˚. Paveikus baltuoju triukšmu ar panaudojus JPEG suspaudimą, jos sumažėja. Atlikus aplkarpymą, ar paveikus Gauso filtru amplitudės ženklas pakinta, t.y. ji nukrypsta į kitą pusę.

2.2. lentelė

Vaizdas ir svarbiausias DCT koeficientas po įvairių apdorojimų

Ataka	Gaunamas vaizdas	Svarbiausia DCT amplitudė
Įterpus vandens ženklą		
Paveikus baltuoju triukšmu		

Gauso filtras		
Apkarpymas		
JPEG suspaudimas		

Pasukimas 5 laipsnių kampu		
Pasukimas 45 laipsnių kampu		

Naudojantis DCT į pradinį paveikslėlį (2.2pav.) įterpiamas vaizdinis vandens ženklas (2.3 pav.). Įterpimo bandymui naudojamas originalus paveikslėli “Lena” 384×384 pikselių nespalvota nuotrauka. Binariam vandens ženklui X naudojamas logotipas (2.3. pav.) 36×36 pikselių nespalvotas paveikslėlis. Rezultatas parodė, kad nėra jokio pastebimo vaizdo suprastėjimo 2.4 pav. Su piko signal ir triukšmo santykiu PSNR = 2.1947e+003 (PSNR – angl. peak signal-to-noise ratio).

$$PSNR = 10 \log \left[\frac{\max\left(I(i,j)\right)^2}{\sum_{N,M}\left(I'(i,j) - I(i,j)\right)^2} \right] \quad \textbf{(2.1)}$$

Kur I – originalus vaizdas.

Normalizuotas koreliacijos koeficienatas:

$$NC = \frac{\sum_{X=0}^{M-1}\sum_{Y=o}^{N-1}(X - X')(Y - Y')}{[\sum_{X=0}^{M-1}\sum_{Y=o}^{N-1}(X - X')^2(Y - Y')^2]^{1/2}} \quad \textbf{(2.2)}$$

Y – išgautas vandens ženklas, X – originalus vandens ženklas.

2.2. pav. Originalus paveikslėlis

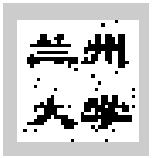
2.3. pav. Vandens ženklas

2.4. pav. Paveikslėlis su vandens ženklu(psnr = 2.1947e+003)

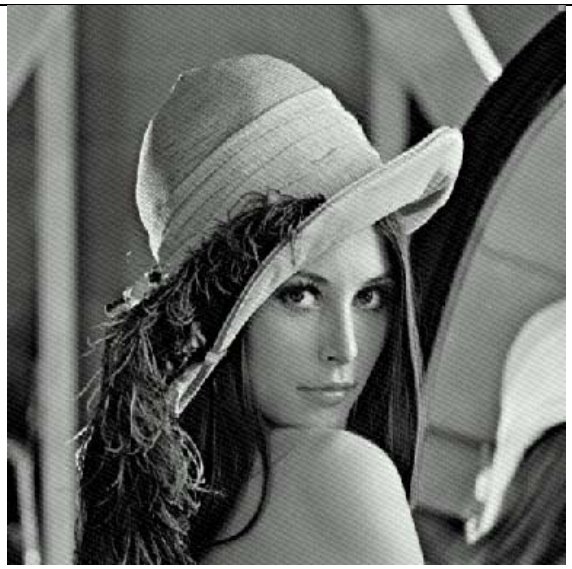
2.5. pav. Ištrauktas vandens ženklas

2.3. lentelė

Ištraukti vandens ženklai iš paženklinto vandensženkliu ir paveikto skirtingomis atakomis paveiksliuko, ir jo ištraukimo trukmė

Atakos pavadinimas	Gautas vaizdas	Ištrauktas vandens ženklas	Vandens ženklo ištraukimo laikas
Paveikus baltuoju triukšmu			elapsed_time = 1.0630
Pritaikius Gauso filtra			elapsed_time = 0.9060

