Sveučilište u Zagrebu

Fakultet organizacije i informatike

Bernard Vukelić

NOVI ALGORITAM ZA IZRADU PERCEPCIJSKIH SAŽETAKA TEMELJEN NA IZDVAJANJU ATRIBUTA BIOMETRIJSKIH KARAKTERISTIKA

DOKTORSKI RAD

Varaždin, 2018.

PODACI O DOKTORSKOM RADU

I. AUTOR

Ime i prezime	Bernard Vukelić
Datum i mjesto rođenja	25.3.1978., Rijeka
Naziv fakulteta i datum diplomiranja na VII/I stupnju	Ekonomski fakultet u Rijeci
Naziv fakulteta i datum diplomiranja na VII/II stupnju	Fakultet organizacije i informatike u Varaždinu
Sadašnje zaposlenje	Veleučilište u Rijeci

II. DOKTORSKI RAD

Naslov	**Novi algoritam za izradu percepcijskih sažetaka temeljen na izdvajanju atributa biometrijskih karakteristika**
Broj stranica, slika, tablica, priloga, bibliografskih podataka	140 stranica, 65 slika, 24 grafikona, 15 tablica, 3 koda, 144 bibliografskih podataka
Znanstveno područje i polje iz kojeg je postignut doktorat znanosti	Društvene znanosti, Informacijske i komunikacijske znanosti
Mentori ili voditelji rada	Prof. dr. sc. Miroslav Bača
Fakultet na kojem je obranjen doktorski rad	Fakultet organizacije i informatike
Oznaka i redni broj rada	141

III. OCJENA I OBRANA

Datum sjednice Fakultetskog vijeća na kojoj je prihvaćena tema	26. travnja 2016.
Datum predaje rada	4. travnja 2017.
Datum sjednice Fakultetskog vijeća na kojoj je prihvaćena pozitivna ocjena rada	15. svibnja 2018.
Sastav povjerenstva koje je rad ocijenilo	Prof. dr. sc. Mirko Maleković, predsjednik Prof. dr. sc. Alen Lovrenčić, član Doc. dr. sc. Mate Boban, član
Datum obrane doktorskog rada	21. lipnja 2018.
Sastav povjerenstva pred kojim je rad obranjen	Prof. dr. sc. Mirko Maleković, predsjednik Prof. dr. sc. Alen Lovrenčić, član Doc. dr. sc. Mate Boban, član
Datum promocije	

Sveučilište u Zagrebu

Fakultet organizacije i informatike

BERNARD VUKELIĆ

NOVI ALGORITAM ZA IZRADU PERCEPCIJSKIH SAŽETAKA TEMELJEN NA IZDVAJANJU ATRIBUTA BIOMETRIJSKIH KARAKTERISTIKA

DOKTORSKI RAD

Mentor:
Prof. dr. sc. Miroslav Bača

Varaždin, 2018.

University of Zagreb

Faculty of Organization and Informatics

Bernard Vukelić

A NOVEL ALGORITHM FOR THE DEVELOPMENT OF PERCEPTUAL HASHES BASED ON EXTRACTION OF ATTRIBUTES OF BIOMETRIC CHARACTERISTICS

DOCTORAL THESIS

Varaždin, 2018

PODACI O MENTORU

Prof. dr. sc. Miroslav Bača

Redoviti je profesor na Fakultetu organizacije i informatike Sveučilišta u Zagrebu. Voditelj je Centra za forenziku, biometriju i privatnost pri Fakultetu organizacije i informatike. Stalni je sudski vještak za informatiku, telekomunikacije i biometriju te ekspert za privatnost informatičkih proizvoda i usluga. Autor je preko stotinu znanstvenih i stručnih radova, autor i suator nekoliko knjiga te voditelj i istraživač u nekoliko znanstvenih i stručnih projekta.

Jedini je znanstvenik i praktičar u RH koji je kao jedan od svojih fokusa istraživanja proučava računalnu forenziku, a svojim radom promovira znanstveni i stručni napredak i van granica RH. Član je nekoliko znanstvenih i stručnih programskih odbora te strukovnih organizacija.

Zahvala

Zahvaljujem mentoru prof. dr. sc. Miroslavu Bači na susretljivosti, savjetima, strpljenju i energiji koju je prenosio na mene tijekom izrade ovog rada.

Mojim roditeljima Ivanu i Bojani zahvaljujem na podršci da ustrajem u svojem cilju.

Posljednje ali i najveće zahvale, i posveta rada u cijelosti, idu mojoj dragoj supruzi Uni i sinčiću Vidu. Supruzi zahvala na potpori i strpljenju, ohrabrenju, razumijevanju te bezuvjetnoj podršci koju mi je davala tijekom studija i pisanja ovog rada, a sinu Vidu, iako je trenutačno "mali", na davanju snage i motivacije za pisanje ovog rada.

Sažetak

S napretkom računalnih i mrežnih tehnologija, količina digitalnih slika koje se prenose ili pregledavaju putem digitalnih uređaja eksponencijalno raste, a u porastu je neovlaštena uporaba kao i krivotvorenje istih. Ovaj doktorski rad bavi se percepcijskim sažetcima koji su „otisak" digitalne slike izveden iz različitih atributa njezina sadržaja, a upotrebljavaju se za provjeru autentičnosti ili identifikaciju digitalnih slika. Postoji mnogo područja njihove primjene: zaštita autorskih prava, računalna forenzika ili pretraživanje baza slika. Njihove su prednosti mala veličina, brzo pretraživanje i slanje putem mreže te robusnost na manipulacije i modifikacije. U disertaciji je razvijen novi algoritam za izradu percepcijskih sažetaka, koji izdvaja i analizira, koristeći se metodom modificirane census transformacije, lokalne atribute interesnih regija slika odnosno biometrijskih uzoraka, a u svrhu ispitivanja mogućnosti njegove upotrebe u biometriji. Napravljena je usporedba s drugim najčešće korištenim algoritmima te se utvrđuje hoće li novorazvijeni algoritam biti točniji i robusniji u području biometrijske autentikacije.

Ključne riječi: percepcijski sažetak, atributi digitalne slike, modificirana cenzus transformacija, biometrija

Abstract

With the advancement of computer and network technologies, the amount of digital images which are transferred or browsed through digital devices increases exponentially. However, unauthorized use and counterfeiting of the same also increases. This doctoral thesis deals with the perceptual hashes which are a "print" of a digital image derived from various attributes of its contents, and which are used for authentication or identification of digital images. There are many areas of their application: protection of copyrights, computer forensics or searching image databases. Perceptual hashes have several advantages, such as a small size, fast searching and sending via the network as well as the robusness to manipulation and modification. In this thesis, an algorithm for making perceptual hashes which extract and analyze attributes of region of interest in an image for the possibility of their use in biometrics using methods of modified census transformation has been developed. A comparison has been made with other commonly used algorithms and an improved robusness and precision of the newly developed algorithm for the purpose of biometric authentication will be determined.

Keywords: perceptual hash, digital image features, modified census transformation, biometrics

SADRŽAJ

POPIS SLIKA

POPIS GRAFIKONA

POPIS TABLICA

POPIS KODOVA

1. UVOD

1.1. Opis problema istraživanja

Tijekom rada s digitalnim slikama može doći do njihovih promjena, a koje mogu nastati slučajno ili biti namjerno napravljene pri čemu se narušava njihov integritet. Sposobnost otkrivanja manipulacija i modifikacija nad digitalnim slikama vrlo je važna, osobito za novinske fotografije, medicinske slike ili umjetnička djela. To je potaknulo interes za istraživanje i razvoj različitih metoda i algoritama koji bi omogućavali provjeru autentičnosti i integriteta digitalnih slika. Iako je dosad razvijen velik broj takvih metoda i algoritama, najviše se upotrebljavaju vodeni žigovi ili kriptografija. Prema Wojtowiczu i Oigeli (Wojtowicz i Oigela, 2012.) vodeni žigovi, čija je namjena zaštita autorskog vlasništva, neovlaštenog kopiranja ili mijenjanja sadržaja, nisu robusni na modifikacije kao što je kompresija ili promjena formata te su podložni različitim načinima prijevare. Kriptografija je znanost koja se bavi logičkom promjenom podataka (šifriranjem), odnosno proučavanjem metoda za slanje poruka u takvom obliku da ih samo osoba kojoj su namijenjene može pročitati te najveću upotrebu upravo bilježe u komunikaciji preko nesigurnog komunikacijskog kanala (telefonska linija, računalna mreža,...) (Wojtowicz i Oigela, 2012.). Kriptografija u zaštiti digitalnih slika koristi se kriptografskim sažetcima (engl. *hash*). Funkcija sažetka jest funkcija za sažimanje i identificiranje podataka. Izvođenje funkcije naziva se *hashing*, a njime se dobije *hash* vrijednost, odnosno sažetak (Weng et al., 2012.). Funkcija sažetka jest transformacija koja od ulaza varijabilne veličine vraća znakovni niz fiksne dužine. Najčešću primjenu takvih funkcija moguće je pronaći pri provjeri autentičnosti datoteka upotrebom nekih od kriptografskih algoritama kao što je MD5 ili SHA-1. Ograničenje pri upotrebi takvih kriptografskih sažetaka jest nemogućnost utvrđivanja djelomične autentičnosti te vizualne sličnosti kod digitalnih slika jer se integritet datoteka utvrđuje usporedbom svih bitova sažetka, koji moraju biti apsolutno jednaki da bi se potvrdila potpuna autentičnost datoteke (Menezes et. Al., 1996.). Provjera integriteta metodom *bit-po-bit* nije prikladna za digitalne slike jer su one često podložne manipulacijama koje vizualno ne utječu na sličnost kao što je na primjer promjena svjetline ili kompresija, a bile bi označene kao neautentične. Vizualno slične slike bi u tom slučaju imale različite atribute.

Jedno od mogućih rješenja jest upotreba percepcijskih sažetaka (engl. *perceptual hash*).

Funkcijom percepcijskog sažetka izdvajaju se i sažimaju samo odabrani atributi digitalne slike kojima se može opisati, interpretirati ili razumjeti njezin sadržaj te se s pomoću njih izračunava vrijednost percepcijskog sažetka slike. Slične digitalne slike imaju slične vrijednosti percepcijskih sažetaka i obrnuto – sličnim percepcijskim sažecima odgovaraju slične digitalne slike. Usporedbom percepcijskih sažetka digitalnih slika može se utvrditi jesu li one slične te u kojoj mjeri. Koncept percepcijskog sažetka prvi su 1996. godine predstavili Schneider i Chang (Schneider i Chang, 1996.) i otad je razvijen velik broj algoritama za izradu i usporedbu percepcijskih sažetaka.

Iako postoji postoji mnogo mogućih područja primjene, pregledom literature primijećeno je da se mali broj radova bavi problemom primjene percepcijskih sažetaka u nekim specifičnim područjima.

Jedno od takvih mogućih područja primjene percepcijskih sažetaka je i biometrija odnosno biometrijska autentikacija. Biometriju se u užem smislu promatra kao istraživanje mogućnosti prepoznavanja osoba na temelju njihovih fizičkih i ponašajnih karakteristika. Biometrijski sustav autentikacije je u suštini sustav prepoznavanja korisnika na temelju usporedbe digitaliziranih atributa slika odnosno uzoraka biometrijskih karakteristika prikupljenih sa senzora s već pohranjenim predloškom u bazi. Ako prikupljeni uzorak i pohranjeni predložak imaju visok stupanj sličnosti, korisnik je prihvaćen kao autentičan (engl. *genuine*). U suprotnom, tvrdnja je odbačena i korisnik je označen kao varalica (engl. *impostor*).

Kako je u pregledu literature primjećeno (Zauner, 2010., Hadmi et. al., 2012., Kozat et al., 2004., Weng et al., 2012.), algoritmi za izradu percepcijskih sažetaka pokazuju sličnost s algoritmima koji se upotrebljavaju u biometrijskoj autentikaciji. I jednim i drugim algoritmima moguće je utvrditi sličnost digitalnih slika usporedbom njihovih atributa.

Glavni fokus istraživanja u ovoj disertaciji je mogućnost primjene percepcijskih sažetaka u biometrijskim sustavima autentikacije. U jednom tipičnom scenariju, autentikacija korisnika u biometrijskim sustavima mogla bi se utvrditi usporedbom percepcijskih sažetaka koji su dobiveni izdvajanjem i analizom atributa digitalne slike odnosno biometrijskog predloška pohranjenog u bazi i biometrijskog uzorka sa senzora kad se korisnik prijavljuje u sustav. Što je veće podudaranje, veći je i rezultat podudaranja (engl. *match score*). Ako rezultat prijeđe prag (engl. *treshold*), odnosno postavljenu numeričku vrijednost podudaranja sa predloškom, osoba je označena kao autentična. Određivanje praga ovisi o samoj primjeni sustava, ali općenito biometrijski sustavi autentikacije zahtjevaju veće podudaranje radi postizanja veće sigurnosti u prepoznavanju korisnika.

Percepcijski sažetci, da bi bili upotrebljivi u takvim sustavima, trebali bi pokazati dvije osobine – robusnost na manipulacije koje uzrokuju promjene na slici koje bi onemogućile diskriminaciju kod njihove usporedbe te osjetljivost na napade modifikacijom kojima će se promijeniti sadržaj slike odnosno bitno narušiti integritet. Primjenom manipulacija trebali bi biti sposobni prepoznati slične slike, a primjenom modifikacija trebali bi moći uočiti promjene. Isto tako, morali bi točno moći razlikovati dvije potpuno različite slike odnosno omogućiti diskriminaciju. Uspješna diskriminacija korištenjem percepcijskih sažetaka bila bi korisna i u biometrijskim sustavima identifikacije kada se treba utvrditi nalazi li se korisnik u bazi ili ne, ali time se ova disertacija neće baviti. U literaturi, operacije manipulacijom i modifikacijom nazivaju se "napadima" te će se tim terminom koristiti i dalje u disertaciji. (Zauner, 2010., Hadmi et. al., 2012., Kozat et al., 2004., Weng et al., 2012.)

