VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

Artūras KRIUKOVAS

VAIZDO SKAITMENINIS PARAŠAS VAIZDINĖS INFORMACIJOS APSAUGAI

DAKTARO DISERTACIJOS SANTRAUKA

TECHNOLOGIJOS MOKSLAI,
INFORMATIKOS INŽINERIJA (07T)

LEIDYKLA
TECHNIKA
Vilnius 2010

Disertacija rengta 2006–2010 metais Vilniaus Gedimino technikos universitete.

Mokslinis vadovas

prof. habil. dr. Romualdas BAUŠYS (Vilniaus Gedimino technikos universitetas, technologijos mokslai, informatikos inžinerija – 07T).

Disertacija ginama Vilniaus Gedimino technikos universiteto Informatikos inžinerijos mokslo krypties taryboje:

Pirmininkas

prof. habil. dr. Antanas ČENYS (Vilniaus Gedimino technikos universitetas, technologijos mokslai, informatikos inžinerija – 07T).

Nariai:

prof. dr. Romas BARONAS (Vilniaus universitetas, fiziniai mokslai, informatika – 09P),

prof. habil. dr. Gintautas DZEMYDA (Matematikos ir informatikos institutas, technologijos mokslai, informatikos inžinerija – 07T),

prof. habil. dr. Genadijus KULVIETIS (Vilniaus Gedimino technikos universitetas, technologijos mokslai, informatikos inžinerija – 07T),

prof. habil. dr. Rimantas ŠEINAUSKAS (Kauno technologijos universitetas, technologijos mokslai, informatikos inžinerija – 07T).

Oponentai:

prof. dr. Dalius NAVAKAUSKAS (Vilniaus Gedimino technikos universitetas, technologijos mokslai, informatikos inžinerija – 07T),

prof. habil. dr. Rimvydas SIMUTIS (Kauno technologijos universitetas, technologijos mokslai, informatikos inžinerija – 07T).

Disertacija bus ginama viešame Informatikos inžinerijos mokslo krypties tarybos posėdyje 2010 m. lapkričio 4 d. 14 val. Vilniaus Gedimino technikos universiteto senato posėdžių salėje.

Adresas: Saulėtekio al. 11, LT-10223 Vilnius, Lietuva.

Tel.: (8 5) 274 4952, (8 5) 274 4956; faksas (8 5) 270 0112;

el. paštas doktor@vgtu.lt

Disertacijos santrauka išsiuntinėta 2010 m. spalio 1 d.

Disertaciją galima peržiūrėti Vilniaus Gedimino technikos universiteto (Saulėtekio al. 14, LT-10223 Vilnius, Lietuva) ir Matematikos ir informatikos instituto (Akademijos g. 4., LT-08663 Vilnius, Lietuva) bibliotekose.

VGTU leidyklos „Technika“ 1799-M mokslo literatūros knyga.

VILNIUS GEDIMINAS TECHNICAL UNIVERSITY

Artūras KRIUKOVAS

DIGITAL SIGNATURE TECHNOLOGIES FOR IMAGE INFORMATION ASSURANCE

SUMMARY OF DOCTORAL DISSERTATION

TECHNOLOGICAL SCIENCES,
INFORMATICS ENGINEERING (07T)

VGTU
LEIDYKLA
TECHNIKA
Vilnius 2010

Doctoral dissertation was prepared at Vilnius Gediminas Technical University in 2006–2010.

Scientific Supervisor

Prof Dr Habil Romualdas BAUŠYS (Vilnius Gediminas Technical University, Technological Sciences, Informatics Engineering – 07T).

The dissertation is being defended at the Council of Scientific Field of Informatics Engineering at Vilnius Gediminas Technical University:

Chairman

Prof Dr Habil Antanas ČENYS (Vilnius Gediminas Technical University, Technological Sciences, Informatics Engineering – 07T).

Members:

Prof Dr Romas BARONAS (Vilnius University, Physical Sciences, Informatics – 09P),

Prof Dr Habil Gintautas DZEMYDA (Institute of Mathematics and Informatics, Technological Sciences, Informatics Engineering – 07T),

Prof Dr Habil Genadijus KULVIETIS (Vilnius Gediminas Technical University, Technological Sciences, Informatics Engineering – 07T),

Prof Dr Habil Rimantas ŠEINAUSKAS (Kaunas University of Technology, Technological Sciences, Informatics Engineering – 07T).

Opponents:

Prof Dr Dalius NAVAKAUSKAS (Vilnius Gediminas Technical University, Technological Sciences, Informatics Engineering – 07T),

Prof Dr Habil Rimvydas SIMUTIS (Kaunas University of Technology, Technological Sciences, Informatics Engineering – 07T).

The dissertation will be defended at the public meeting of the Council of Scientific Field of Informatics Engineering in the Senate Hall of Vilnius Gediminas Technical University at 2 p. m. on 4 November 2010.

Address: Saulėtekio al. 11, LT-10223 Vilnius, Lithuania.
Tel.: +370 5 274 4952, +370 5 274 4956; fax +370 5 270 0112;
e-mail: doktor@vgtu.lt

The summary of the doctoral dissertation was distributed on 1 October 2010.

A copy of the doctoral dissertation is available for review at the Library of Vilnius Gediminas Technical University (Saulėtekio al. 14, LT-10223 Vilnius, Lithuania) and at the Library of Institute of Mathematics and Informatics (Akademijos str. 4, LT-08663, Vilnius, Lithuania).

Įvadas

Mokslo problemos aktualumas. Nuo asmeninių kompiuterių atsiradimo laikų ir interneto plėtros pradžios, technologinė evoliucija skatina skaitmeninių vaizdų ir nuotraukų plitimą plačiojoje visuomenėje. Profesionalių vaizdo redagavimo programų tobulėjimas leidžia lengvai redaguoti skaitmeninį atvaizdą taip, kad neprofesionalas nepastebėtų jokių pakeitimų. Todėl vis aktualesni tampa vaizdų autentiškumo užtikrinimo ir pažeidimų nustatymo klausimai. Medicininiai duomenys, naujausios žinios ar politinių įvykių nuotraukos yra tik keli pavyzdžiai to, kai „tikime vaizdu“ ir neteisinga informacija čia nėra priimtina.