Suspaudimas			elapsed_time = 1.6560
Dalies vaizdo iškirpimas			elapsed_time = 0.8910
Sušvelninus fokusuotę			elapsed_time = 0.9530

Pasukimas 90 laipsniu			elapsed_time = 0.9850
Spalvu derinimas			elapsed_time = 0.9690
Spalvu derinimas			elapsed_time = 0.9530

Kaip matome iš 2.3 lentelės, net elementarūs vaizdų apdorojimo būdai turi įtako įterptąjam vandens ženklo vaizdui. Vaizdo ženklas atsparus vaizdo suspaudimui ir paveikimu Gausu filtru. Tačiau tokie elemtarūs paveikslėlio apdorojimo budai, kaip dalies vaizdo iškirpimas, pasukimas gali neatpažystamai pakeisti vandens ženklą. Tačiau vandens ženklas lieka atpažįstapas po spalvų derinimo, arba netgi išlieka nepakitės. Tai rodo, kad šis vandens ženklo įterpimo metodas, nėra labai tvirtas, tačiau DCT metodas yra vienas iš pagrindinių taikomų paveikslelių ženklinimiui vandens ženklais. Pangrinėjus paveikslėlių dydį, pastebime, kad vandens ženklas neįtakoja jo dydžio. Mūsų nagrinėjamas paveikslėlis „Lena“ užima 145 KB, o „Lena“ su įtrauktu vandens ženklu, kurio dydis 1,5 KB, užima tiek pat atminties, kaip ir be vandens ženklo 145 KB.

IŠVADOS

Tyrimui pasirinktas vienas iš dažniausia naudojamų vandens ženklų metodų, siekiant nustatyti šio metodo atsparumą įvairioms vaizdo transformacijoms.

Atlikus vaizdo kontrasto keitimą, kurį galima užfiksuoti akimis, tačiau vaizdo kokybei pasikeitus nežymimai, vandens ženklas nepasikeičia. Kontrastą pakeitus ženkliai dėl kurio nukenčia ir vaizdo kokybės registruojamas akimis, vandens ženklas yra pakitęs, bet lieka dar atpažįstamas. Tai yra pakankamas vandens ženklo atsparumas kontrasto modifikacijai, nes tokio iškraipyto vaizdo stebėjimas neturi praktinės reikšmės.

Ištirtas vandens ženklo atsparumas atliekant vaizdo pasukimą. Nustatyta, kad pasukus vaizdą iki 15°, vandens ženklas dar atpažįstamas.

Ištirtas vandens ženklo atsparumas, iškerpant dalį vaizdo, nustatyta, kad pašalinus iki 25% vaizdo, vandens ženklas yra pasikeitęs, bet dar atpažįstamas.

Atlikus vaizdo suspaudimą JPEG metodu, vandens ženklo pakitimas nepastebimas.

Paveikus vaizdą su vandens ženklu baltuoju triukšmu suprastėja vaizdo kokybė, dėl to šiek tiek transformuojasi ir vandens ženklas, bet jis dar puikiai atpažįstamas.

Nustatyta, kad diskrečiojo kosinuso transformacija tinka vandens ženklo formavimui ir yra pakankamai atsparus paveikimui baltuoju triukšmu, suspaudimo, vaizdo kontrasto pakeitimo, dalies vaizdo iškirpimo transformacijoms.