Da bi ispitali robusnost i točnost, u disertaciji će se napraviti vrednovanje algoritama za percepcijske sažetke, koji su u literaturi isticani kao standardni (engl. *state of art*), analizom atributa slika biometrijskih karakteristika lica, uha i potpisa. Pri vrednovanju algoritama upotrijebljeni su po grupama podijeljeni negeometrijski, geometrijski i zlonamjerni napadi manipulacijom i modifikacijom koji se najčešće javljaju i kao problem u biometrijskim sustavima prilikom autentikacije korisnika. Tako podijeljeni napadi trebali bi u vrednovanju testirati algoritme sa tri aspekta. Prvi aspekt je robusnost na negeometrijske napade. Negeometrijski napadi kao što je promijena svjetline ili kompresija ne bi trebali bitno utjecati na sličnost percepcijskih sažetaka s obzirom da se sadržaj slike ili struktura bitno ne mijenja. Drugi aspekt je robusnost na geometrijske napade. Geometrijski napadi su zanimljivi jer se rotacijom ili translacijom, napadnuta slika ljudskom oku vizualno ne mijenja iako je njezina

digitalna prezentacija promijenjena, a dosta su česti u biometrijskim sustavima. Treći aspekt su zlonamjerni napadi kao što je namjerno brisanje ili dodavanje manjih i većih dijelova slike. Takve napade, algoritmi bi trebali uspješno otkriti da bi bili upotrebljivi u autentikaciji.

Treba se napomenuti i to da se velik broj autora u svojim radovima bavio vrednovanjem algoritama primjenom nekih od spomenutih napada (Zauner, 2010., Prungsinchai, 2014., Hadmi et. al., 2012.) ali ne na setovima biometrijskih digitalnih slika. Njihova istraživanja pokazala su da vrednovani algoritmi nisu dovoljno robusni na sve napade te su radi toga pogodniji za identifikaciju odnosno u situacijama kada je potrebno istražiti nalazi li se analizirana digitalna slika u bazi ili ne. Ističe se da prilikom identifikacije nije potrebna velika točnost te se može tolerirati određeni broj lažno pozitivnih rezultata. S obzirom da većina tih vrednovanih algoritama analizira globalne atribute slika, u disertaciji se predlaže novi pristup izrade percepcijskih sažetaka temeljen na izdvajanju lokalnih atributa interesnih regija na slikama biometrijskih karakteristika i njihovom analizom metodom modificirane cenzus transformacije. Metodom modificirane cenzus transformacije uspoređuje se intenzitet svakog pojedinog piksela odabrane regije slike s prosječnom vrijednošću intenziteta te regije. Na temelju usporedbe je li intenzitet pojedinog piksela veći od prosječnog intenziteta ili nije, generira se percepcijski sažetak odabrane regije. Takav novorazvijeni algoritam trebao bi pokazati prednosti u odnosu na ostale u vrednovanju korištene algoritme zato što bi lokalni atributi trebali biti osjetljiviji na promjene odnosno spomenute napade te bi time algoritam trebao biti prikladniji za upotrebu u biometrijskim sustavima autentikacije gdje je potrebnija veća točnost prepoznavanja korisnika radi veće sigurnosti.

1.2. Motivacija za istraživanje

S brzim napretkom računala, multimedijskih i mrežnih tehnologija, količina multimedijalnih podataka koji se prenose, emitiraju ili pregledavaju putem digitalnih uređaja eksponencijalno raste. Istodobno, u porastu su i neovlaštena upotreba i krivotvorenje digitalnih podataka, stoga je zaštita takvih sadržaja sve zahtjevnija. Posljednih nekoliko godina primijećen je povećan znanstveni i praktični interes za područje percepcijskih sažetaka i njihove primjene.

Percepcijski sažetci pokazali su se korisnima za brzu provjeru sličnosti digitalnih slika u odnosu na već postojeće metode. Kako raste količina digitalnih slika, može se zaključiti da postoji mnogo mogućih područja primjene percepcijskih sažetaka – od zaštite autorskih prava, računalne forenzike pa sve do pretraživanja velikih baza slika.

Prednosti upotrebe percepcijskih sažetaka pri utvrđivanju sličnosti između dviju ili više slika su višestruke. Percepcijski sažetci nisu isključivi kao kritpografski sažetci te su male veličine, zbog čega su pogodni za pohranu u bazama podataka umjesto orginalnih slika, za brzo pretraživanje baze te slanje putem mreže. Da bi se napravila vizualna usporedba dviju slika, nije potrebno posjedovati cijele slike, već samo njihove percepcijske sažetke. Isto tako ne ovise o formatu u kojem je pohranjena digitalna slika.

S obzirom na analiziranu literaturu, takve osobine su poželjne i u biometrijskim sustavima. Autentikacija u biometriji označava usporedbu (1 : 1), odnosno pohranjeni predložak uspoređuje se s prikupljenim uzorkom na senzoru te se na temelju postavljenog praga odlučuje o autentičnosti korisnika. Budući da su i predložak i uzorak zapravo digitalne slike, kod većine biometrijskih karakteristika (pogotovo fizičkih) oni se prije usporedbe i odluke o autentičnosti moraju obraditi da bi se izdvojili atributi za analizu. Pritom se primjenjuju mnogobrojne metode i algoritmi koji imaju određena ograničenja te generiraju manji ili veći broj pogrešaka kod prepoznavanja i očitavanja atributa kod biometrijskih uzoraka. Problemi zbog kojih nastaju pogreške u biometrijskim sustavima najčešće se odnose na otežano i nepotpuno očitavanje biometrijskih karakteristika na senzoru radi promjene različitih uvjeta kao što je npr. osvjetljenje, pojavu šuma u prijenosu podataka ili na visoku razinu sličnosti očitanih atributa kod više osoba. Takve pogreške su rezultat deformacije slika odnosno biometrijskih uzoraka. Deformacija podrazumijeva manipulaciju i modifikaciju digitalne slike. Razlikovat će se jedino napad manipulacijom i napad modifikacijom. Napad manipulacijom predstavlja operaciju nad slikom, kojom se ona vizualno bitno ne mijenja. Primjeri takvih napada su promjena svjetline ili kontrasta na slici, rotacija ili kompresija slike. Napad modifikacijom predstavlja operaciju nad slikom, kojom se ista vizualno bitno mijenja. Nakon takvih operacija pretpostavlja se da će slika znatno promijeniti jer se takvim napadima mijenja sadržaj ili struktura odnosno narušava se integritet slike. Primjeri takvih napada su brisanje ili dodavanje dijelova slike, te promjena boje ili teksture. Takvi napadi, u biometrijskim sustavima, također mogu biti posljedica zlonamjernih promjena kojima napadači žele kompromitirati sustav i utjecati na prepoznavanje korisnika.

Može se zaključiti da su svi biometrijski sustavi ipak, kada se uzme u obzir kriterij robusnosti i točnosti, podložni pogreškama nastalim zbog takvih deformacija, te se javlja potreba za stalnim usavršavanjem istih, što je i glavna motivacija za ovo istraživanje.

Pregledom literature također je utvrđeno da još uvijek nije razvijen algoritam za izradu percepcijskih sažetaka temeljen na izdvajanju i analizi lokalnih atributa interesnih regija biometrijskih karakteristika te da nije provedeno vrednovanje algoritama za upotrebu percepcijskih sažetka u području biometrije radi utvrđivanja autentičnosti.

1.3. Hipoteze i ciljevi istraživanja

Cilj ove disertacije jest razviti novi algoritam za izradu percepcijskih sažetaka, koji se temelji na izdvajanju lokalnih atributa biometrijskih karakteristika metodom modificirane cenzus transformacije (MCT) te njegovo vrednovanje robusnosti i točnosti u odnosu na do sada najčešće korištene algoritme. U disertaciji se najčešće korištenim algoritmima smatraju oni koje je najveći broj autora u svojim radovima prikazivao kao standardne, a sljedeći algoritmi opisani su i upotrijebljeni pri vrednovanju: algoritam temeljen na metodi diskretne kosinusove transformacije (DCT ili pHash), algoritam temeljen na metodi diskretne *wavelet* transformacije (DWT), algoritam temeljen na detekciji točaka vizualno značajnih atributa (VFPH), algoritam temeljen na Marr-Hildreth metodi i algoritam temeljen na metodi prosječne vrijednosti bloka (engl. *Block Mean Value*). Treba napomenuti da se u disertaciji najčešće korišteni algoritmi za usporedbu s novorazvijenim algoritmom definiraju kao skup NA = { DCT, DWT, VFPH, MH, BMV } prema metodama na kojima se temelje.

Pojedinačni ciljevi istraživanja jesu:

- opisati dosad najčešće korištene algoritme za izradu percepcijskih sažetaka,
- opisati dosad najčešće korištene metode za usporedbu percepcijskih sažetaka,
- razviti novi algoritam za izradu percepcijskih sažetaka temeljen na izdvajanju atributa biometrijskih karakteristika u cilju poboljšanja učinkovitosti provjere autentičnosti,
- napraviti vrednovanje novog algoritama u odnosu na dosad najčešće korištene algoritme percepcijskih sažetaka s obzirom na njihovu točnost i robusnost.

Istraživačka pitanja jesu:

- u kojoj mjeri manipulacije i modifikacije nad digitalnim slikama utječu na robusnost i točnost algoritama za izradu percepcijskih sažetaka?
- koji je dosad korišteni algoritam najmanje osjetljiv (ili najrobustniji) na manipulacije i modifikacije slike?
- pokazuje li vrednovanje novorazvijenog algoritma za izradu percepcijskih sažetaka unapređenje korištenja u analizi biometrijskih uzoraka radi utvrđivanja njihove autentičnosti u biometrijskim sustavima u odnosu na dosad najčešće korištene algoritme?

Slijedom navedenoga postavljena je hipoteza:

H1: Novi algoritam za izradu percepcijskih sažetaka temeljen na izdvajanju atributa biometrijskih karakteristika daje rezultate koji će ukazati na to da je robusniji i točniji u odnosu na NA = { DCT, DWT, VFPH, MH, BMV } u autentikaciji biometrijskih uzoraka.

1.4. Struktura disertacije

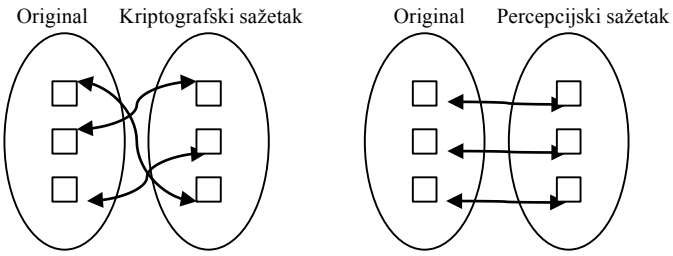
Rad je podijeljen u osam poglavlja. Osim Uvoda i Zaključka, rad se sastoji od šest poglavlja. U drugom poglavlju definiraju se pojam percepcijski sažetak i njegove karakteristike. U trećem poglavlju pod nazivom Algoritmi za izradu percepcijskih sažetaka opisuju se dosadašnja istraživanja u području percepcijskih sažetaka te najčešće korišteni algoritmi za izradu percepcijskih sažetaka, a koji se kasnije u disertaciji uspoređuju s novorazvijenim algoritmom. U četvrtom poglavlju defifniraju se metode koje su se pri vrednovanju upotrebljavale za utvrđivanje sličnosti percepcijskih sažetaka. U petom poglavlju opisuju se općeniti biometrijski sustav i u disertaciji korištene biometrijske karakteristike. U šestom poglavlju opisuju se pojedine faze novorazvijenog algoritma kao i metode na kojima se taj algoritam temelji. Sedmo i najvažnije poglavlje odnosi se na vrednovanje novorazvijenog algoritma s obzirom na njegovu robusnost i točnost u odnosu na spomenute najčešće korištene algoritme kao i mogućnost upotrebe u području biometrijske autentikacije.

U zadnjem poglavlju dan je zaključak disertacije.

Implementacija opisanog rješenja ima znanstvenu važnost i mogućnost praktične primjene. U području biometrije bit će moguće na jednostavan način upotrebljavati učinkovit algoritam za autentikaciju korisnika. Iz znanstvene perspektive svakako treba napomenuti da još nije razvijen algoritam za izradu percepcijskih sažetaka temeljen na izdvajanju i analizi atributa interesnih regija biometrijskih karakteristika te da nije provedeno vrednovanje algoritama za upotrebu percepcijskih sažetka u području biometrije radi utvrđivanja njihove autentičnosti. Drugim riječima, predloženo istraživanje predstavlja novi pristup odabiru, razvoju i procjeni algoritama percepcijskih sažetaka radi upotrebe u biometrijskim sustavima.

2. PERCEPCIJSKI SAŽETAK

Enciklopedija Hrvatskog leksikografskog zavoda Miroslav Krleža percepciju (lat. *perceptio*) definira kao „proces kojim se zahvaća i upoznaje objektivna realnost, a nastaje djelovanjem fizikalnih procesa iz okoline na osjetila. Percepcija omogućuje stjecanje informacija o važnim svojstvima okolnih predmeta, bića, pojava, o njihovu prostornom i vremenskom razmještaju, oblicima i veličini te kvalitativnim i intenzitetnim razlikama" (Hrvatska enciklopedija – mrežno izdanje, Percepcija, Leksikografski zavod Miroslav Krleža, 2017.). „Percepcijski sažetak je 'otisak' datoteke koji se izvodi iz različitih atributa njihovog sadržaja" (Zauner, 2010.). Za razliku od kriptografskih *hash* funkcija, koje se ponašaju na način da male promjene u ulazu rezultiraju velikim promjenama na izlazu, percepcijski sažetci (*phash* funkcije) bliže su i sličnije jedna drugoj što su atributi datoteka vizualno sličniji. Takve funkcije moraju biti dovoljno robusne na promjene atributa, a istodobno dovoljno fleksibilne da bi uspješno razlikovale različite datoteke odnosno uzorke.