Įprastiniai duomenų apsaugos metodai – kriptografinės kontrolinės sumos ar asimetrinė kriptografija su skaitmeniniais parašais – gali būti tiesiogiai pritaikomi atvaizdų apsaugai. Bet yra vienas pakankamai svarbus skirtumas tarp atvaizdų ir skaitmeninių dokumentų, kuriems paprastai yra taikomi įprastiniai kriptografiniai duomenų apsaugos metodai. Skaitmeninės nuotraukos, video medžiaga, pasižymi didele pertekline informacija. Duomenų apdorojimas – suspaudimas ar kokybės gerinimas ryškinant ar blukinant vaizdą – manipuliavimas ta pertekline informacija, yra labai tikėtinas prieš pateikiant vaizdą galutiniam vartotojui. Toks apdorojimas nepakeičia nei vaizdo autentiškumo, nei esmės. Įprastiniai duomenų apsaugos metodai atmes tokį apdorojimą kaip neleistiną, nes jie tikrina ir autentifikuoja binarinę skaitmeninio vaizdo formą, o ne turinį, saugomą toje skaitmeninėje formoje. Tačiau tikrinant vaizdo autentiškumą, svarbus būtent turinys, esmė, o ne tos esmės skaitmeninė išraiška ar formatas.

Žvelgiant giliau, vien tik autentiškumo nustatymo ne visada pakanka – pažeidimų radimo procedūros įgalina mus nustatyti patikimas ir pažeistas zonas. Šios žinios leidžia efektyviau išnaudoti gautą neautentišką atvaizdą – leidžia nustatyti, kokie pakeitimai atlikti, leidžia nustatyti, ar mus dominanti vaizdinės informacijos dalis nėra sąmoningai padirbta. Blokiniai metodai aptinka pažeistą bloką. Pikselių tikslumo metodai aptinka pažeistus pikselius. Žinoma, pikselių tikslumas yra reikalingesnis – blokiniai metodai neleidžia atlikti tikslios analizės – identifikavus pažeistą bloką neįmanoma pasakyti ar netyčia pažeistas vienas pikselis 100x100 dydžio bloke – ar visi 9‘999 pikseliai.

Pastaraisiais metais atvaizdo autentiškumo nustatymui ir pažeidimų suradimui atsirado nauji sprendimai – vaizdo vandens ženklai ir skaitmeniniai parašai (reikia pastebėti, kad vaizdo skaitmeninis parašas skiriasi nuo skaitmeninio parašo naudojamo asimetrinėje kriptografijoje). Dauguma šių metodų orientuojami į jautrų vaizdo autentifikavimą ir pažeidimų lokalizavimą, t. y. metodo tikslas yra identifikuoti ir surasti bet kokius atvaizdo pakeitimus.

Nepalyginamai mažiau yra metodų, leidžiančių pusiau jautrų vaizdo autentifikavimą ir pažeidimų radimą – metodų, atsparių, arba nejautrių, tam tikrai vaizdo pakitimų aibei – ir jautrių visiems kitiems vaizdo pakeitimams. Pvz., metodas gali būti nejautrus vaizdo pasukimui ar suspaudimui – visai kasdieninėms vaizdo apdorojimo procedūroms. Yra ir tokių įprastų vaizdo apdorojimo procedūrų – vaizdo išblukinimo ar paryškinimo (*angl. blurring or sharpening*) – kurioms nėra atsparių vaizdo apsaugos metodų. Toks naujas metodas, atsparus blukinimui ir ryškinimui, ir bus pristatytas šiame darbe.

Šiame darbe analizuojami metodai, skirti patikrinti atvaizdo autentiškumą ir galintys atlikti pikselių tikslumo lygmens pažeidimų lokalizavimą. Šie metodai, atsparūs vadinamosioms bendroms vaizdų apdorojimo procedūroms (blukinimui, ryškinimui, suspaudimui ar pasukimui) ir jautrūs visoms kitoms modifikacijoms. Įsitikinus, kad tokių metodų nėra, sukuriama nauja vaizdo transformacija, kurios erdvė atspari blukinimo ir ryškinimo operacijoms. Sukuriama duomenų neprarandanti diskretinė vaizdo transformacija į polines koordinates, kad būtų užtikrintas atsparumas pasukimui. Pristatomas naujas vaizdo skaitmeninio parašo metodas, paremtas pasiūlytomis transformacijomis, skirtas atspariam autentiškumo nustatymui ir pusiau jautriam pažeidimų lokalizavimui. Specialus dėmesys atkreipiamas į pažeistų pikselių lokalizavimo efektyvumą, nepaisant vaizdo blukinimo ar ryškinimo operacijų, nes šios paprastos ir kasdienės vaizdo apdorojimo procedūros pasižymi labai intensyviu poveikiu visiems atvaizdo pikseliams ir dėl to jos yra ypatingai sudėtingos visiems pikselių tikslumą suteikiantiems metodams.

Tyrimo objektas. Tyrimo objektas – atvaizdo autentiškumo nustatymas ir pažeistų pikselių lokalizavimas po bendrųjų vaizdo apdorojimo procedūrų.

Darbo tikslas ir uždaviniai. Pagrindinis darbo tikslas yra metodo, apjungiančio atsparų atvaizdo autentifikavimą ir pusiau jautrų (atsižvelgiant į vaizdo blukinimą, aštrinimą, pasukimą ir suspaudimą, t. y. į vadinamąsias bendrąsias vaizdo apdorojimo procedūras, kurios nekeičia atvaizdo esmės) pažeistų pikselių lokalizavimą, sukūrimas. Darbo tikslui pasiekti reikia išspręsti šiuos uždavinius:

1. Sukurti vaizdo transformaciją, atsparią blukinimui, aštrinimui, pasukimui ir suspaudimui, bet jautrią visiems kitiems vaizdo pakeitimams. Transformacija turi išlaikyti griežtą pikselių sąsają su atvaizdo pikseliais, kad būtų galima surasti pažeistus atvaizdo pikselius.
2. Sukurti algoritmą, pusiau jautriam paskirų pikselių tikslumo pažeidimų lokalizavimui, remiantis sukurta transformacija. Algoritmas

turi būti atsparus bendroms vaizdo apdorojimo procedūroms ir jautrus visiems kitiems veiksniams.

3. Sukurti algoritmą atspariam vaizdo autentifikavimui, nepriklausomą nuo pažeidimų lokalizavimo algoritmo.
4. Parašyti programą skaitmeniniu parašu paremtam metodui realizuoti, apjungiančią anksčiau pasiūlytus algoritmus vaizdo autentifikavimui ir pažeidimų lokalizavimui. Metodas turi pasižymėti šiomis savybėmis:
    a) vaizdo autentifikavimas turi būti atsparus visoms vaizdo apdorojimo procedūroms, kurios tik išlaiko atvaizdo esmę;
    b) vaizdo autentifikavimo procesas turi susilaikyti nuo griežto binarinio atsakymo – „patikima/nepatikima“. Turi būti išduodama procentinė patikimumo įvertinimo reikšmė;
    c) pažeidimų lokalizavimas turi būti paskirų pikselių tikslumo;
    d) pažeidimų lokalizavimo procesas turi būti atsparus bendroms vaizdo apdorojimo procedūroms. Visos kitos vaizdo apdorojimo operacijos turi būti laikomos neleistinomis, šių operacijų pakeisti pikseliai turi būti surandami;
    e) pažeidimų lokalizavimo procesas turi būti atskirtas nuo autentiškumo nustatymo, kad būtų išvengta orakulo tipo atakų;
    f) metodas turi remtis skaitmeninio parašo technologija, kad būtų neveikiamas steganalizės.