LITERATŪRA

1. A. Noore, An Improved Method to Watermark Images Sensitive to Blocking Artifact, International Journal of Signal Processing, Vol. 1, Nr. 3. 129-134 p.
2. Biermann, Christopher J. (1996). "7". *Handbook of Pulping and Papermaking* (2 ed.). San Diego, California, USA: Academic Press. p. 171. ISBN 0-12-097362-6
3. Biermann, Christopher J. (1996). "7". *Handbook of Pulping and Papermaking* (2 Ed.). San Diego, California, USA: Academic Press. p. 171. ISBN 0-12-097362-6
4. C. Venkata Narasimhulu, K. Satya Prasad, A hybrid watermarking scheme using contourlet transform and singular value decomposition, IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.9, September 2010, 12-17p.
5. Chinese remainder theorem, http://en.wikipedia.org/wiki/Chinese_remainder_theorem (žiūrėta 2011.05.25)
6. Digital Watermarking for Digital Media
7. Discrete cosine transform , http://en.wikipedia.org/wiki/Discrete_cosine_transform (žiūrėta 2011.05 25)
8. G. Radhamani, G. S. V. Radha Krishna Rao, Web Services Security and E-Business
9. http://www.watermarker.com/links.aspx
10. I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, T. Kalker, Digital Watermarking and Stenography, 2008
11. I.J.Cox, J.Kilian, F.T,Leighton ir T.Shamoon, Secure spread spectrum watermarking for multimedia, IEEE Transactions on Image Processing. Vol 6, no. 12 pp. 1673-1687, 1997
12. Y. Feng, S. Luo, L. Pan, An Extensive Method to detect thr Image Digital Watermarking Based on the Know Template, 2006, 7h Pacific Rim Conference on Multimedia, Hangzhou, China, 31- 40p. http://books.google.lt/books?id=cdjzYLNgs_kC&pg=PA31&dq=image+digital+watermarking&hl=lt&ei=tlfCTZOAH8qEOuy1mZ0I&sa=X&oi=book_result&ct=result&resnum=1&ved=0CEAQ6AEwAA#v=onepage&q=image%20digital%20watermarking&f=false (žiūrėta 2011.05.20).
13. J. Cummins, P. Diskin, S. Lau, R. Parlett, Stegonography and digital watermarking; 2004
14. K. Gopalakrishnan, N. Memon, P. L. Vora, Protocols for Watermark Verification, Multimedia and security 66-70p.
15. L. Yongliang, W. Gao, Secure Watermark Verification Scheme, 0-7803-8603-5/04/$20.00 ©2004 IEEE.
16. S. Baba, L. Krikor, T. Arif, Z. Shaaban; Watermarking of digital images in frequency domain; International Journal of Automation and Computing 00(0).
17. S. P. Mahonty, K. R. Ramakrishnan, M. S. Kankanhalli, A DCT Domain Visible Watermarking Technique for images.

18. Shing-Chi Cheunng, Dickson K.W, Chiu, Cedric Ho, The use of Digital Watermarking for Intelligence Multimedia Document Distribution, Journal of Theoretical and Applied Electronic Commerce Research, Vol 3/ISSUE 3/ December 2008/ 103-118. (www.jtaer.com).