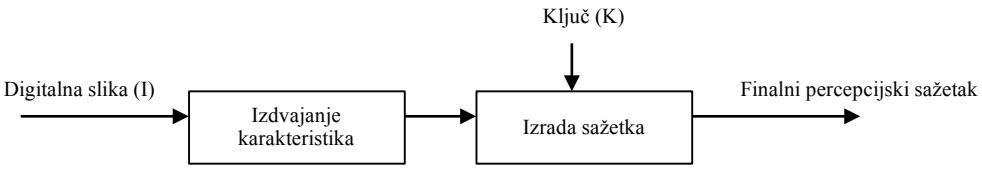


Slika 1. Usporedba kriptografskog i percepcijskog sažetka (Bertolami, 2014.)

Funkcijom percepcijskog sažetka izdvajaju se određeni atributi iz slike te se iz njih izračunava vrijednost sažetka. Atribut koji se izdvaja jest boja, tekstura ili intenzitet skale sive boje (engl. *grayscale*) slike. Vizualno slične digitalne slike imaju slične vrijednosti percepcijskih sažetaka i obrnuto – vizualno različite digitalne slike imaju različite vrijednosti percepcijskih sažetka. Upotrebom metoda za utvrđivanje sličnosti vrijednosti percepcijskih sažetka može se utvrditi jesu li te slike vizualno slične te u kojoj mjeri.

Funkcija percepcijskog sažetka (*h*) opisuje se kao ***h=H(I,K)*** gdje (*I*) predstavlja sliku u digitalnom formatu, a (*K*) tajni ključ, odnosno način prema kojem se izrađuje sažetak (Monga i Evans, 2006.). Na taj je način moguće iz iste slike, a promjenom tajnog ključa, generirati

više različitih percepcijskih sažetaka. Funkcija izrade percepcijskog sažetka opisuje se općenito u dvjema fazama (slika 2.). Prvu fazu predstavlja izdvajanje atributa slike (*I*) u vektore, a drugu fazu predstavlja izrada percepcijskog sažetka. Tajni ključ (*K*) omogućuje jedinstvenost sažetka s obzirom na to da bez poznavanja tajnog ključa nije moguće dobiti istovjetan percepcijski sažetak slike.



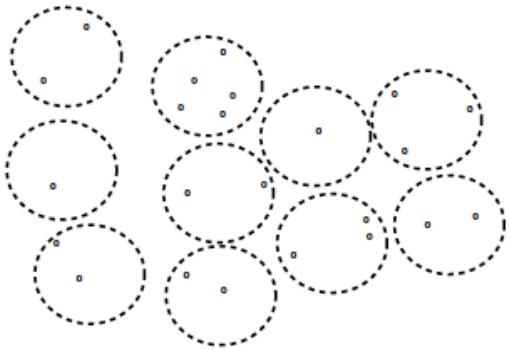
Slika 2. Izrada percepcijskog sažetka (prilagođeno prema Davarzani et. al., 2015.)

Neki autori, kao što su Hadmi i suradnici (Hadmi et. al., 2012.), opisuju i dodatne detaljnije faze (slika 4.). Proces izrade percepcijskog sažetka počinje fazom transformacije u kojoj se atributima slike dodjeljuju vrijednosti gradijenta ili frekvencije. U toj fazi prvo se izvode operacije pretprocesiranja, odnosno veličina slike mijenja se na odgovarajuću rezoluciju slika i pretvara u skalu sive boje (engl. *grayscale*). Slikama se visina i širina smanjuju na zadanu vrijednost. Time se dobiva dvostruka korist: smanjivanje utrošenog vremena računanja za izdvajanje atributa čime se postiže bolja efikasnost algoritma; izdvojeni atributi slika standardizirane veličine u pravilu su robusniji na geometrijske napade povezane s mijenjanjem veličina širine i visine slika. Digitalne slike u boji pretvaraju se u slike sive skale radi smanjivanja utroška vremena računanja za izdvajanje atributa. Važno je napomenuti i da se pretprocesiranjem digitalnih slika mogu popraviti artefakti na slici i na taj način poboljšati utvrđivanje njihovih sličnosti. Neki od elemenata za korekciju jesu greške nastale na senzoru (npr. mrtvi pikseli, greške zbog iskrivljenosti leće i sl.), greške u osvjetljenju, šumovi, geometrijske promjene ili promjene boje.

Smisao faze transformacije jest da se svi izdvojeni atributi slike povežu s vrijednostima piksela ili koeficijentima frekvencije.

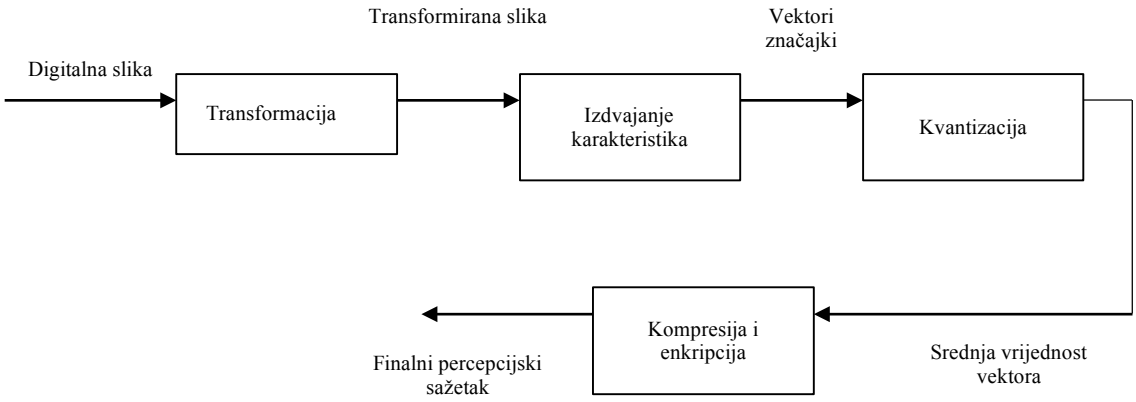
U drugoj fazi atributi slike izdvajaju se u određeni vektor i tada se atributi slike izdvajaju s pomoću odabranog algoritma.

Faza kvantizacije najvažniji je korak. Kvantizacija je proces pretvaranja kontinuiranih vrijednosti u diskontinuirane zaokruživanjem vrijednosti signala na najbliži cjelobrojni iznos. Na taj se način gube međuvrijednosti koje su bile prisutne prije kvantizacije. Taj dio posebno je važan za robusnost i utvrđivanje sličnosti percepcijskih sažetaka što je prikazano na slici 3. Točke unutar istog klastera pripadaju sličnim percepcijskih sažetcima. Robusnost percepcijskog sažetka ovisi o veličini klastera, odnosno što je klaster veći, veći je i prag prihvatljivog odstupanja od percepcijskog sažetka originalne slike. Cilj kvantizacije jest smanjenje količine podataka potrebne za predstavljanje informacija u novoj domeni (Hadmi et. al., 2012.).



Slika 3. Kvantizacija vektora i grupiranje u klastere (Weng Li, 2012.)

Zadnja faza jest faza kompresije i kriptografske enkripcije uz napomenu da enkripcija sažetka nije obvezna. Budući da je kompaktnost jedno od poželjnih svojstava percepcijskih sažetaka, kompresija se također smatra smanjenjem dimenzionalnosti slike. Nakon tih faza izračunava se percepcijski sažetak slike uz određeni uvjet, a prikazuje se u binarnom obliku.



Slika 4. Dodatne faze izrade percepcijskog sažetka (prilagođeno prema Hadmi et al., 2012.)

Nakon izrade percepcijskog sažetka utvrđuje se sličnost slika s pomoću vrijednosti njihovih percepcijskih sažetaka. Neka je *P* vjerojatnost, a *H* funkcija percepcijskog sažetka koja uzima jednu sliku kao ulaz i od nje izrađuje binarni *string* neke veličine l. *I* označava određenu sliku, a I_{ident} označava modificiranu verziju slike koja je vizualno slična slici I. I_{diff} označava sliku koja je vizulano različita slici I. $h1$ i $h2$ označavaju percepcijske sažetke originalne slike *I* i vizulano različite slike I_{diff}. $\{0/1\}^l$ predstavlja binarni *string* dužine *l*. Tada se četiri poželjna svojstva funkcije percepcijskog sažetka mogu opisati kao (Hadmi, 2012.):

Nepredvidivost vrijednosti (jednaka distribucija) sažetka:

$$P(H(I) = h_1) \approx \frac{1}{2^l}, \forall h_1 \in \{0,1\}^l$$

Neovisnost za percepcijski različite slike *I* i I_{diff}:

$$P(H(I) = h_1 \big| H(I_{diff}) \approx P(H(I_{ident}) = h_1), \ \ \forall h_1, h_2 \in \{0,1\}^l$$

Invarijantnost za percepcijski slične slike *I* i I_{ident}:

$$P(H(I) = H(I_{ident})) \geq 1 - \theta_1 , \qquad za\ \theta_1 \approx 0$$

Razlika za percepcijski različite slike *I* i I_{diff}:

$$P\left(H(I) \neq H(I_{diff})\right) \geq 1 - \theta_2 \qquad za\ \theta_2 \approx 0$$

2.1. Identifikacija i autentikacija percepcijskih sažetaka

Percepcijski sažetci slika mogu se upotrebljavati za autentikaciju i za identifikaciju digitalnih slika.

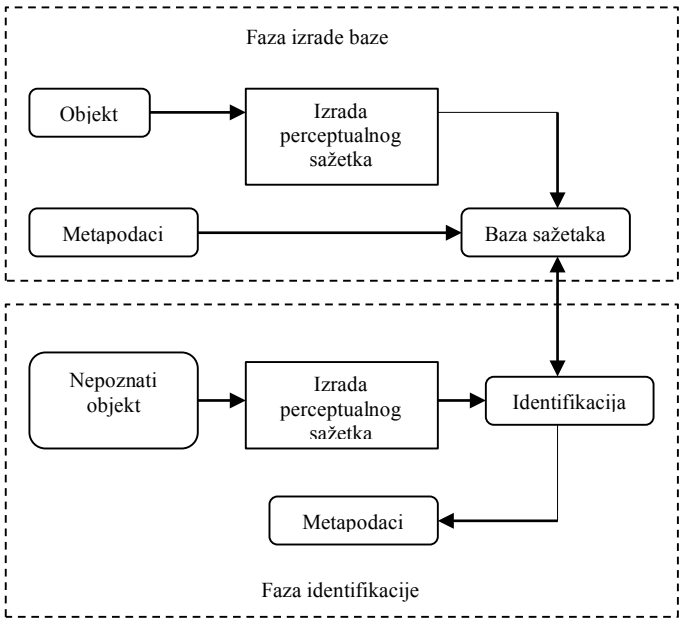
Autentikacija je općenito proces utvrđivanja autentičnosti. Kod digitalnih slika autentičnost se utvrđuje usporedbom s originalom (1 : 1).

Schneider i Chang (Schneider i Chang, 1996.) autentičnost digitalnih slika opisuju kroz usporedbu *bit-po-bit* slike s originalnom slikom i autentičnost definiraju kao vrijednost 1.0

ako je slika u svakom bitu istovjetna. Ako te istovjetnosti nema, slika nije autentična s originalom i ima vrijednost 0.0. U svojem radu definiraju i parcijalnu (djelomičnu) autentičnost, odnosno vrijednost postotka istovjetnosti bitova iako napominju da je to pitanje subjektivnosti i primjene takvih usporedba. Što je veće podudaranje, veći je i rezultat podudaranja (engl. *match score*). Ako rezultat prijeđe prag, odnosno postavljenu numeričku vrijednost pohranjenog predloška (engl. *treshold*), osoba je označena kao autentična. Ono što se javlja kao problem jest što ponekad ljudskom oku vizualno slične slike imaju različite atribute. Kao primjer navodi se modifikacija kompresijom slike.

Percepcijski sažetci mogu se upotrebljavati i za identifikaciju digitalnih slika (1 : N). U literaturi (Lv, 2013.) i (Meixner i Uhl, 2006.) najviše se spominju u kontekstu pretraživanja velikih baza podataka. Važno je istaknuti da se u takve baze pohranjuju samo percepcijski sažetci i metapodaci (npr. naziv datoteke), a ne cijele digitalne slike, što uvelike pridonosi smanjenju veličine kao i povećanju brzine pretraživanja takve baze. Također treba napomenuti da pojava malog broja lažno pozitivnih rezultata ne utječe na performanse sustava.

Zauer (Zauner, 2010.) također opisuje primjer identifikacije upotrebom percepcijskih sažetaka. Sustav za identifikaciju prikazan je na slici 5.



Slika 5. Sustav za identifikaciju multimedijalnog objekta pomoću percepcijskih sažetaka (prilagođeno prema Zauner, 2010.)

Vidljivo je da je sustav podijeljen na dva dijela ili dvije faze: izradu baze i identifikaciju atributa. U fazi izrade baze podaci se u bazi pohranjuju u obliku percepcijskih sažetaka originalnih datoteka te se svakom sažetku dodjeluju i metapodaci (naziv ili opis datoteke – npr. Exchangeable image file format (Exif)). U fazi identifikacije atributa nepoznati objekt (datoteka) predstavlja se sustavu te se njegov percepcijski sažetak uspoređuje s onima pohranjenima u bazi. Ako je identifikacija pozitivna, sustav će prikazati i dodatne informacije o datoteci.