Tyrimų metodika. Siekiant užsibrėžtų tikslų, buvo taikomi šie tyrimų metodai:

1. Lyginamosios analizės ir literatūros analizės metodai. Šie metodai buvo taikomi analizuojant atvaizdų vandens ženklus ir skaitmeninius parašus, JPEG-2000 standartą, bangelių ir Furje transformacijas, orakulo, blukinimo ir ryškinimo atakas.
2. Apibendrinant analizės rezultatus bei formuluojant pasiūlymus buvo taikomi apibendrinimo ir loginės indukcijos metodai.
3. Eksperimentinio tyrimo metodai buvo taikomi tikrinant sukurto metodo veikimo tikslumą ir efektyvumą.

Mokslinis naujumas. Rengiant disertaciją, gauti šie informatikos inžinerijos mokslui nauji teoriniai ir praktiniai rezultatai:

1. Sukurta modifikuoto fazės filtro transformacija. Ši transformacija išnaudoja Furjė fazės ypatybę – invariantiškumą vaizdo blukinimui arba ryškinimui ir sukuria griežtą sąryšį tarp pikselių paprastoje vaizdo erdvėje ir Furje fazės erdvėje.

2. Sukurta nauja vaizdo transformacija, duomenų neprarandančiai diskretinei konversijai į polines koordinates ir atgal. Priešingai egzistuojantiems metodams, konversijai nereikia interpoliacijos, ji vykdoma sveikųjų skaičių erdvėje – taip išvengiama duomenų praradimo. Tai leidžia sukurti pikselių tikslumo pažeidimų lokalizavimą, atsparų pasukimui.
3. Sukurtas algoritmas, leidžiantis lokalizuoti pažeistus atvaizdo pikselius, nepaisant bendrųjų vaizdo apdorojimo procedūrų.
4. Sukurtas skaitmeninio parašo metodas atspariam atvaizdo autentifikavimui su pusiau jautriu pažeistų pikselių lokalizavimu. Metodo architektūra leidžia lengvai integruoti subjektyvią žmogaus nuomonę į autentiškumo nustatymo procesą, garantuoja matematiškai paprastą autentiškumo nustatymo mechanizmą, garantuoja apsaugą nuo orakulo atakų, nuo steganalizės metodų, garantuoja, kad originalus atvaizdas išliks nepakeistas, garantuoja autentiškumo nustatymą ir pažeistų pikselių radimą nepriklausomai nuo atliktų bendrųjų vaizdo apdorojimo procedūrų, garantuoja mažą parašo dydį (<10% pradinio atvaizdo dydžio), o taip pat pažeidimų lokalizavimą su skiriamąja geba iki vieno paskiro pikselio.

Praktinė vertė. Siūlomą metodą galima taikyti srityse, kur reikia autentifikuoti atvaizdą ir rasti piktybiškai pažeistus pikselius po bendrųjų vaizdo apdorojimo procedūrų.

Ginamieji teiginiai. Formuluojami šie ginamieji teiginiai:
1. Atvaizdo skaitmeninio parašo naudojimas garantuoja visų vaizdo bitų apsaugą.
2. Atvaizdo autentifikavimo algoritmo atskyrimas nuo pažeidimų lokalizacijos leidžia išvengti orakulo tipo atakų.
3. Furje fazės modifikuota transformacija gali būti naudojama pakeistų pikselių suradimui atvaizde nepriklausomai nuo atvaizdo blukinimo ar ryškinimo.

Darbo apimtis. Darbą sudaro įvadas, keturi pagrindiniai skyriai ir bendrosios išvados. Darbo apimtis – 119 puslapių, tekste panaudotos 104 numeruotos formulės, 8 paveikslai ir 11 lentelių. Rašant disertaciją panaudoti 150 literatūros šaltiniai. Darbas buvo pristatytas 2 konferencijose. Disertacijos tema publikuoti 3 straipsniai.

1. Esami metodai atvaizdų apsaugai užtikrinti

Skyriuje analizuojami esami metodai, skirti užtikrinti atvaizdų autentiškumą ar pažeistų pikselių radimą. Literatūros analizė rodo, kad šie metodai gali būti skirstomi pagal savo jautrumą – į jautrius, pusiau jautrius ir atsparius, pagal pažeidimų lokalizacijos tikslumą – į paskirų pikselių ar pikselių blokų (vadinamieji blokiniai metodai).

1 lentelė. Paryškinimo poveikis

Originalus atvaizdas

137	92	114	64	39	43	33	56
56	39	40	48	36	47	61	96
75	36	47	35	38	51	100	80
110	42	39	45	64	121	12	106
72	94	95	116	133	83	70	85
56	117	120	57	47	70	121	39

Pikselių reikšmių skaitmeninė matrica iš baltu stačiakampiu pažymėtos zonos. Paimkime dešiniojo apatiniojo kampo reikšmę – 39 – tolesnei analizei.

1x paryškintas atvaizdas

29	70	200	0	33	22	0	0
0	10	0	75	18	56	29	201
124	0	93	11	29	0	165	11
255	0	0	0	0	248	203	166
58	131	93	219	255	28	0	168
14	225	153	0	0	0	255	0

Kaip matome, reikšmė 39 nukrito iki nulio. Šalimais esanti reikšmė 255 – originale buvo 121.

Vienas iš didžiausių iššūkių ieškant pažeistų pikselių yra vaizdo blukinimo ar ryškinimo operacijų identifikavimas. Paprastai, kasdieniniame naudojime, šios operacijos nekeičia atvaizdo esmės. Bet jos yra tokios pavojingos dėl jų poveikio skaitmeninėms atvaizdų matricoms. Pirmoje lentelėje pateikiami keli atvaizdai – originali „Lena“ ir jos paryškinta versija – ir atitinkamos jų skaitmeninės matricos.