PRIEDAI

Dct_watermarkIN.m

```
clear all;
clc
% apskaiciavimo laikas
start_time=cputime;

k=50;      % minimalus koeficientu skirtumas
blocksize=8;      %   nustatytas   bloku   apimties   dydis   naudojant   bitus
vandenszenklyje

% originalaus vaizdo nuskaitymas
file_name='lena.bmp';
cover_object=double(imread(file_name));

% originalaus vaizdo dydzio testavimas
Mc=size(cover_object,1);       %ilgis
Nc=size(cover_object,2);       %plotis


max_message=Mc*Nc/(blocksize^2);

% nuskaitomas vandenszenklis
file_name='lzdx.jpg';
message0=double(im2bw(imread(file_name),0.7));
Mm=size(message0,1);          %ilgis
Nm=size(message0,2);          %plotis

% vektoriaus transformacija vandenzenklio informacijai
message=reshape(message0,Mm*Nm,1);

% tikrinama ar vandenszenklis neperdidelis
if (length(message) > max_message)
  error('vandens zenklo informacija per didele iterpimui!')
end

message_pad=ones(1,max_message);
message_pad(1:length(message))=message;
watermarked_image=cover_object;

% bloku procesas paveiksleliui
%  sifravimo  procesas,  jei  pranesimas  (kk)  =  0  tada  (5,2)  "(4,3);  jei
pranesimas (kk) = 1 tada (5,2) <(4,3)
x=1;
y=1;
for (kk = 1:length(message_pad))

  % DCT transformacija
  dct_block=dct2(cover_object(y:y+blocksize-1,x:x+blocksize-1));

  % jei informacijos bitas yra "juodas", (5,2) "(4,3)
```

```
  if (message_pad(kk) == 0)

    % jei (5,2) <(4,3) keitimas
    if (dct_block(5,2) < dct_block(4,3))
        temp=dct_block(4,3);
        dct_block(4,3)=dct_block(5,2);
        dct_block(5,2)=temp;
    end

  % jei informacijos bitas yra "baltas", (5,2) <(4,3)
  elseif (message_pad(kk) == 1)

    % jei (5,2) > (4,3)
    if (dct_block(5,2) >= dct_block(4,3))
        temp=dct_block(4,3);
        dct_block(4,3)=dct_block(5,2);
        dct_block(5,2)=temp;
    end
  end

  % koeficientu reguliavimas
  if dct_block(5,2) > dct_block(4,3)
    if dct_block(5,2) - dct_block(4,3) < k
      dct_block(5,2)=dct_block(5,2)+(k/2);
      dct_block(4,3)=dct_block(4,3)-(k/2);
    end
  else
     if dct_block(4,3) - dct_block(5,2) < k
      dct_block(4,3)=dct_block(4,3)+(k/2);
      dct_block(5,2)=dct_block(5,2)-(k/2);
    end
  end

  % kiekvieno erdvinio bloko transformacija
  watermarked_image(y:y+blocksize-1,x:x+blocksize-1)=idct2(dct_block);

  if (x+blocksize) >= Nc
    x=1;
    y=y+blocksize;
  else
    x=x+blocksize;
  end
end

% Perskaičiavimas į 8-bitų vaizda ir išėjima
watermarked_image_int=uint8(watermarked_image);
imwrite(watermarked_image_int,'dct1_watermarked.bmp','bmp');

% proceso trukme
elapsed_time=cputime-start_time,

%vandenszenklio vaizdo PSNR
psnr=psnr(cover_object,watermarked_image,Nc,Mc),
NC=NC(cover_object,watermarked_image);
```

```
% parodomas pazenklintas vandens zenklu vaizdas
figure(1)
imshow(cover_object,[]);
title('pradinis paveikslelis');
figure(2)
imshow(watermarked_image,[]);
title('paveikslelis su iterptu vandens zenklas');
figure(3)
imshow(message0,[]);
title('vandens zenklas');
a1=watermarked_image;
%%%%%% eksperimiantines testas vandens zenklo tvirtumui %%%%%%%%%%
disp('vandens zenklo bandymas paveikiant paveiksleli, pasirinkite:');
disp('1 - pridedamas baltasis triuksmas ');
disp('2 - Gauso filtras ');
disp('3 - JPEG suspaudimas ');
disp('4 - paveikslelio apkarpymas');
disp('5 - pasukimas');
disp('6 - aptikti vaizda su nesugadintu vandens zenklu');
disp('kita - nera tokio poveikio');
d=input('Pasirinkite viena (1-6 ):');
start_time=cputime;

  figure(1);
      switch d
        case 6
      subplot(1,1,1);
      imshow(a1,[]);