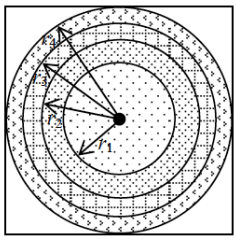
3. ALGORITMI ZA IZRADU PERCEPCIJSKOG SAŽETKA

Brojni autori bavili su se percepcijskim sažecima. Tako Venkatesan i suradnici (Venkatesan et. al., 2000.) u svojem radu predlažu upotrebu percepcijskih sažetaka u upravljanju digitalnim slikama u velikim bazama podataka u smislu pretraživanja duplikata, u bržem indeksiranju slika te zaštiti intelektualnog vlasništva. Algoritam koji upotrebljavaju za izradu percepcijskog sažetka temelji se na metodi diskretne *wavelet* transformacije (DWT) nasumce odabranih pravokutnika na slici. Monga i suradnici (Monga et. al., 2006.) opisuju okvir za izradu percepcijskog sažetka koji uključuje fazu izdvajanja globalnih i lokalnih atributa slike iz kojih se izrađuje sažetak. Globalni atributi odnose se na promjene u cijeloj slici, a lokalne samo na određena područja u slici. Fridrich i Goljan (Fridrich i Goljan, 2000.) u svojem algoritmu za izradu percepcijskih sažetaka upotrebljavaju metodu diskretne kosinusove transformacije (DCT). Lef`ebvre i suradnici (Lef`ebvre et al.) predlažu algoritam izrade percepcijskih sažetaka na temelju metode Radonove transformacije. Lei i suradnici (Lei et al., 2011.) također upotrebljavaju Radonovu transformaciju koju nadopunjavaju Fourierovom diskretnom transformacijom (FDT) radi otpornosti na manipulaciju slike rotacijom. Pri izradi percepcijskih sažetaka Kozat i suradnici (Kozat et al., 2004.) upotrebljavaju metodu dekompozicije singularne vrijednosti (engl. *Singular Value Decomposition* (SVD)). Swaminathan, Yinian i Wu (Swaminathan et al., 2005.) pokušavaju se baviti pitanjem sigurnosti atributa slika iz kojih se generiraju percepcijski sažetci. Isti autori nekoliko godina kasnije (Swaminathan et al., 2006.) pokušavaju napraviti vrednovanje postojećih algoritama za zaštitu atributa slika. Schneider i Chang (Schneider i Chang, 1996.) za izradu percepcijskih sažetaka upotrebljavaju intenzitet histograma pojedinih blokova slike. Weng i suradnici (Weng et al., 2012.) u svojem radu kombiniraju percepcijske sažetke i vodeni žig te među ostalim ističu da bi percepcijski sažetak trebao imati sljedeća obilježja:

- kompaktnost
- robusnost
- diskriminativnost
- ovisnost o tajnom ključu.

Zauner (Zauner, 2010.) u svojem radu opisuje okvir za mjerenje učinkovitosti funkcija percepcijskih sažetaka. Spominje pojam „napad", odnosno opisuje metode manipulacije i modifikacije nad slikama te mjeri utjecaj na prepoznavanje sličnosti slika s pomoću sažetaka. U radu uspoređuje RADIAL, DCT i Marr-Hildreth algoritme za izradu percepcijskih sažetaka. Hadmi i suradnici (Hadmi et. al., 2012.) percepcijski sažetak vide kao moguću alternativu algoritmima digitalnog potpisivanja, odnosno metodi vodenog pečata kojom se potvrđuje autentičnost slike. Krawetz (Krawetz, 2011.) opisuje jednostavnije algoritme koji se temelje na statističkim podacima slika kao što je srednja vrijednost boje (engl. *Average hash*) ili razlika između vrijednosti boje susjednog piksela (engl. *Difference hash*) te s pomoću njih uspoređuje učinkovitost i brzinu izrade percepcijskih sažetaka. Yang i suradnici (Yang et al., 2006.) upotrebljavaju algoritam koji se koristi metodom prosječne vrijednosti bloka (engl. *Block Mean Value*). Svaka testna slika dijeli se na blokove jednake veličine iz koje se potom izračunava vrijednost boje (gradijenta) za svaki blok. Ovisno o odstupanju od prosječne boje slike bloku se pri izradi percepcijskog sažetka dodjeljuje binarna vrijednost 0 ili 1. Ramirez-Gutierrez i suradnici (Ramirez-Gutierrez et al., 2013.) upotrebljavaju globalne i lokalne atribute na slikama radi otkrivanja neovlaštenih izmjena na slikama s pomoću percepcijskih sažetaka.

Tang i suradnici (Tang et al., 2012.) iznose poseban problem modifikacija rotacijom slike i algoritme dijele na one koje su robusni na rotaciju i one koje nisu. Zaključuje se da je većina dotad predstavljenih algoritama robusna na manipulacije i modifikacije kao što su JPEG kompresija, svjetlina, kontrast i sl., ali da ih većina nije robusna na rotaciju. U radu daje svoj prijedlog izrade perceptualnog sažetka prstenastim pregradama oko centralnog piksela slike (slika 6.).



Slika 6. Prstenaste pregrade oko centralnog piksela slike (Tang et al., 2012.)

Noviji radovi kao što je rad Ramakrishnana i suradnika (Ramakrishnan et al., 2014.) pokazuju spajanje globalnih (izdvajanje karakteristika Zernikovim momentima) i lokalnih atributa (tekstura) slike u izradi percepcijskog sažetka te način osiguravanja tajnog ključa kaotičnom neuronskom mrežom. Shradha i suradnici (Shradha et al., 2016.) upotrebljavaju prosječnu vrijednost gradijenta radi vizualne usporedbe proizvoda u sustavu kupovine. Govindaraj i Sandeep (Govindaraj i Sandeep, 2015.) kombiniraju metodu diskretne *wavelet* transformacije (DWT) i prstenaste pregrade kako bi dobili percepcijske sažetke invarijantne na rotaciju. Lv i Wang (Lv i Wang, 2012.) opisuju SIFT-Harrisov detektor radi izdvajanja atributa koji su robusni na geometrijske translacije. Fang i Cheng (Fang i Cheng, 2015.) opisuju metodu za izradu percepcijskih sažetaka s pomoću atoma vala (engl. *wave atom*) radi prepoznavanja malicioznih napada te napada na sadržaj slike.

Na temelju analize prethodno navedene literature uočava se da se algoritmi za izradu percepcijskih sažetaka mogu podijeliti u skupine prema korištenim metodama:

- **metode temeljene na statističkim podacima atributa slika**: metode za izdvajanje atributa slike koje se upotrebljavaju za izradu percepcijskog sažetka izračunavaju se iz statističkih pokazatelja kao što je srednja vrijednost, varijanca ili histogram;
- **metode temeljene na relacijama između atributa slika**: metode za izdvajanje atributa slike koje se upotrebljavaju za izradu percepcijskog sažetka izračunavaju se s pomoću diskretne *wavelet* transformacije (DWT) ili diskretne kosinusove transformacije (DCT);
- **metode temeljene na „grubim" atributima slika**: metode za izdvajanje atributa slike koje se upotrebljavaju za izradu percepcijskog sažetka izračunavaju se s pomoću metoda prostorne distribucije koeficijenata slike, koeficijenata frekvencija slike, Fourierove transformacije i sl.;
- **metode temeljene na „vidljivim" atributima slika**: metode za izdvajanje atributa slike koje se upotrebljavaju za izradu percepcijskog sažetka izračunavaju se samo iz pojedinih uočljivijih atributa slika.

Kao što se može primijetiti, većina autora ističe da je glavni cilj primjene percepcijskih sažetaka izdvajanje robusnih atributa slike kojima se mogu uspješno otkriti modifikacije i manipulacije nad slikom.

Algoritmi za izradu percepcijskog sažetka koji se upotrebljavaju u disertaciji te s kojim se uspoređuje novorazvijeni algoritam jesu:

1. algoritam temeljen na metodi diskretne kosinusove transformacije (*DCT ili pHash*),
2. algoritam temeljen na metodi diskretne wavelet transformacije (*DWT*),
3. algoritam temeljen na detekciji točaka vizualno značajnih atributa (*VFPH*),
4. algoritam temeljen na *Marr-Hildreth* metodi (MH) i
5. algoritam temeljen na metodi prosječne vrijednosti bloka (engl. *Block Mean Value (BMV)*).

Prije opisivanja navedenih algoritama potrebno je napomenuti da se metode na kojima se algoritmi temelje upotrebljavaju i u područjima obrade digitalnih slika kao što su računalni vid (engl. *computer vision*) ili sustavi za pretraživanje slikovnih baza (engl. *Content-Based Image Retrival – CBIR*), no za potrebe disertacije opisuju se samo njihove karakteristike važne za područje percepcijskih sažetaka.

Računalni vid (engl. *computer vision*) jest područje umjetne inteligencije koje se bavi izlučivanjem informacije iz slike. Računalni vid bavi se i izradom sustava koji služe za prikupljanje informacija iz slike. Slike se mogu prikupljati iz različitih izvora kao što su kamera, određeni medicinski uređaji (CT skener, ultrazvuk) itd. Neke od poddisciplina računalnog vida jesu praćenje, detekcija i prepoznavanje objekata, detekcija događaja, restauracija slike i slično. Računalni vid srodan je mnogim drugim znanstvenim disciplinama kao što su optika, obrada i analiza slike, raspoznavanja uzoraka, robotika, umjetna inteligencija itd. (Rojković, 2009.).

Biološki i računalni vid blisko su povezani. Istraživanje biološkog vida uključuje istraživanje vizualnih percepcija ljudi i životinja u cilju izgradnje modela funkcioniranja tih sustava s aspekta fizioloških procesa. S druge strane, računalnim vidom istražuju se i opisuju umjetni vizijski sustavi koristeći se znanjima dobivenima proučavanjem biološkog vida.

Sustavi za pretraživanje slikovnih baza (engl. *Content-Based Image Retrival – CBIR*) temelje se na uspoređivanju sličnosti tražene slike s pohranjenim slikama u bazi i na uspoređivanju njihovih atributa boje, teksture ili oblika. Lew i suradnici (Lew et al., 2006.) u

svojem radu navode najčešće korištene metode kojima se koriste sustavi za pretraživanje slikovnih baza. Kod atributa boje uglavnom se uspoređuju histogrami cijele slike ili pojedine regije. Pri traženju sličnosti tekstura slika upotrebljavaju se metode kojima se uspoređuje vizualna komponenta teksture (npr. svjetlina gradijenta) ili prostorna komponenta (položaj ili smjer) uzoraka tih tekstura. Usporedba oblika odnosi se na oblike pojedinih regija u slici. Najčešća metoda koja se pritom upotrebljava jest segmentacija ili traženje rubova. Detektori oblika trebali bi biti invarijantni na translaciju, rotaciju ili skaliranje.

3.1. Algoritam temeljen na metodi diskretne kosinusove transformacije

Diskretna kosinusna transformacija jest linearna transformacija vrijednosti uzoraka (piksela) u koeficijente (nove numeričke vrijednosti uzoraka), čijom je kvantizacijom omogućeno uklanjanje prostorne redundancije unutar slike. DCT, poput svake transformacije povezane s diskretnom Fourierovom transformacijom (engl. *DFT-Discrete Fourier Transform*), izražava funkciju ili signal u smislu sume sinusoida s različitim frekvencijama i amplitudama. Diskretna kosinusova transformacija upotrebljava samo funkciju kosinusa, za razliku od diskretne Fourierove transformacije, koja upotrebljava i sinus i kosinus. Jezgra transformacije jednaka je za sve blokove što omogućuje veću brzinu proračunavanja DCT-a. DCT je odvojiva transformacija što znači da se može provoditi zasebno za horizontalni i vertikalni smjer. DCT transformacija upotrebljava kosinusne funkcije čiji su argumenti diskretni valni oblici (Jančić, 2002.). Budući da je DCT realna transformacija, ne postoji fazni dio spektra, već samo amplitudni dio. Iako postoji više verzija DCT (DCT-I − DCT-VIII), kada se govori o DCT-u, obično se podrazumijeva DCT-II.

Opis transformacije preuzet je iz nastavnih materijala kolegija Digitalna televizija Fakulteta elektronike i računarstva u Zagrebu dostupnih na poveznici http://www.vcl.fer.hr/dtv/jpeg/dct.htm i prikazan je u nastavku disertacije.