Nors vaizdo esmė akivaizdžiai nepasikeitė, tačiau pikselių reikšmės drastiškai svyruoja tarp juodos ir baltos (balta yra 255, juoda – 0) – tai teoriškai maksimaliai galimi pokyčiai, ribojami tik standartinio vaizdų apdorojime vieno baito sveikojo skaičiaus kompiuteryje ribomis – ir mes juos matome po pačios įprasčiausios vaizdo apdorojimo procedūros. Natūralu, kad pažeistų pikselių lokalizavimo algoritmai aptinka tokius pokyčius kaip neleistinus ir pažeidžiančius atvaizdo esmę – nors iš tiesų taip nėra – vaizdo esmė juk nepasikeitė. Štai kodėl dauguma metodų nebegali identifikuoti iš tikrųjų pažeistų pikselių jei atakuotas atvaizdas yra papildomai išblukintas arba paryškintas – visas atvaizdas atrodo masiškai pakeistas, sąmoningai pakeisti pikseliai tiesiog „paskęsta“ bendrame triukšme. Nėra paskirų pikselių tikslumo pažeidimų lokalizavimo metodų, atsparių vaizdo blukinimui arba ryškinimui. Net daliai blokinių metodų įprastinis ir kasdieninis blukinimas ar paryškinimas sukelia rimtų problemų. Jeigu norime turėti pažeistų pikselių lokalizavimą *po* blukinimo ar ryškinimo operacijų, mums reikia naujo sprendimo.

2. Siūlomo metodo teorinis pagrindimas

Antrame skyriuje įrodoma, kad jei blukinimo ar ryškinimo funkcijos yra simetrinės apie centrą (o taip ir yra standartiniu blukinimo/ryškinimo atveju), tuomet blukinimo ar ryškinimo funkcijos Furje transformacija yra realus skaičius ir fazė tuomet yra lygi tik 0 arba π. Šis įrodymas tapo vienu iš pagrindinių siūlomo metodo elementų, suteikiančių invariantiškumą vaizdo blukinimui ir ryškinimui. Reikia pastebėti, kad Furje transformacija ir taip pat Furje fazė neišlaiko erdvinio sąryšio su pradiniu atvaizdu. Pradinio atvaizdo pikselis transformuojamas į sinuso bangos savybę Furje erdvėje. Todėl jei norime turėti ne tik bendrą atsparumą blukinimui ar ryškinimui, bet ir pažeistų paskirų pikselių lokalizavimą, turime sukurti ir išlaikyti erdvinį sąryšį tarp pikselio pradiniame atvaizde ir pikselio Furje transformacijoje. Šio sąryšio sukūrimas ir buvo pagrindinė darbo problema, kuri išspręsta sukūrus modifikuotos fazės filtrą.

Metodo atsparumas pasukimui kilo iš Furje-Mellin transformacijos. Ši transformacija, remdamasi konversija į polines koordinates, paverčia sukimą apie centrą į vertikalų/horizontalų poslinkį. Kadangi atvaizdai kompiuteryje yra

diskretiniai, tiesioginė konversija į polines koordinates yra veikiama interpoliavimo paklaidų. Neradę pakankamai efektyvaus duomenų neprarandančio diskretinio konvertavimo metodo, mes turėjome sukurti savo, duomenų neprarandantį konvertavimo į polines koordinates ir iš jų, metodą.

Papildomas dėmesys buvo skirtas orakulo atakai, kaip vienai iš efektyviausių vaizdų autentiškumo metodų atakų. Aukštas atakos efektyvumas atsiranda dėl to, kad ataka nukreipiama ne į saugomus atvaizdus, bet į autentiškumo nustatymo ir pažeidimų lokalizavimo mechanizmus duomenų apsaugos metode. Taip pat atkreiptas dėmesys ir į tai, kad vandens ženklu apsaugotame piešinuke iš tikrųjų saugomas tik vienas bitas iš aštuonių – likusius bitus galima laisvai keisti, keisti atvaizdo esmę ir taip „apgauti“ autentiškumo nustatymo metodą. Dėl to, kad išvengti tokių „apgavysčių“, sukurtas metodas ne tik remiasi vaizdo skaitmeniniu parašu (kai apsaugomi visi bitai, ne tik pasirinktiniai), bet ir griežtai atskiria atvaizdo autentifikavimą nuo pažeidimų lokalizavimo.

3. Siūlomas metodas

Skyriuje detaliai aprašomi siūlomi nauji algoritmai, formuojantys galutinį metodą. Pirmas algoritmas garantuoja atsparumą nuo blukinimo ar ryškinimo operacijų – nauja modifikuotos fazės filtro transformacija. Antras algoritmas – nauja duomenų neprarandanti diskretinė konversija į/iš polinių koordinačių. Abu šie algoritmai apjungiami į naują skaitmeninio parašo metodą, galintį autentifikuoti atvaizdą nepriklausomai nuo atlikto blukinimo, ryškinimo, pasukimo ar suspaudimo, o taip pat rasti sąmoningai pažeistus pikselius.

3.1. Modifikuotos fazės filtras

Modifikuotos fazės filtro transformacija (MPOF) yra specialiai sukurta tam, kad išlaikytų griežtą ir tikslų sąryšį tarp pradinio atvaizdo pikselių ir Furje transformacijos fazės pikselių. Savo konstrukcijos dėka ši transformacija suteikia galimybę lokalizuoti piktybiškai pažeistus pikselius nepaisant atvaizdo blukinimo ar ryškinimo.

3.2. Duomenų neprarandanti diskretinė konversija į polines koordinates

Tolydžiuoju atveju, konvertuojant atvaizdą iš Dekarto į polines koordinates, pikseliai atvaizdo centre yra pernelyg smulkiai imami, lyginant su pikseliais kraštuose, kur atsiranda duomenų praradimas dėl pernelyg stambios imties. Diskrečiu atveju situacija yra dar blogesnė, nes trūkstamos reikšmės yra

interpoliuojamos iš artimiausios aplinkos – ir ši interpoliacija dar labiau padidina konversijos paklaidą. Bendruoju atveju, vien tik konversija į polines koordinates ir atgal, iškraipo konvertuojamą atvaizdą. Dėl šio netobulumo sukurta duomenų neprarandanti diskretinė konversija į polines koordinates.

3.3. Suspaudimas

Atskiras dėmesys skirtas efektyviam galutinio metodo veikimui. Siekiant gauti mažesnį atvaizdo skaitmeninį parašą, tikslinga panaudoti papildomus suspaudimo mechanizmus. Praktiniai eksperimentai su labiausiai paplitusiais suspaudimo metodais parodė, kad LZW metodo pritaikymas MPOF duomenims nesuteikė didelio suspaudimo laipsnio – buvo pasiektas maždaug 50% suspaudimas, kai paprastai pasiekiamas 70–90% suspaudimas. Huffmann'o metodas parodė blogiausius rezultatus – ~26% suspaudimas. Aritmetinė kompresija pasiekė ~32% suspaudimą. Toks žemas suspaudimo lygis yra dėl Furje fazės struktūros – duomenys ten labai artimi atsitiktiniam išsibarstymui. Tačiau pasiektas žymiai geresnis suspaudimo laipsnis – ~92% suspaudimas, išnaudojant specifines Furje fazės ypatybes.