      title('vaizda su nesugadintu vandens zenklu');
      M1=a1;
      M_1=uint8(M1);
       imwrite(M_1,'watermarked.bmp','bmp');
        case 1
       WImage2=a1;
       noise0=20*randn(size(WImage2));
       WImage2=WImage2+noise0;
       subplot(1,1,1);
       imshow(WImage2,[]);
       title('Po paveikslelio paveikimo baltuoju triuksmu');
       M1=WImage2;
       M_1=uint8(M1);
       imwrite(M_1,'whitenoise.bmp','bmp');

        case 2
       WImage3=a1;
       H=fspecial('gaussian',[4,4],0.2);
       WImage3=imfilter(WImage3,H);
       subplot(1,1,1);
       imshow(WImage3,[]);
       title('po paveikimo Gauso filtras');
       M1=WImage3;
       M_1=uint8(M1);
       imwrite(M_1,'gaussian.bmp','bmp');
```

```
         case 3
        WImage5=a1;
        WImage5=im2double(WImage5);
        cnum=10;
        dctm=dctmtx(8);
        P1=dctm;
        P2=dctm.';
        imageDCT=blkproc(WImage5,[8,8],'P1*x*P2',dctm,dctm.');
        DCTvar=im2col(imageDCT,[8,8],'distinct').';
        n=size(DCTvar,1);
        DCTvar=(sum(DCTvar.*DCTvar)-(sum(DCTvar)/n).^2)/n;
        [dum,order]=sort(DCTvar);
        cnum=64-cnum;
        mask=ones(8,8);
        mask(order(1:cnum))=zeros(1,cnum);
        im88=zeros(9,9);
        im88(1:8,1:8)=mask;
        im128128=kron(im88(1:8,1:8),ones(16));
        dctm=dctmtx(8);
        P1=dctm.';
        P2=mask(1:8,1:8);
        P3=dctm;

WImage5=blkproc(imageDCT,[8,8],'P1*(x.*P2)*P3',dctm.',mask(1:8,1:8),dctm);
       WImage5cl=mat2gray(WImage5);
       subplot(1,1,1);
       imshow(WImage5cl);
       title(' JPEG suspaustas vaizdas');
       M1=WImage5cl;
       M_1=uint8(M1);
       imwrite(M_1,'JEPG express.bmp','bmp');

        case 4
       WImage4=a1;
       WImage4(1:64,1:512)=512;
       WImage4cl=mat2gray(WImage4);
       figure(2);
       subplot(1,1,1);
       imshow(WImage4cl);
       title('dalies vaizdo iskirpimas');
       figure(1);
       M1=WImage4cl;
       M_1=uint8(M1);
       imwrite(M_1,'cutpart.bmp','bmp');

        case 5
      WImage6=a1;
      WImage6=imrotate(WImage6,10,'bilinear','crop');
      WImage6cl=mat2gray(WImage6);
      figure(2);
      subplot(1,1,1);
      imshow(WImage6cl);
      title('pasukimas 10 laipsniu kampu');
```

```
      figure(1);
      M1=WImage6cl;
       M_1=uint8(M1);
       imwrite(M_1,'turnround.bmp','bmp');


        otherwise
      disp('neteisinga, duomenys yra skaitmeninys (1:6), tiesiogiai aptikamas
vandenženklis');
      subplot(1,1,1);
      imshow(a1,[]);
      title('nesugadintas vandens zenklo vaizdas');
      M1=a1;
        End
```

Dct_watermarkOUT.m

```
clear all;

% ivykdymo laikas
start_time=cputime;

blocksize=8;

%pazenklinto vaizdo nuskaitymas
file_name='watermarked.bmp';
watermarked_image=double(imread(file_name));

Mw=size(watermarked_image,1);        %ilgis
Nw=size(watermarked_image,2);        %plotis

% maksimalalaus bitu nustatymas
max_message=Mw*Nw/(blocksize^2);

x=1;
y=1;
for (kk = 1:max_message)

   % DCT
  dct_block=dct2(watermarked_image(y:y+blocksize-1,x:x+blocksize-1));

   % if dct_block (5,2)> dct_block (4,3) then message (kk) = 0
   % Other message (kk) = 1
  if dct_block(5,2) > dct_block(4,3)
    message_vector(kk)=0;
  else
    message_vector(kk)=1;
  end

    if (x+blocksize) >= Nw
    x=1;
    y=y+blocksize;
  else
```

```
    x=x+blocksize;
  end
end

% vaizdo iterpimas
message=reshape(message_vector(1:36*36),36,36);

% proceso trukme
elapsed_time=cputime-start_time,

figure(4)
imshow(message,[])
title('vandens zenklas')
```