Definicija DCT transformacije opisana je izrazom (Jančić, 2002.):

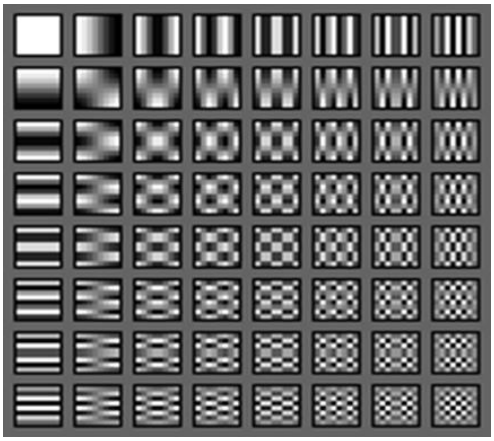
$$F(u,v) = 2\frac{C(u)\cdot C(v)}{\sqrt{M\cdot N}}\left[\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)\cdot cos\frac{(2\cdot x+1)\cdot u\cdot \pi}{2M}\cdot cos\frac{(2\cdot y+1)\cdot v\cdot \pi}{2N}\right]$$

, a njoj inverzna transformacija (IDCT) izrazom (Jančić, 2002.):

$$f(x,y) = 2\frac{C(u)\cdot C(v)}{\sqrt{M\cdot N}}\left[\sum_{u=0}^{M-1}\sum_{v=0}^{N-1} f(u,v)\cdot cos\frac{(2\cdot x+1)\cdot u\cdot \pi}{2M}\cdot cos\frac{(2\cdot y+1)\cdot v\cdot \pi}{2N}\right]$$

pri čemu su *M* i *N* broj redaka i stupaca matrice nad kojom se vrši DCT. $f(x,y)$ je diskretna vrijednost elemenata slike u bloku s koordinatama x,y. Kao rezultat DCT-a nastaje matrica s vrijednostima transformacijskih koeficijenata $F(u,v)$ s koordinatama u,v. $C(u)$ i $C(v)$ konstantni su članovi te iznose (Jančić, 2002.):

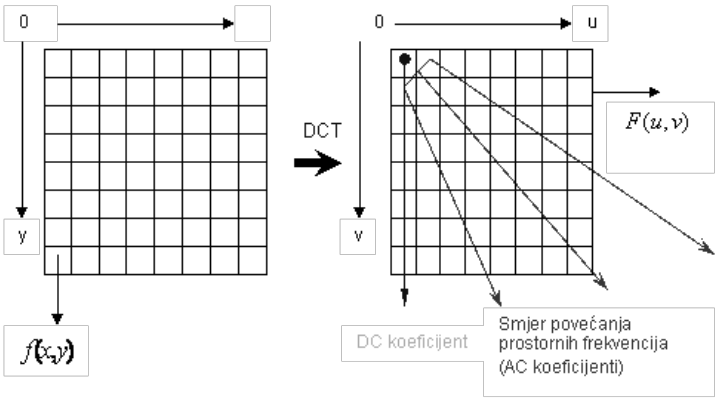
$$C(u) = C(v) = \begin{Bmatrix} \frac{1}{\sqrt{2}}, \xrightarrow{za} u,v = 0 \\ 1, \xrightarrow{za} u,v \neq 0 \end{Bmatrix}$$



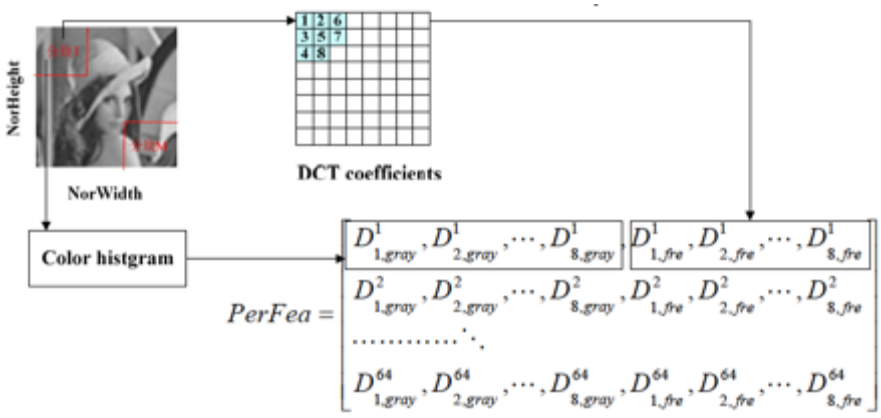
Slika 7. Osnovni valni oblici DCT transformacije (Jančić, 2002.)

Uočava se da DCT za određivanje svakog pojedinog DCT koeficijenta prolazi kroz sve elemente bloka. Da bi se dobio jedan DCT koeficijent, potrebno je 8 x 8 = 64 operacija, što za sva 64 DCT koeficijenta, odnosno jedan cijeli blok daje ukupno 4096 operacija. Za cijelu sliku veličine 256 x 256 elemenata slike potrebno je: 1024 (blokova) * 4096 (operacija po jednom bloku) što daje 4.194,304 operacija. To je prihvatljiv hardverski zahtjev. Kada bi blok bio jedak dimenziji slike od 256 x 256 elemenata slike, tada bi broj operacija bio otprilike 1025 puta veći. Budući da je brzina transformacije jedno od važnih svojstava, blok 8 x 8 smatra se idealnim za diskretnu kosinusnu transformaciju. DCT koeficijenti, $F(u, v)$ sadržavaju informaciju o frekvencijskom sastavu slike. Koeficijent $F(0,0)$ zove se istosmjerni ili DC koeficijent i nalazi se u lijevom gornjem uglu transformacijske matrice. DC koeficijent jednak je osmerostrukoj srednjoj vrijednosti svih DCT koeficijenata.

DC koeficijent sadržava najveći dio informacije o slici i najvažniji je za rekonstrukciju slike. Kada bi blok sadržavao jednake vrijednosti, tada bi od svih DCT koeficijenata DC koeficijent bio jedini različit od nule. On bi nosio cijelu informaciju o slici. Preostala 63 koeficijenta nazivaju se izmjeničnim ili AC koeficijentima. AC koeficijenti sadržavaju informaciju o prostornim frekvencijama u bloku odnosno u slici. U smjeru povećanja koordinata smanjuje se vrijednost AC koeficijenata. Pritom AC koeficijenti koji se nalaze u okolini DC koeficijenta odgovaraju nižim prostornim frekvencijama, a AC koeficijenti koji su smješteni prema donjem desnom uglu opisuju više prostorne frekvencije. DCT transformacija na temelju frekvencijske analize nad elementima bloka provodi preraspodjelu energije koju nosi pojedini element u bloku. Najveći dio energije koncetriran je u DC koeficijentu te niskofrekvencijskim AC koeficijentima koji ga okružuju. AC koeficijenti nižih prostornih frekvencija nose korisnije informacije nego oni viših frekvenija. Ovakav način koncetracije energije u skladu je sa svojstvom ljudskoga vizualnog sustava. DCT visoke frekvencije prikazuje, po apsolutnoj vrijednosti, malim brojevima, koje se onda kodiraju s manjom preciznošću.



Slika 8. Ulazni i izlazni parametri DCT transformacije (Jančić, 2002.)



Slika 9. Izdvajanje atributa slike s pomoću diskretne kosinusne transformacije (DCT) (Zeng, 2013.)

Na slici 9. prikazan je primjer izdvajanja atributa slike diskretnom kosinusnom transformacijom (DCT) (Zeng, 2013.). Kako bi transformacija bila brža i efikasnija, slika se dijeli na kvadratne blokove veličine 8 x 8 elemenata slike. Svaki blok sadržava 64 elementa slike, tj. vrijednosti njihovih amplituda. Vrijednosti funkcije nazivaju se DCT koeficijentima.

Slika 10. Originalna slika i njezina DCT domena (Prungsinchai, 2014.)

Koraci algoritma izrade percepcijskog sažetka slike diskretnom kosinusnom transformacijom (DCT) prikazani su u nastavku (Krawetz, 2011.):

1. Reducira se veličina – 8 x 8 = 64 px ili 32 x 32 px za veće slike.
2. Pretvori se u skalu sive boje (engl. *grayscale*).
3. Izračuna se diskretna kosinusnova transformacija – DCT koeficijenti za svaki blok.
4. Reducira se DCT – na blok u gornjem lijevom kutu s najnižim frekvencijama kod većih slika jer posjeduje više informacija o slikovnim elementima bloka u prostornoj domeni.
5. Izračuna se okvirna srednja vrijednost DCT koeficijenata.

$$S = \frac{1}{64}\sum_{x=0}^{7}\sum_{y=0}^{7} f(x,y)$$

6. Izračuna se percepcijski sažetak u binarnom obliku (0 ili 1) za svaki blok – ovisno o tome je li iznad ili ispod srednje vrijednosti.

3.1. Algoritam temeljen na metodi diskretne wavelet transformacije

Naziv dolazi od francuske riječi *ondelette*, što znači mali val ili valić. „Valić (engl. *wavelet*) je vrsta matematičke funkcije koja se koristi kako bi se dana funkcija podijelila na različite frekvencijske komponente te bi se na taj način moglo promatrati svaku komponentu u najmanjem razlučivom dijelu koji odgovara odgovarajućoj skali" (Bilan 2010.).

Radi jednostavnijeg praćenja, u disertaciji se za to područje umjesto termina valić upotrebljava uobičajen engleski termin *wavelet*.

Waveleti su vremenski ograničene matematičke funkcije, koje mogu imati bilo kakav oblik. Postoje različite obitelji *wavelet* funkcija. Signal se promatra u vremenskim razmacima te se za pojedini vremenski interval računa spektar čime se može dobiti više informacija o položaju frekvencijskih komponenti. Umjesto spektra upotrebljava se naziv skala koja je inverzna frekvenciji, tj. za veće skale *waveleta* spektar bi obuhvaćao niže frekvencijske komponente. „Osnovno načelo *waveleta* je multirezolucijsko predstavljanje signala, a uz pomoć *waveleta*, signal se može prikazati u vremenskoj i frekvencijskoj domeni, tako da osim što je moguće odrediti sve frekvencijske komponente signala, moguće je odrediti i kada se one javljaju" (Bjeropera, 2012.). Kao što se uz pomoć Fourierove analize svaki signal može predstaviti zbrojem sinusnih i kosinusnih funkcija koje se protežu u vremenu, tako se i uz pomoć *wavelet* analize signal može prikazati kao linearna kombinacija *waveleta* konačne energije, tj. dobiva se *wavelet* transformacija (Bjeropera, 2012.).

Kod digitalne slike pojavljuje se statistička i subjektivna redudancija. Statistička redundancija odnosi se na korelirane elemente unutar slika i između njih, a subjektivna redundancija na karakteristiku ljudskoga vizualnog sustava (engl. *HVS-Human Visual System*), odnosno može se napraviti manipulacija nad digitalnom slikom, a da osoba i ne vidi razliku između originalne i deformirane slike. *Wavelet* transformacijom cijela se digitalna slika iz prostornog područja prebacuje u frekvencijsko područje, tj. ne dijeli se na blokove kao što je slučaj kod već opisane diskretne kosinusne transformacije (DCT) (Lees, 2002.).

Efikasna transformacija trebala bi većinu informacija koncentrirati u niskofrekvencijske transformacijske koeficijente. Visokofrekvencijski koeficijenti koji se odnose na detalje slike na koje je ljudsko oko manje osjetljivo, mogu se i odbaciti (Mallat S., 1999.).

Wavelet transformacija dijeli se na: diskretnu transformaciju (DWT), kontinuiranu transformaciju (CWT) i multirezolucijsku analizu (MRA).

Budući da posljednje dvije nisu predmet disertacije, u nastavku se ukratko opisuje diskretna *wavelet* transformacija. Opis transformacije preuzet je iz rada „Poželjna svojstva diskretne wavelet transformacije za primjenu u kompresiji slike" autorice Bjeropere A. (Bjeropera, 2012.)

Dekompozicija slike u niz *waveleta* može se postići skalirajućom funkcijom za niske frekvencije te *wavelet* funkcijom za visoke frekvencije koja odgovara detaljima slike. Ova dva valna oblika translatiraju se i skaliraju na vremenskoj osi preko cijele domene funkcije kako bi dobili niz *wavelet* funkcija na različitim lokacijama i na različitim skalama. Visoke frekvencije transformiraju se kratkim funkcijama (duga skala), a niske frekvencije dugim funkcijama (kratke skale). Rezultat *wavelet* transformacije jest niz *wavelet* koeficijenata kojima se mjeri doprinos *waveleta* na pojedinim lokacijama i skalama (Grgić et al., 1999).

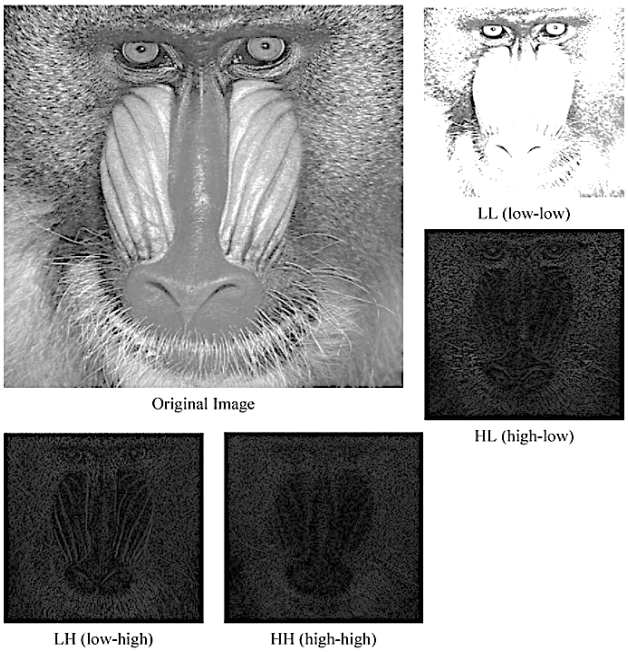
Kod diskretnog *waveleta* skaliranje s i translacija τ izvode se nekontinuirano, tj. u diskretnim koracima. Premda se naziva diskretni *wavelet*, funkcije su i dalje kontinuirane što se može prikazati kao (Bjeropera, 2012.):

$$\Psi_{j,k}(t) = \frac{1}{\sqrt{{s_0}^j}} \Psi\left(\frac{t - k\tau_0 {s_0}^j}{{s_0}^j}\right)$$

gdje su *j,k* cijeli brojevi, a s_0 >1 je fiksni korak skaliranja o kojem ovisi korak translacije τ_0.

Upotrebom diskretnih *waveleta* za transformaciju kontinuiranog signala kao rezultat se dobiva serija *wavelet* koeficijenata.