3.4. Palyginimas su kitais metodais

Nepavyko rasti metodo, pasižyminčio visomis siūlomo metodo charakteristikomis (atsparus autentiškumas, pusiau jautrus pikselių tikslumo pažeidimų lokalizavimas), todėl tiesioginio lyginimo su kitais metodais atlikti negalima. Todėl bus lyginamos atskiros charakteristikos ir jomis panašūs metodai.

Išanalizavus literatūrą, pavyko rasti blukinimui ar ryškinimui atsparius metodus, tačiau jie visi yra blokiniai, kur bloko dydis yra mažiausiai 8x8 pikselių. Pažeidus bent vieną pikselį, visas 64-ių pikselių blokas identifikuojamas kaip nebepatikimas. Kai kuriais atvejais tokio lokalizacijos tikslumo pakanka, tačiau yra poreikis tiksliai, vieno pikselio tikslumo lokalizacijai, ir galima norimą tikslumą pasiekti. Tam sukurta MPOF transformacija, kuri suformuoja griežtą sąryšį tarp pikselio pradiniame atvaizde ir pikselio Furje transformacijos fazėje. Šio sąryšio buvimas leidžia nustatyti pažeistus pikselius nepaisant papildomo vaizdo blukinimo ar ryškinimo.

Literatūros apžvalga taip pat rodo, kad tipinis sprendimas apsaugai nuo pasukimo yra Furje-Mellin transformacija, paremta konversija į logaritmines-polines koordinates. Tačiau konversijos metu atsiranda paklaida, kuri didėja artėjant prie atvaizdo kraštų. Paklaidos efektas kažkuria prasme primena blukinimo ar aštrinimo efektą – pakeičiami visi atvaizdo pikseliai. Yra metodų

sumažinančių interpoliacijos paklaidą, pvz., analitinė Furje-Mellin transformacija, tačiau jos pilnai nepanaikina. Todėl siūloma duomenų neprarandanti diskrečioji konversija į polines koordinates.

Galimybė pilnai integruoti žmogaus nuomonę į autentiškumo nustatymo procesą yra dar viena naujovė. Kai kurie metodai leidžia pačiam vartotojui priimti galutinį sprendimą, remiantis gauta procentine arba indeksuota reikšme ir atsižvelgiant į panašius atvejus. Sukurtas metodas ne tik suteikia autentiškumo procentinę reikšmę, bet ir leidžia vizualiai įsitikinti autentiškumo nustatymo metodo priimto sprendimo teisingumu.

3.5. Siūlomo metodo privalumai

Pirmas privalumas yra vaizdo skaitmeninio parašo struktūros naudojimas. Kaip buvo parodyta pirmame skyriuje, yra situacijų, kada originalų atvaizdą reikia išlaikyti nepakeistą – medicinos, karinėse ir panašiose srityse. Priešingai nei vandens ženklai, vaizdo skaitmeninis parašas neįrašo į apsaugomą atvaizdą jokių papildomų dirbtinių struktūrų. Papildomas privalumas – atsparumas steganalizės atakoms.

Galimybė galutiniam vartotojui, paprastam žmogui, pačiam pasitikrinti atvaizdo autentiškumą paprastu, intuityviu būdu, nesileidžiant į matematines formules ir skaičiavimus, taip pat yra aiškus privalumas. Tuo labiau, kad visi matematiniai skaičiavimai išlieka laisvai prieinami tolesniam naudojimui.

Autentiškumo ir pažeidimų lokalizavimo atskyrimas algoritmo lygmenyje leidžia autentiškumo nustatymą padaryti pigesniu ir greitesniu, nes nebūtina ieškoti pažeidimų jei autentiškumas yra patvirtinamas 100%. Toks atskyrimas taip pat leidžia blokuoti orakulo ataką.

Metodo, vienu metu pasižyminčio atsparumu autentiškumo nustatyme ir pusiau jautrumu pažeidimų lokalizavime, kūrimas, pasižymi ypatingu sudėtingumu, nes reikia tarpusavyje suderinti du vienas kitam prieštaraujančius mechanizmus. Siūlomas sprendimas sėkmingai derina savyje geriausias atsparumo ir pusiau jautrumo charakteristikas.

Invariantiškumas bendrosioms vaizdo apdorojimo procedūroms – vaizdo blukinimui, ryškinimui, pasukimui ir suspaudimui – tiek autentiškumo nustatyme, tiek pažeidimų lokalizavime, yra dar viena siūlomo sprendimo naujovė. Bendro pobūdžio atvaizdo apdorojimas, siekiant pakelti jo vertę nekeičiant atvaizdo pateikiamos informacijos esmės, yra gana dažnas mūsų šiuolaikiniame skaitmeniniame pasaulyje. Natūralu, kad vaizdų autentiškumo nustatymo ir pažeidimų lokalizavimo metodai turi prisitaikyti prie realaus pasaulio reikalavimų, neturi tokių atvaizdo pakeitimų traktuoti kaip įtartinų ir neleistinų.

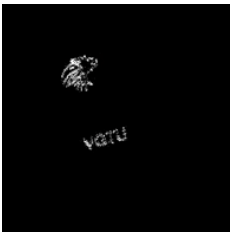
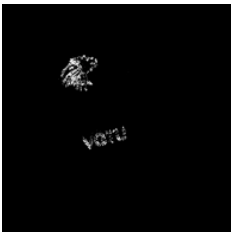
Atsparumas piktybiniams pažeidimams, autentiškumo nustatymo ir pažeidimų lokalizavimo procedūrose, yra skirtingo jautrumo lygio. Pažeidimų lokalizavimas yra pusiau jautrus – atsparus tik apibrėžtai aibei bendrųjų vaizdo apdorojimo procedūrų. Autentiškumo nustatymas, iš kitos pusės, yra modeliuotas taip, kad atvaizdas būtų traktuojamas kaip autentiškas tol, kol atvaizdo esmė išlieka mažai pakeista. Bet kokie atvaizdo skaitmeninės matricos pakeitimai, ar jie būtų lokalūs, ar globalūs, neįtakoja metodo tol, kol išlaikomas atvaizdo autentiškumas.

Pusiau jautrus pažeidimų lokalizavimas, iki paskirų pikselių lygmens, atsparus atvaizdo blukinimui ar aštrinimui, yra siūlomo metodo naujiena ir neginčijamas privalumas.