Wavelet transformacijom radi se dekompozicija slike u četiri seta *wavelet* koeficijenata odnosno četiri potpojasa (LL (*low-low*), HL (*high-low*), LH (*low-high*) i HH (*high-high*)). Potpojas LL predstavlja aproksimaciju slike, dok preostala tri pojasa predstavljaju detalje slike, tj. horizontalno orijentiranu podsliku, vertikalno orijentiranu podsliku i dijagonalno orijentiranu podsliku kako je prikazano na slici 11. Svaki potpojas sadržava DWT koeficijente koji sadržavaju informaciju o energiji slike (Živić, 2015.).



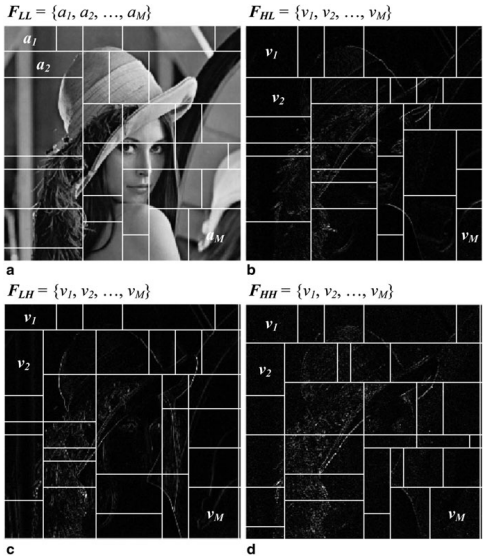
Slika 11. Dekompozicija slike upotrebom DWT transformacije, (Živić, 2015.)

Venkatesan i suradnici (Venkatesan et al., 2000.) razvili su algoritam za izradu percepcijskih sažetaka koji se temelji na prethodno opisanoj metodi diskretne *wavelet* transformacije. Koraci algoritma jesu:

1. Napravi se DWT dekompozicija ulazne digitalne slike.
2. Svaki potpojas nasumično se podijeli na manje pločice (engl. *tiles*) odnosno pravokutnike *M*.
3. Za svaki pravokutnik *M* izračunaju se vrijednosti atributa *F* slike: (slika 12.):
   a) izračuna se prosjek koeficijenata $a_i(1 \leq i \leq M)$ za svaki pravokutnik da bi se dobio F_{LL} spajanjem svih rezultata;
   b) izračuna se varijanca koeficijenata $v_i(1 \leq i \leq M)$ za svaki pravokutnik da bi se

dobio F_{LH} , F_{HL} i F_{HH} .

4. Svi dobiveni vektori spajaju se i kvantiziraju upotrebom kvantizatora, koji se temelji na Reed-Mullerovom dekoderu grešaka *D* (Dolecek, 2007.) da bi se dobio konačni binarni sažetak *n* veličine.



Slika 12. Izračunavanje vrijednosti atributa slike - a) F_LL b) F_HL c) F_(LH) d) F_(HH) (Živić, 2015.)

Na temelju dosadašnjih istraživanja i objavljenih radova uočeno je da je predloženi algoritam robusan na nekoliko napada na digitalnu sliku kao što je rotacija (do 2 °), skaliranje (do 10 %) i kompresija, ali nije robusan na promjene u kontrastu ili svjetlini slike. Isto tako, primijećeno je da algoritam nije robusan na male promjene u slici ako one ne mijenjaju uvelike statističke vrijednosti slike (Venkatesan et al., 2000.).

3.2. Algoritam temeljen na Marr-Hildret metodi

Nekoliko metoda koje se upotrebljavaju u obradi slika, kao što su Sobel, Canny, Prewitt (Petrou, 2010.) i slične, temelje se na izdvajanju atributa s pomoću otkrivanja rubova u slici. Rub (engl. *edge*) predstavlja granicu ili konturu između susjednih dijelova slike. Da bi se rub otkrio, upotrebljava se promjena boje ili teksture, a najčešće promjena intenziteta sive boje (kod *greyscale* slika) ili promjena svjetline piksela. Ako se rub definira kao nagla promjena intenziteta sive boje, tada se analiza intenziteta može upotrebljavati za otkrivanje rubova u slikama s pomoću gradijentnih maski. Proces otkrivanja rubova označava se mapom rubova koja radi klasifikaciju piksela i njihovih dodatnih atributa kao što su magnituda i orijentacija. Prema Zauneru (Zauner, 2010.), ako se s $f_c(x, y)$ definira funkcija gradijenta linije (jednodimenzionalnog niza piksela), pri traženju ruba traže se pozicije gdje prva derivacija funkcije doseže lokalni ekstrem. Prvu derivaciju kod obrade slika predstavlja gradijent. Gradijent 2-D funkcije definiran je kao vektor (Sović et al., 2009.):

$$\nabla f_c = \begin{bmatrix} G_x \\ G_y \end{bmatrix} = \begin{bmatrix} \frac{\partial f_c}{\partial x} \\ \frac{\partial f_c}{\partial y} \end{bmatrix}$$

Magnituda (engl. *magnitude*) ovog vektora jest (Sović et al., 2009.):

$$\nabla f_c = mag(\nabla f_c) = \left[G_x^2 + G_y^2\right]^{1/2} = \left[\left(\frac{\partial f_c}{\partial x}\right)^2 + \left(\frac{\partial f_c}{\partial y}\right)^2\right]^{1/2}$$

Radi pojednostavljenja proračuna upotrebljava se aproksimacija magnitude izostavljanjem drugog korijena:

$$\nabla f_c \approx G_x^2 + G_y^2$$

ili upotrebom apsolutnih vrijednosti:

$$\nabla f_c \approx |G_x| + |G_y|$$

Prethodne aproksimacije poprimaju vrijednost 0 na područjima konstantnog intenziteta, a njihove su vrijednosti proporcionalne stupnju promjene intenziteta na područjima na kojima su vrijednosti pojedinih piksela promjenjive. Uobičajeno je magnitudu gradijenta ili njegovih aproksimacija nazivati jednostavno gradijent.

Drugi pristup jest traženje derivacije drugog reda funkcije $f_c(x)$. U slučaju obrade slika derivacije drugog reda općenito se proračunavaju s pomoću Laplaceovog operatora. Laplaceov operator 2-D funkcije $f(x, y)$ prikazuje se na sljedeći način (Sović et al., 2009.):

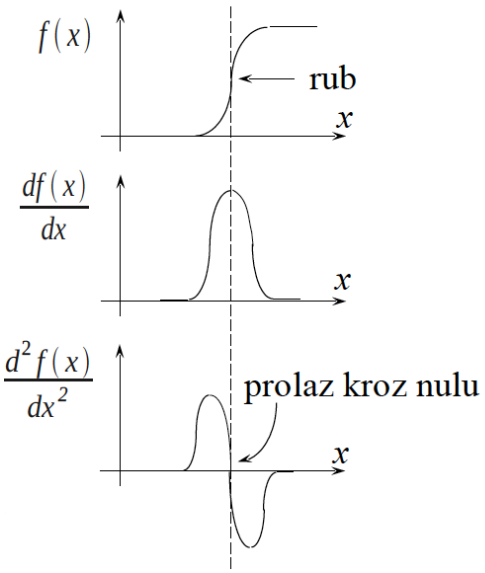
$$\nabla^2 f_c(x, y) = \frac{\partial^2 f_c(x, y)}{\partial x^2} + \frac{\partial^2 f_c(x, y)}{\partial y^2}$$

Cilj je traženje lokacija prolaza kroz vrijednost 0, funkcije $f''_c(x)$ koje označavaju rub (slika 13.).

Kako je već navedeno, osnovna ideja pristupa jest pronaći lokacije na slikama gdje se intenzitet brzo mijenja primjenom nekih od sljedećih dvaju kriterija:

1. pronaći lokacije gdje je magnituda prve derivacije intenziteta veća od definirane vrijednost praga (engl. *threshold*);
2. pronaći lokacije gdje druga derivacija intenziteta poprima vrijednost 0 (prolazi kroz nulu).

Oba pristupa mogu se upotrebljavati u obradi dvodimenzionalnih slika, ali uz upotrebu dodatnih atributa i metoda kao što je određivanje smjera ruba i sl. Na primjer, neprihvatljivo je osjetljiv na šum i smetnje (2. pristup). Njegova magnituda prouzročuje pojavu tzv. duplih rubova te ne može detaljno detektirati smjer rubova (1. pristup).



Slika 13. Detekcija rubova prolazom druge derivacije kroz nulu (Lončarić, 2008.)

Slika 14. Primjer detekcije rubova prolazom kroz nulu (Prungsinchai, 2014.)

Da bi se povećala točnost detekcije rubova, odnosno smanjila osjetljivost na šumove i smetnje, jedno od rješenja jest upotreba različitih filtara. U izradi percepcijskih sažetaka moguće je kombinirati Laplaceov operator (2. pristup) i Gaussov filtar.

U nastavku disertacije prvo se definira kontinuirani Laplaceov operator.

Prema Zauneru (Zauner, 2010.), ako se s $f_c(x, y)$ označi funkcija sive skale u slici, tada je kontinuirani Laplaceov operator:

$$\nabla^2 f_c(x, y) = \nabla \cdot \nabla f_c(x, y) = \frac{\partial^2 f_c(x, y)}{\partial x^2} + \frac{\partial^2 f_c(x, y)}{\partial y^2}$$

gdje se s $\nabla^2 f_c(x, y)$ označavaju prolasci kroz nulu na točkama koje predstavljaju rubove u $f_c(x, y)$.

Tada je moguće primijeniti različite filtre $h(n_1, n_2)$ na sliku upotrebom konvolucije $(*)$. Laplaceova (pr)ocjena (engl. *estimate*) za sliku $f(n_1, n_2)$ tada je:

$$\widehat{\nabla}^2 f(n_1, n_2) = f(n_1, n_2) * h(n_1, n_2)$$

Da bi se detektirali rubovi, odnosno dobili prolasci kroz nulu $\nabla^2 f(n_1, n_2)$, predlaže se usporedba vrijednosti svakog piksela s osam vrijednosti svojih susjednih piksela (matricom kernela). Ako vrijednost piksela *p* znatno odstupa od vrijednosti susjednih piksela *q*, tada postoji rub između njih te se piksel *p* označava mjestom prolaska kroz nulu ako je:

$$|\nabla^2 f(p) \leq \nabla^2 f(q)|.$$

Marr Hildret operator naziva se Laplaceov rubni operator Gaussa (engl. *Laplacian of Gaussian; LoG*). Značajka operatora jest bolja detekcija rubova različitih veličina (skale).

Ako se Gaussov filter definira kao:

$$g_c(x, y) = e^{-\frac{x^2+y^2}{2\sigma^2}},$$

konvolucija i Laplaceov operator mogu se prikazati kao:

$$\nabla^2[f_c(x,y) * g_c(x,y)] = [\nabla^2 g_c(x,y) * f_c(x,y)]$$

Tada se LoG filter označen kao $h_c(x,y)$ definira kao:

$$h_c(x,y) = \nabla^2 g_c(x,y)$$
$$= \frac{x^2 + y^2 - 2\sigma^2}{\sigma^4} \cdot e^{-\frac{x^2+y^2}{2\sigma^2}}$$

Slika 15. LoG vrijednost σ=1, σ=2, σ=3, σ=4
(Woodham, 2013.)

Da bi se implementirao LoG u diskretnoj formi, potrebno je odabrati i vrijednost σ (varijabla skale) što je prikazano na slici 15. Filtar se tada može primijeniti na sliku koristeći se diskretnom korelacijom ili konvolucijom što se može prikazati kao rezultat *R* (Liverovski, 2014.):

$$R(x,y,z) = \sum_{i,j,k} I(x-i, y-j, z-k) M(i,j,k)$$

gdje su x, y i z širina, visina i dubina slike I, a i, j i k širina, visina i dubina maske M.

Sada se mogu prikazati i koraci algoritma za izradu percepcijskih sažetaka temeljenog na Marr-Hildret metodi:

1. korak obuhvaća pretprocesiranje slike I na način da se sve slike pretvore u slike sive skale (engl. *grayscale*);
2. korak jest skalirnje slika I na jednaku veličinu;
3. korak jest primjena filtra zamagljenja na sliku I (engl. *blur*);
4. korak jest traženje rubova u slici odnosno traženje lokacija prolaza kroz vrijednost 0 nakon filtriranja s Laplacian of Gaussian (LoG). Prije se odredi vrijednost σ;
5. korak jest izrada percepcijskog sažetka.

3.3. Algoritam temeljen na metodi srednje vrijednosti bloka

Yang i suradnici (Yang et al., 2006.) predložili su 2006. godine jednostavan algoritam izrade percepcijskih sažetaka digitalne slike metodom srednje vrijednosti bloka (engl. *Block Mean Value*). Da bi takvi percepcijski sažetci bili robusni na napade manipulacijom i modifikacijom orginalne digitalne slike, razvili su čak četiri verzije algoritma koje će se opisati u nastavku disertacije. Da bi povećali sigurnost, upotrijebili su enkripciju tajnim ključem *K*.