4. Skaitiniai eksperimentai

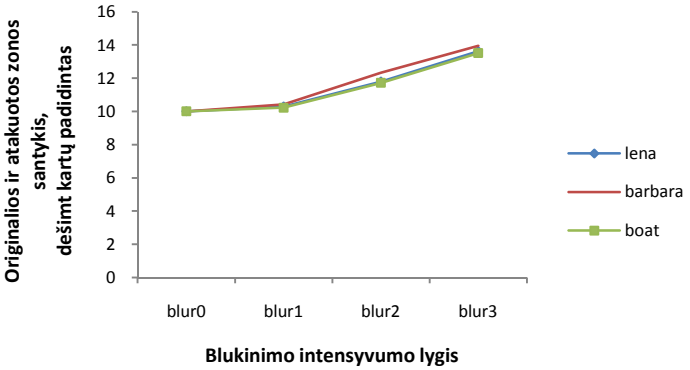
Siekiant patikrinti siūlomo metodo efektyvumą buvo atlikta daug skaitinių eksperimentų, tiek su įvairiais atvaizdais, tiek su įvairiomis atakomis bei jų variacijomis. Įdomesni arba išskirtiniai rezultatai yra parodomi antroje lentelėje.

2 lentelė. Skaitinių eksperimentų rezultatai

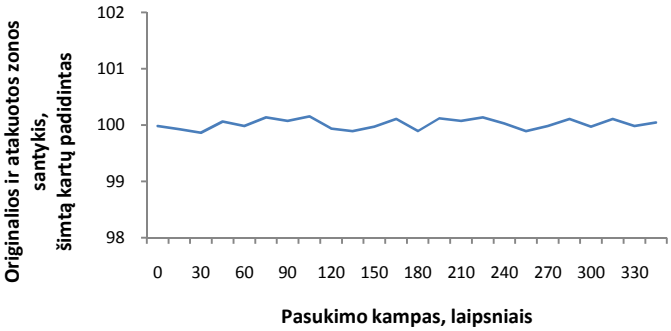
 Tekstas - VGTU	 Tekstas ir varna pridėti, tada atvaizdas globaliai blukinamas	 Tekstas ir varna pridėti, tada atvaizdas globaliai ryškinamas
 Rastos pažeistos vietos	 Rastos pažeistos vietos	 Rastos pažeistos vietos

Matome, kad nepaisant blukinimo ar ryškinimo, pažeidimų radimo metodas sėkmingai nustato pažeistus pikselius.

Pažeidimų aptikimo priklausomybė nuo blukinimo intensyvumo ir pasukimo kampo parodoma atitinkamai pirmame ir antrame paveiksle.



1 pav. Pažeistų zonų radimo efektyvumas priklausomai nuo blukinimo



2 pav. Pažeistų zonų radimo efektyvumas priklausomai nuo pasukimo kampo

Pirmame paveiksle matome, kad metodas stabiliai veikia su skirtingais blukinimo lygiais. Šie rezultatai skiriasi nuo kitų pikselių tikslumo metodų, kur bet koks blukinimas ar ryškinimas sukelia Gauso triukšmo efektą, paslepiantį sąmoningai pakeistus pikselius bendrame triukšme. Blokiniai metodai, kurie yra

atsparesni blukinimui ar ryškinimui, nėra pajėgūs suteikti paskirų pažeistų pikselių suradimo galimybės.

Antrame paveiksle matome, kad metodo veikimas nepriklauso nuo atvaizdo pasukimo kampo.

Bendrosios išvados

1. Disertacijoje analizuota atsparaus autentiškumo apjungto su pusiau jautriu pažeistų pikselių lokalizavimu problema. Pasiūlytas naujas metodas, pasižymintis invariantiškumu atvaizdo turinį išsaugančioms modifikacijoms – blukinimui, aštrinimui, JPEG suspaudimui ir pasukimui – ir išlaikantis galimybę surasti pakeistus pikselius.
2. Sukurta modifikuotos fazės transformacija. Ji remiasi Furje transformacijos faze ir garantuoja invariantiškumą blukinimui ar aštrinimui, sukurdama griežtą pikselių sąsają su pradinio atvaizdo pikseliais.
3. Sukurta duomenų neprarandanti atvaizdo transformacija į polines koordinates. Transformacija garantuoja invariantiškumą pasukimui. Garantuojamas paklaidos nebuvimas diskrečiuoju atveju (lyginant su interpoliavimo paklaida klasikiniu atveju).
4. Sukurtas metodas pusiau jautriam paskirų pažeistų pikselių suradimui. Metodas remiasi modifikuotos fazės transformacija ir duomenų neprarandančia diskretine konversija į polines koordinates – tai suteikia reikiamą atsparumą prieš bendrąsias vaizdo apdorojimo procedūras – atvaizdo blukinimą, ryškinimą, JPEG suspaudimą ir pasukimą – ir išlaiko pažeidimų lokalizavimą iki paskirų pikselių skiriamosios gebos visoms kitoms modifikacijoms, įskaitant ir objektų pridėjimą ar ištrynimą.
5. Sukurtas atsparus atvaizdo autentiškumo nustatymo metodas, pasižymintis galimybe įvertinti atvaizdą tiek binarine, tiek procentine reikšme ir papildoma nauja savybe – pasirinktiniu vartotojo nuomonės įvertinimu.
6. Sukurtas vaizdo skaitmeninio parašo metodas, integruojantis tiek atsparų atvaizdo autentiškumo nustatymą, tiek pusiau jautrų pažeistų pikselių lokalizavimą. Priešingai vandens ženklams, sukurtas metodas apsaugo visus pikselio bitus.
7. Autentiškumo nustatymo ir pažeidimų suradimo mechanizmai atskirti tam, kad būtų išvengta algoritmo atakų, tokių kaip orakulo ataka. Įrodyta, kad tokio atskyrimo pakanka, kad sustabdyti ataką, kai

pažeidimų lokalizavimo mechanizmas naudojamas atakai prieš patį atvaizdą.

8. Skaitmeninio vaizdo parašo mechanizmo naudojimas įgalina išvengti steganalizės atakų, leidžia lengvai atlikti programinės įrangos atnaujinimus bei išplėtimus (lyginant su vandens ženklinimo mechanizmu).
9. Nustatyta, kad galutinio parašo dydis neviršija 10% originalaus atvaizdo dydžio. Tačiau ir su tokiu mažu duomenų kiekiu, metodas pajėgus užtikrinti 100% atvaizdo bitų apsaugą.