Prvi algoritam temeljen na metodi srednje vrijednosti bloka sastoji se od pet koraka (Zauner, 2010.):

1. korak obuhvaća pretprocesiranje slike na način da se sve slike pretvore u slike sive skale (engl. *greyscale*) te skaliraju na jednaku veličinu;

2. korak obuhvaća određivanje veličine percepcijskog sažetka *N* u bitovima (npr. 256 bitova) te podjelu slike *I* na nepreklapajuće blokove $I_1, I_2, \ldots, I_N$;

3. korak obuhvaća enkripciju blokova $\{I_1, I_2, \ldots, I_N\}$ s tajnim ključem *K* da bi se dobio novi nasumični redosljed blokova $\{I'_1, I'_2, \ldots, I'_N\}$;

4. korak jest izračunavanje srednje vrijednosti gradijenta boje $\{M_1, M_2, \ldots, M_N\}$ svakog pojedinog bloka $\{I'_1, I'_2, \ldots, I'_N\}$. Da bi se dobila srednja vrijednost cijele digitalne slike, izračuna se medijan svih srednjih vrijednosti blokova M_d;

5. korak obuhvaća izradu konačne vrijednosti sažetka *h* u binarnom obliku na način da je:

$$h(i) = \begin{cases} 0\,, M_i < M_d \\ 1\,, M_i \geq M_d \end{cases}$$

Drugi algoritam, koji se temelji na metodi srednje vrijednosti bloka, sastoji se od istovjetnih prethodno opisanih pet koraka s tom razlikom da se pri izradi percepcijskih sažetaka blokovi digitalne slike mogu preklapati. Na taj način povećava se robusnost algoritma, a postotak preklapanja blokova postavlja se na polovicu veličine bloka.

Treći algoritam razvijen je kako bi bio robusan na napad rotacijom.

Koraci kod trećeg algoritma jesu (Zauner, 2010.):

1. korak obuhvaća pretprocesiranje slike na način da se sve slike pretvore u slike sive skale (engl. *greyscale*) te skaliraju na jednaku veličinu;

2. korak obuhvaća određivanje veličine percepcijskog sažetka *N* u bitovima (npr. 256 bitova) te podjelu slike *I* na nepreklapajuće blokove $I_1, I_2, \ldots, I_N$;

3. korak obuhvaća enkripciju blokova $\{I_1, I_2, \ldots, I_N\}$ s tajnim ključem *K* da bi se dobio novi nasumični redoslijed blokova $\{I'_1, I'_2, \ldots, I'_N\}$;

4. korak jest izračunavanje srednje vrijednosti gradijenta boje $\{M_1, M_2, \ldots, M_N\}$ svakog pojedinog bloka $\{I'_1, I'_2, \ldots, I'_N\}$. Da bi se dobila srednja vrijednost cijele digitalne slike, izračuna se medijan svih srednjih vrijednosti blokova M_d;

5. matrica M ($\{M_1, M_2, \ldots, M_N\}$) rotira se za određeni stupanj rotacije *D* gdje je $D = \{0{,}15{,}30, \ldots, 345\}$. Time se dobiju 24 matrice M_i $(i = 1{,}2, \ldots, 24)$. Tada se svaka od 24 matrica podijeli na *N* blokova i izračuna se srednja vrijednost svakog bloka pojedinačno $(M_{i1}, M_{i2}, \ldots, M_{iN})$ te ukupna srednja vrijednost svih blokova M_{di};

6. vrijednost sažetka *h* dobije se na istovjetan način kao u prvom opisanom algoritmu, samo što se primjenjuju srednje vrijednosti blokova M_{di}.

Četvrti algoritam jest kombinacija drugog i trećeg algoritma. Digitalna slika podijeli se na *N* preklapajućih blokova kao što je opisano u drugom algoritmu, a zatim se doda korak rotiranja matrica iz trećeg algoritma.

3.4. Algoritam temeljen na detekciji i izdvajanju točaka vizualno značajnih atributa

Monga i Evans (Monga i Evans, 2006.) predložili su algoritam koji se temelji na detekciji i izdvajanju točaka kod vizualno značajnih atributa (engl. *Visual Feature Points Hash* – VFPH) na digitalnoj slici metodom *waveleta* graničnih točaka (engl. *end-stopped wavelet*). Metoda upotrebljava 2D kontinuiranu *wavelet* transformaciju da bi se atributi izdvojili i upotrijebili se kao vrijednosti percepcijskih sažetaka. Općenito je primijećeno da ljudsko oko na digitalnoj slici najprije primjećuje obilježja kao što su kutovi ili krivulje. Bhattacherjee i Vandergheynst (Bhattacherjee i Vandergheynst, 1999.) konstruirali su *wavlete* graničnih točaka da bi zabilježili takve atribute. Metoda u suštini kombinira metodu Morletovih *waveleta* (engl. *Morlet wavelet*) i prvu derivaciju Gaussiana (*FDoG*) (Monga i Evans, 2006.):

$$\psi_E(x, y, \theta) = (FDoG)\ o(\psi_M(x, y, \theta))$$

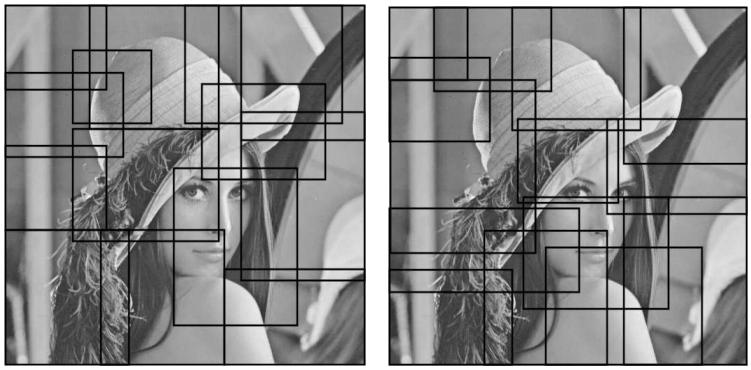
gdje *x* i *y* označavaju koordinate lokacija, a orijentacija je prikazana kao $\theta = tan^{-1}\left(\frac{k_1}{k_0}\right)$. k_1 i k_0 označavaju *wavelet* vektor.

Prva omogućuje detekciju strukture i orijentaciju linija na digitalnoj slici, a druga označava njihove granične točke.

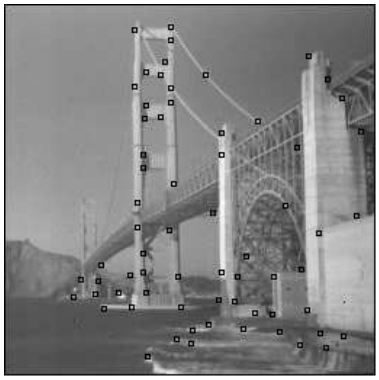
Slika 16. Detekcija strukture i orjentacije linija metodom Morletovih valića (Monga i Evans, 2006.)

Algoritam za izradu percepcijskih sažetaka koji su predložili Monga i Evans navedenu metodu upotrebljava za detekciju i izdvajanje točaka vizuano značajnih atributa na slici. Slika je u prvoj fazi podijeljena na preklapajuće pravokutne regije ili regije u obliku elipse s nasumično odabranim radijusom ili veličinom. Za svaku lokaciju napravi se *wavelet* transformacija da bi se dobili koeficijenti. Značajni atributi regije identificiraju se na način da se traži lokalni maksimum vektora *wavelet* koeficijenata. Poželjno je postaviti i prag detekcije (engl. *treshold*) da bi se izbjegla lažna detekcija atributa. Da bi se postigla robusnost algoritma na manipulacije koje utječu na vrijednosti vektora, autori predlažu i kvantizacijsku shemu koja se temelji na procjeni vjerojatnosti distribucije značajnih atributa.

Vektori detektiranih atributa tada se binariziraju da bi se dobio percepcijski sažetak. Za izradu percepcijskog sažetka upotrebljavaju dva algoritma. Prvi algoritam jest deterministički algoritam odabira fiksnih atributa, a drugi algoritam jest algoritam nasumično odabranih preklapajućih regija slike s pomoću različitih ključeva *K* što je prikazano na slici 17.



Slika 17. Podjela slike na N = 13 pravokutnika, ali s različitim tajnim ključem K (Monga i Evans, 2006.)



Slika 18. Testna slika s konačnim izdvojenim vizualno značajnim atributima (Monga i Evans, 2006.)

4. METODE ZA USPOREDBU SLIČNOSTI PERCEPCIJSKIH SAŽETAKA

Metode za usporedbu percepcijskih sažetaka koje se najčešće upotrebljavaju, jesu BER (engl. *Bit Error Rate*) odnosno Hammingova udaljenost (engl. *Hamming distance*) s obzirom na to da se s pomoću njih može izračunati sličnost, odnosno različitost između dvaju binarnih nizova. U disertaciji se upotrebljava i Demerau-Levenshteinova udaljenost (engl. *Demerau-Levenshtein distance*), a kojom se uspoređuju binarni nizovi koji nisu iste dužine.

4.1. Hammingova udaljenost

Budući da je percepcijski sažetak prikazan kao binarni niz, mjere za usporedbu percepcijskih sažetaka uspoređuju udaljenost ili sličnost između dvaju binarnih nizova iste dužine. Udaljenost ili sličnost prikazana je kao razlika između binarne 1 i 0.

Prema Zengu (Zeng, 2013.) BER označava vrijednost nepodudaranja bitova pri usporedbi dvaju percepcijskih sažetaka. Ako su dvije slike (*i* i *i'*) vizualno različite, teoretska optimalna vrijednost BER M_{BER} (*pHash*) može biti procijenjena na sljedeći način:

$$\text{BER } M_{BER}(pHash) = E[\text{BER}(i, i')]$$

gdje E označava očekivanu vrijednost. Prema Coscunu i Memonu (Coscun i Memon, 2006.) teoretska očekivana vrijednost između dviju različitih slika jest 0,5. Yang i suradnici (Yang et al., 2006.) BER u percepcijskim sažetcima mjere Hammingovom udaljenošću koju stavljaju u omjer s ukupnim brojem bitova percepcijskog sažetka. Hammingova udaljenost mjeri različitost (broj grešaka) podudaranja dvaju *stringova*.

Tablica 1. označava primjer Hammingove udaljenosti između različitih *stringova*.

Tablica 1. Primjer Hammingove udaljenosti (prilagođeno prema Zauner, 2010.)

String 1	*String 2*	*Hammingova udaljenost*
0*0101*	***1****0101*	*1*
*1****2****34****5***	*1****3****34****4***	*2*

Zauner (Zauner, 2010.) opisuje Hammingovu udaljenost i normaliziranu Hammingovu udaljenost. Hammingova udaljenost Δ između *x* i *y* definira se kao:

$$\Delta(x, y) \coloneqq \sum_{x_i \neq y_i} 1, i = 1, \dots, n.$$

gdje $x = (x_1, \dots, x_n)$ označava *string* konačne duljine skupa *A* gdje je x∈ *A*, a za $y = (y_1, \dots, y_n)$ vrijedi isto. Da bi se olakšala usporedba *stringova* prema njihovoj dužini *n,* normalizirana Hammingova udaljenost definira se kao:

$$\Delta(x, y) \coloneqq \frac{\sum_{x_i \neq y_i} 1, i = 1, \dots, n.}{n}$$

Za binarne *stringove* jednake dužine *a* i *b* Hammingova udaljenost jednaka je broju jedinica u *a* XOR *b*, odnosno $a \oplus b$.

U distribuciji $\{0,1\}^n$, što su percepcijski sažetci sličniji, vrijednosti BER i normaliziranu Hammingovu udaljenost imaju **bliže 0**.

4.2. Damerau-Levenshteinova udaljenost

Kako je navedeno, Hammingovom udaljenošću mjeri se udaljenost, odnosno različitost (broj grešaka) elemenata samo kada se uspoređuju dva niza jednake dužine. Levenshtein je 1966. godine predstavio rješenje zahvaljujući kojem se mogu mjeriti nizovi različite dužine. Levenshteinova udaljenost predstavlja minimalni broj operacija koje je potrebno napraviti da bi dva niza bila jednaka. Operacije koje se pritom mogu upotrebljavati jesu:

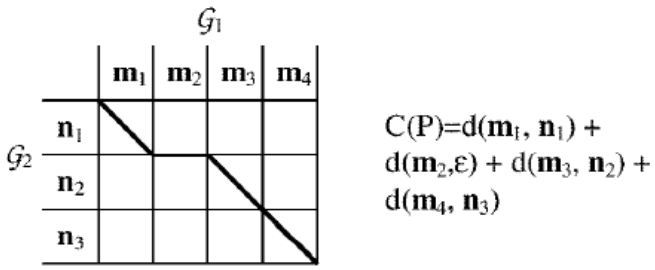
- brisanje elementa,
- zamjena elemenata i
- dodavanje elemenata.

Matematički gledano, Levenshteinova udaljenost između dva niza a, b dužine $|a|, |b|$ može se prikazati kao $lev_{a,b}(|a|, |b|)$, gdje je (Agarwal et al., 2015.):

$$lev_{a,b}(i,j) = \begin{cases} \max(i,j) \\ min \begin{cases} lev_{a,b}(i-1,j)+1 \\ lev_{a,b}(i,j-1)+1 \\ lev_{a,b}(i-1,j-1)+1_{(a_i \neq b_j)} \end{cases} \end{cases}$$

ako je $\min(i,j) = 0$ i gdje je $1_{(a_i \neq b_j)}$ pokazatelj funkcije jednak 0 kad je $a_i = b_j$ jednako 1.

Proces utvrđivanja Levenshteinove udaljenosti prikazan je slici 19. Wilson i Hancock (Wilson i Hancock, 2004.) Levenshteinovu udaljenost upotrebljavali su u mjerenju sličnosti grafova vektora značajki gdje putanja od gornjeg lijevog do desnog donjeg kuta predstavlja najmanju različitost između dvaju grafova $\mathcal{G}_1$ i $\mathcal{G}_2$, odnosno njihovih spektralnih modova (n, m).



Slika 19. Levenshteinova udaljenost između dvaju grafova (Wilson i Hancock, 2004.)

Slika 20. Levenshteinova udaljenost između dvaju znakovnih nizova (Sulzberger, 2016.)

Primjer izračunavanja Levenshteinove udaljenosti između dvaju znakovnih nizova dan je na slici 20. gdje simbol = predstavlja jednakost elemenata, simbol ∘ operaciju zamjene elemenata, simbol + dodavanje elemenata, a simbol − potrebnu operaciju brisanja elemenata.