Autoriaus publikacijų disertacijos tema sąrašas
Recenzuojamuose mokslo žurnaluose

Baušys, R.; Kriukovas, A. 2008. Digital Signature Approach for Image Authentication, *Elektronika ir elektrotechnika* 6(86): 65–68. (ISI Web of Science)

Baušys, R.; Kriukovas, A. 2008. A new scheme for image authentication framework, *Information Technology and Control* 37(4): 294–300. (ISI Web of Science)

Baušys, R.; Kriukovas, A. 2009. Blur Resistant Image Authentication Method with Pixel-wise Tamper Localization, *Elektronika ir elektrotechnika* 3(91): 35–38. (ISI Web of Science)

Straipsniai kituose leidiniuose

Baušys, R.; Kriukovas, A. 2006. Reversible watermarking scheme for image authentication in frequency domain, *48th International Symposium ELMAR focused on Multimedia Signal Processing and Communications*: 53–56.

Trumpos žinios apie autorių

Artūras Kriukovas gimė Vilniuje, 1981 m. lapkričio 17 d. 2004 m. įgijo informatikos inžinerijos bakalauro laipsnį Vilniaus Gedimino technikos universiteto (VGTU) Fundamentinių mokslų fakultete. 2006 m. įgijo informatikos inžinerijos mokslo magistro laipsnį VGTU. Turi darbo patirties kaip sistemų administratorius. 2006–2010 m. – VGTU doktorantas. Dabar – lektorius Grafinių sistemų katedroje, Fundamentinių mokslų fakultete, VGTU.

DIGITAL SIGNATURE TECHNOLOGIES FOR IMAGE INFORMATION ASSURANCE

Topicality of the problem. In the past decades, the technological evolution of international communication networks has facilitated efficient digital image exchanges. The availability of versatile digital image processing tools has made image manipulations trivial and discernable for the human visual system. Therefore image authentication and integrity verification problems are becoming of superior importance. Medical data, news reports or political events are just some examples where "seeing is believing" and false information is unacceptable.

Methods for conventional data authentication – digital signatures based on asymmetrical cryptography, cryptography hashes like MD5 – can be directly applied to multimedia data. But there is one subtle difference between multimedia data and standard digital data – documents, executables, archives – conventional cryptography methods are usually applied to. Unlike other digital data, multimedia data contains high redundancy and irrelevancy. Some signal processing, like compression or quality enhancement via sharpening or blurring, is likely or even required to be applied to multimedia signals without affecting the authenticity of the data. Conventional authentication algorithms will reject such signal modifications as the signal has been modified and manipulated. In fact, conventional algorithms can only authenticate the binary representation of digital multimedia data instead of its perceptual content. However, in digital multimedia authentication it is desirable that the perceptual content is authenticated despite modifications to the binary representation.

Furthermore, authentication is not always enough – tamper localization procedures enable location and identification of trusted and not-trusted regions. This knowledge can be used to determine if the semantic meaning of the content has been preserved, to determine what changes were introduced. It is important to have pixel-wise tamper localization ability, as block-wise methods with a large block size do not allow for exact tamper analysis – it is not possible to say whether 1 pixel in the block of 100x100 pixels was changed accidentally – or all 9'999 pixels intentionally.

In recent years new technologies appeared – watermarking and digital signatures – for multimedia authentication and tamper localization. Various methods how to ensure image security were proposed. Most of them focused on fragile image authentication and tamper localization, i.e. when objective of the method is to locate any change of the image in question. Noticeable less are of methods presenting semi-fragile protection – robust to some common image processing operations, like rotation or compression and fragile to other

manipulations. There are even some general and everyday image processing operations, like blurring or sharpening, that no methods present robustness to. We try to fill this gap.

In this thesis we analyze methods for image authentication and pixel-wise tamper localization, robust to some limited set of general image processing operations (blurring, sharpening, compression and rotation) and fragile to all other modifications. A new transformation robust to blur/sharpen operations is developed. A lossless discrete log-polar conversion is developed to ensure robustness against rotation. A digital signature method for robust image authentication and semi-fragile tamper localization based on the developed transformations is proposed. We especially focus our attention on effectiveness of pixel-wise localization in spite of blurring and sharpening, as these simple and very common image processing operations have extensive effect on all pixels in the image and thus present serious challenges for pixel-wise oriented methods.

The object of the research. The objective of the thesis is image authentication and tamper localization after general image processing operations.

Main objective and tasks of the work. The main goal of the thesis is creation of a method that combines robust image authentication and semi-fragile (with the respect to: blurring, sharpening, rotation, compression, i.e. image processing operations that does not change the essence of the image) pixel-wise tamper localization. The following problems had to be solved:

1. To develop a method, invariant to blurring, sharpening, rotation and compression, but fragile to all other modifications. The method developed has to retain 1:1 spatial reference in order to present pixel-wise tamper localization.
2. To present an algorithm for semi-fragile pixel-wise tamper localization, based on the method developed. Semi-fragility is defined against blurring, sharpening, rotation and compression.
3. To present an algorithm for robust image authentication, independent of tamper localization algorithm.
4. To introduce digital signature based method, consolidating proposed methods on robust image authentication and semi-fragile tamper localization. The method has to possess the following characteristics:
    a) image authentication has to be robust for all general image processing operations, especially for: blurring, sharpening, compression and rotation;

b) image authentication must refrain from concluding a binary answer trusted/not trusted. A percentage measure of trustiness must be evaluated; if needed, it can be later converted to binary answer;
c) tamper localization has to be pixel-wise;
d) tamper localization has to be robust for: blurring, sharpening, compression and rotation. All other modifications are considered to be malicious; tamper localization algorithm should detect them;
e) tamper localization has to be independent from authentication establishment in order to prevent oracle-type attacks;
f) the method has to be digital signature based, to be indistinguishable for steganalysis methods.

Research methodology. To achieve the objective, the following research methods were used:

1. Comparative research and literature research methods were used.
2. The analysis results were summarized and the approach was expanded using the research generalization and logical induction methods.
3. The experimental research methods were applied while performing analysis of the proposed method.

Importance of the scientific novelty. The thesis addresses a problem of establishing image authentication and performing tamper localization with resolution up to one pixel, semi-invariant to general image processing operations, such as blurring, sharpening, rotation and compression. The following new results were obtained:

1. A new transformation, called MPOF (modified phase only filter), was developed. The transformation takes advantage of phase of Fourier transform invariance against blurring/sharpening and introduces strict relation between pixels in spatial domain and Fourier phase.
2. A new transformation for lossless discrete log-polar conversion was developed. Contrary to other methods, conversion to log-polar and back to Cartesian coordinates does not require interpolation and does not introduce data loss. This allows having pixel-wise tamper localization robust to rotation.
3. An algorithm for pixel-wise tamper localization, semi-fragile to common image processing operations, was developed. The algorithm is based on newly developed transforms and ensures robustness against

blurring, sharpening, rotation and compression at the same time remaining sensitive to any other manipulations.

4. A digital signature based method for robust image authentication with semi-fragile tamper localization was developed. The architecture of the method allows for optional human opinion integration in image authenticity establishment process; ensures mathematically simple authenticity establishment process; ensures protection against algorithmic oracle attack; ensures protection against steganalysis; ensures "no change" on original image; ensures authentication and tamper localization before or after common image processing operations, such as blurring, sharpening, rotation or compression; ensures limited signature size; ensures pixel-wise localization of malicious modifications.

Practical significance of the achieved results. Practical application is in image security where robustness to general image processing is required and, at the same time, the method should exhibit sensitivity to malicious manipulations.

The defended statements. The following defendable statements are defined:

1. Digital signature protects all bits in the image.
2. Separation of authentication algorithm from tamper localization algorithm ensures robustness against oracle attack.
3. Solution of how modified phase of Fourier transformation can be used to locate tampered pixels in spatial domain.

The scope of the scientific work. The dissertation is composed of Introduction, four main chapters and general conclusions. The total dissertation scope is 119 pages, 8 pictures and 11 tables.

In Introduction topicality of the problem is analyzed, work main objective and tasks are formulated, scientific novelty is proved, research methods used are listed and defended statements are presented.

Chapter 1 reviews types of image authentication systems – fragile, semi-fragile and robust, and mechanisms – watermark and digital signature. Common misconceptions are clarified, as digital signature for images is not the same as digital signature in asymmetrical cryptography. Special attention is given for simple image processing operations – blur/sharpen influence on images. As it is shown in Table 1, original image and blurred versions of it look almost identical – but their pixel matrixes are completely different – value 39 becomes

0, value 121 becomes 255 and etc. These are enormous changes in complete range between black (value 0) and white (value 255). This devastating effect is the reason why most pixel-based tamper localization algorithms fail to detect attacks after blurring or sharpening – the whole picture appears to be tampered with, after only a single innocent image quality enhancement operation. Detailed review of current image security methods follows, illustrating that no pixel-wise methods, robust for image blurring or sharpening, exist. Even for some block-based algorithms general blurring or sharpening present problems. Finally, comparison of digital signature and watermark mechanisms is performed, arguing for our decision to use a digital signature scheme.

Chapter 2 presents theoretical foundation for the proposed method. It is shown that the usage of the framework of the new JPEG-2000 compression method provides no advantage against damage from blurring or sharpening. Some other solutions had to be found and it was noticed and proved that Fourier phase has invariance against blurring and sharpening. The phase has another disadvantage – no correlation between pixels in spatial domain and in Fourier phase domain, i.e. it is not possible to perform pixel-wise tamper localization. This problem is solved in the next Chapter. Important aspects of Oracle attack, Structured-Similarity Index, log-polar conversion and discrete version of it, compression methods – that had influence on final method are also shown.

Chapter 3 presents the details of the proposed method. Two new transformations are defined. MPOF is for enforcing strict unique relation between each pixel in spatial domain and pixel in Fourier phase domain. Then discrete conversion to polar coordinates is defined in order to provide robustness against rotation. Compression method is also presented that enables to have size of the final signature less than 10% of the original image. It should be noticed that these 10% are enough to detect a change in each bit of each pixel of the original image independent of blurring, sharpening or rotation applied. Algorithm of the final method – authentication establishment, tamper localization – is also presented here. Comparison with other methods was performed although it was not possible to perform a direct comparison as no direct competitors for the method are known. Therefore specific functions of the proposed method are compared with other methods, where it is applicable.

Numerical experiments are presented in Chapter 4. Table 2 presents tamper localization results (attacked, attacked + blurred, attacked + sharpened and corresponding tamper localization maps). Figures 1 and 2 illustrate dependency on blur intensity and rotation angle.

General conclusions as well as recommendations for further research summarizes the present study. It is followed by an extensive list of 150

references and a list of 4 publications by the author on the topic of the dissertation.

General conclusions

In this thesis a novel method for determining image authentication and performing tamper localization with the respect to allowed image processing operations was developed. The following conclusions can be made:

1. The problem of robust authentication with semi-fragile pixel-wise tamper localization has been addressed. A new method for the solution of the problem is proposed. The method is invariant to content-preserving image modifications – blurring, sharpening, JPEG compression, rotation – and presents pixel-wise sensitivity to content-changing modifications.
2. A new modified phase only filter transformation is proposed. The transformation is loosely based on the phase of Fourier transform and ensures invariance to blur/sharpen image processing operations while retaining spatial reference information.
3. A new lossless log-polar conversion is proposed. The transformation enables invariance against rotation. The conversion is completely lossless, on the contrary to classical log-polar conversion where interpolation inevitably introduces interpolation errors in the conversion process.
4. A new method for semi-fragile pixel-wise tamper localization is proposed. The method is based on the new modified phase only filter transformation and the new lossless log-polar conversion. This gives the required robustness against general image processing operations – blurring, sharpening, JPEG compression and rotation – and retains pixel-wise fragility to other processing – like object addition or removal – intact, resulting in semi-fragility against general image processing.
5. A robust image authentication method is developed. The method features both binary and percentage measures for authenticity establishment as well as novel feature – optional human opinion integration.
6. A complete digital signature based method is developed. The method integrates both robust authentication and semi-fragile pixel-wise tamper localization. Also, the method provides protection for all bits of the pixel, contrary to most pixel-wise watermarking methods.

7. Separate image authentication and tamper localization mechanisms are specifically enforced in order to prevent general algorithmic attacks, such as oracle attack. It is proved that such separation is required to stop an attack were authenticator itself can be used to attack the protected image.
8. Digital signature approach is introduced in order to rupture attacks based on steganalysis as contrary to watermarking approach nothing is embedded into the protected picture. Additional advantage of future upgrades is gained – no image re-watermarking is required.
9. Performance gains were also addressed in the proposed method. Final size of the signature is less than 10% of initial image; tamper localization procedures are not executed if authentication process confirms 100% authenticity; only simple and effective mathematical operations are used.

About the author

Artūras Kriukovas was born in Vilnius, on 17 of November 1981. First degree in Informatics Engineering, from Faculty of Fundamental Sciences, Vilnius Gediminas Technical University (VGTU), 2004. Master of Science in Informatics Engineering, from Faculty of Fundamental Sciences, VGTU, 2006. Has a job experience as a system administrator, teacher. In 2006–2010 – PhD student of VGTU. At present – lecturer at Department of Graphical Systems, Faculty of Fundamental Sciences of Vilnius Gediminas Technical University.