Damerau-Levenshteinova metoda predstavlja nadogradnju Levenshteinove metode te udaljenost sažetaka opisuje kroz minimalni broj operacija koje je potrebno napraviti da bi dva sažetka bila jednaka. Operacije koje se pritom mogu upotrebljavati jesu: brisanje elementa, zamjena elemenata i dodavanje elemenata u sažetak kao i transpozicija elemenata.

		1	1	1	1	1	0	0	0	1
	0	**1**	2	3	4	5	6	7	8	9
1	1	0	**1**	2	3	4	5	6	7	8
1	2	1	0	**1**	2	3	4	5	6	7
1	3	2	1	0	**1**	2	3	4	5	6
1	4	3	2	1	0	**1**	2	3	4	5
0	5	4	3	2	1	1	**1**	2	3	4
1	6	5	4	3	2	1	**2**	2	3	3
0	7	6	5	4	3	2	1	**2**	2	3
0	8	7	6	5	4	3	2	1	**2**	3
1	9	8	7	6	5	4	3	2	2	**2**

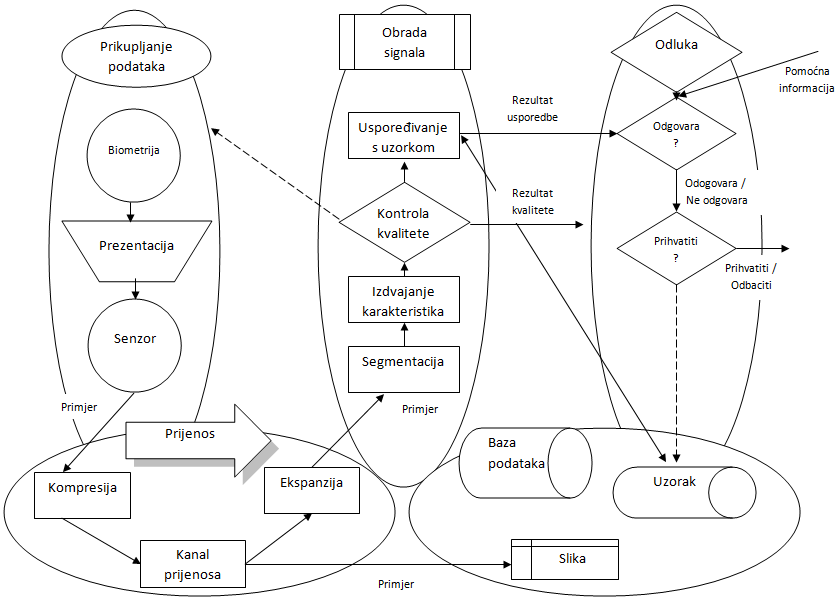
Slika 21. Usporedba dvaju binarnih *stringova* Damerau-Levenshteinovom metodom (Heeringa, 2004.)

Treba napomenuiti i da pri izradi percepcijskog sažetka nije nužno prikazati konačni percepcijski sažetak u binarnom obliku. Ovisno o metodama pretprocesiranja slike mogu se upotrebljavati i druge metode za usporedbu sažetaka. Neke od metoda koje se upotrebljavaju za mjerenje sličnosti između dvaju perceptualnih sažetaka jesu PCC (engl. *Peak of Cross Correlation*) (Zauner, 2010.), PSNR (engl. *Peak Signal to Noise Ratio*) (Lv et al., 2012.) i SIMM (engl. *Structural similarity*) (Wang, 2004.), no one nisu predmet ove disertacije te se neće posebno opisivati.

5. OPĆENITI BIOMETRIJSKI SUSTAV

Prije definiranja novorazvijenog algoritma u ovom poglavlju opisat će se općeniti biometrijski sustav kao i za vrednovanje korištene biometrijske karakteristike.

Prema Waymanu i suradnicima (Wayman et al., 2005.) biometrijski sustav sastoji se od pet podsustava (slika 22.): prikupljanja podataka, prijenosa, obrade signala, pohrane i odluke. On detaljnije opisuje svaki podsustav kako je prikazano u nastavku.



Slika 22. Općeniti biometrijski sustav (Wayman et al., 2005.)

Biometrijski sustav započinje mjerenjem ponašajne ili fizičke karakteristike. Temeljna je pretpostavka da je biometrijska karakteristika karakteristična za pojedinca te da je ponovljiva tijekom vremena. Problem mjerenja i kontroliranja počinje upravo u podsustavu za prikupljanje podataka.

Biometrijska karakteristika mora biti prezentirana senzoru kako bi se dobila ulazna vrijednost. Prezentacija svake biometrijske karakteristike senzoru, neovisno o tome radi li se o fizičkoj ili ponašajnoj, uvodi elemente za svaku biometrijsku metodu. Ti elementi ovise o

različitim čimbenicima, poput samih biometrijskih karakteristika, primjenama te raznim vanjskim čimbenicima koji mogu utjecati na kvalitetu čitava sustava.

Biometrijski sustav može mjeriti jednodimenzionalne (npr. glas), višestruko paralelne jednodimenzionalne (npr. potpis), dvodimenzionalne (npr. otisak prsta), višestruko dvodimenzionalne (npr. šarenica) ili trodimenzionalne signale (npr. lice).

Povratna informacija o uzetom uzorku dobiva se putem provjere kvalitete uzorka, a u slučaju da uzeti uzorak nije odgovarajuće kvalitete, mora se uzeti ponovno.

Rezultat izlaza iz senzora su digitalizirani uzorci biometrijske karakteristike (engl. *sample*). Izlazni podaci iz senzora zapravo ovise (1) o biometrijskoj karakteristici, (2) o načinu na koji je mjerenje karakteristike prezentirano, (3) o tehničkim karakteristikama senzora i (4) o samim korisnicima sustava. Na primjer, biometrijska karakteristika lica može biti promjenljiva – brada, brkovi, ožiljci, naočale i sl. Jednako tako, različiti vremenski uvjeti mogu utjecati na sam uzorak (npr. hladno i toplo vrijeme pri uzimanju uzorka biometrijske karakteristike termograma). Način prezentiranja biometrijske karakteristike također utječe na uzorak (npr. krivo postavljen dlan na senzor). Tehničke karakteristike senzora ovise o kvaliteti njegove izrade. Zadnji, a možda i najvažniji čimbenik jest sam korisnik sustava, koji odlučuje o prihvatljivosti uzimanja uzorka, odnosno mjerenja. Ako je to za njega iz nekog razloga neprihvatljivo, veća je vjerojatnost od odustajanja i neprihvaćanja sustava.

Pojedini biometrijski sustavi prikupljaju podatke na jednoj lokaciji, ali ih obrađuju ili spremaju na drugoj. Takvi sustavi zahtijevaju prijenos podataka. Da bi se ubrzao prijenos u slučaju kada postoje veće količine podataka, upotrebljava se metoda sažimanja odnosno kompresije. Digitalizirani uzorak biometrijske karakteristike kompresira se i šalje putem komunikacijskog kanala u kompresiranom obliku. Pri kompresiji upotrebljavaju se dvije metode: (1) kompresija bez gubitaka (engl. *lossless compression*) i (2) kompresija s gubicima (engl. *lossy compression*) (Wayman et al., 2005.).

Za biometrijski sustav izbor prihvatljive metode ovisi o biometrijskoj karakteristici i specifičnosti samog sustava. Na primjer, ako je lokacija senzora za prikupljanje podataka fizički udaljena od sustava za obradu i pohranjivanje podataka, moraju se upotrebljavati određene mrežne tehnologije, koje vrlo često mogu imati ograničene kapacitete. Stoga se

zbog brzine prijenosa upotrebljavaju metode s većim omjerom kompresije. No, u slučaju da je važnija točnost prikupljenog uzorka, omjer kompresije potrebno je prilagoditi. Isto tako, na prijenos podataka mogu utjecati i različiti drugi čimbenici, poput vrste komunikacijskog protokola te vanjski utjecaji na komunikacijski kanal. Na primjer, ako se upotrebljava nesiguran ili tehnički neispravan komunikacijski kanal, može doći do šuma (neispravnosti) i gubitka prikupljenih podataka. U takvom slučaju izlazni podaci neće odgovarati ulaznima i sam proces prikupljnja podataka najvjerojatnije će se morati ponoviti.

Ekspanzija podataka jest proces rekonstrukcije kompresiranih u originalne podatke, odnosno u podatke podobne za daljnju obradu. Metode koje se pritom upotrebljavaju ovise o metodama kompresije. U slučaju gubitka dijelova podataka koji su nastali pri kompresiji ili prijenosu mogu se upotrebljavati i metode restauracije, odnosno nadoknađivanja izgubljenih podataka, ali i one zadiru u teoriju informacije i specifična područja kao što je obrada slike, videozapisa i zvuka, što znači da o njima u ovoj disertaciji neće biti previše riječi. Kompresija i ekspanzija odvijaju se prije obrade signala i pohrane podataka.

Nakon prikupljanja biometrijske karakteristike i digitaliziranja uzorka uzorak valja pripremiti za uspoređivanje sa sličnim, već pohranjenim uzorcima. Podsustav obrade signala dijeli se u četiri zadatka: (1) segmentaciju, (2) izdvajanje značajki, (3) kontrolu kvalitete i (4) uspoređivanje uzorka. Segmentacija je proces pronalaska biometrijskog uzorka unutar prenesenog signala – traženje njegove strukture. Metode koje se upotrebljavaju pri segmentaciji uvelike ovise o biometrijskoj karakteristici koja je dobivena prilikom prikupljanja podataka. Postoje općenite metode, koje su karakteristične za više biometrijskih karakteristika te posebne metode, koje su specifične za jednu karakteristiku. Na primjer, sustav prepoznavanja lica mora prvo pronaći granice (strukturu) jednog ili više lica u prenesenoj slici. Sustav verifikacije glasa mora pronaći govornu aktivnost unutar signal, koji može sadržavati zvukove koji nisu glas. Nakon pronalaska neobrađenog (engl. *raw*) biometrijskog uzorka i njegova izdvajanja iz većeg signala, uzorak se šalje u proces izdvajanja značajki. Prikupljeni biometrijski uzorak, čak i nakon segmentacije iz većeg signala, može sadržavati neponovljive deformacije prouzročene procesima prikupljanja, kompresije i prijenosa signala. Takve deformacije nemoguće je kontrolirati te svi suvišni elementi moraju biti uklonjeni iz biometrijskog uzorka, dok se istodobno mora sačuvati struktura i kvaliteta uzorka. Pritom se upotrebljavaju različite matematičke metode, a njihova primjena ovisi o karakteristikama samog sustava (Wayman et al., 2005.).

Nakon izdvajanja atributa provjerava se je li primljeni signal iz podsustava prikupljanja podataka dobre kvalitete. Ako karakteristike „nemaju smisla" ili su na neki način nedovoljne, može se brzo zaključiti da su primljeni signali neispravni te se zatražiti novi uzorak od podsustava podataka dok je korisnik još uvijek na senzoru. Ovo područje provjere kvalitete uzorka još je uvijek u stručnoj literaturi nedovoljno opisano i slabo istraženo.

Nakon toga prikupljeni uzorak uspoređuje se s već pohranjenim uzorkom (predloškom). Struktura pohranjenog uzorka mora odgovarati strukturi prikupljenog uzorka. Na primjer, ako je prikupljeni uzorak u matematičkom smislu vektor, i pohranjeni uzorak također je vektor. U slučaju da se uzorci prikupljaju prvi put, mogu se pohraniti u bazu podataka za daljnje usporedbe (engl. *enrollment*).

Wayman, kao i većina ostalih autora, dodaje još i modul pohrane podataka koji upotrebljava jedan ili više oblika pohrane, ovisno o biometrijskom sustavu i prikupljenim uzorcima. Prikupljeni uzorci spremaju se u bazu podataka i služe kao predlošci za daljnje usporedbe.

Tri su tipična pristupa pohrani predložaka (Jain et al., 2005.):

1. lokalna pohrana na uređaj predstavlja siguran i brz način autentikacije. Ovaj je pristup neupotrebljiv u situacijama kada je potrebna mogućnost autentikacije na raznim lokacijama, kao na primjer na bankomatima;
2. pohrana u udaljenu centralnu bazu podataka, pri čemu se podaci razmjenjuju preko sigurne veze. Premda ovaj pristup omogućava autentifikaciju s različitih lokacija, korisnici koji drže do privatnosti ne slažu se s time da se njihovi biometrijski podaci čuvaju u centralnoj bazi;
3. pohrana na prijenosnom mediju kao što je pametna kartica rješava probleme spomenute u prethodno navedenim pristupima. Podaci se ne čuvaju u centralnoj bazi i ne putuju preko mreže, već ih sam korisnik nosi na željene lokacije. Nedostatak je u tome što ovakav sustav za autentifikaciju treba biti opremljen i čitačem prijenosnog medija.

Oblikovanje baze podataka i način njezina funkcioniranja predmet su teorije baze podataka te se s ovog aspekta rad neće time baviti.

Podsustav odluke uključuje preuzimanje uzorka iz podsustava obrade signala te se na temelju većih ili manjih razlika s pohranjenim predloškom (engl. *matching*) donosi odluka o daljnjem postupku. Odluka uključuje prihvaćanje ili odbacivanje ovisno o tome je li sustav prepoznao uzorak ili nije. Takve odluke temelje se na rezultatu (engl. *score*) koji predstavlja numeričku vrijednost, a koja više ili manje odstupa od numeričke vrijednosti pohranjenog predloška. Standardizirana skala odstupanja ne postoji i ovisi o pojedinom sustavu i uređaju. Na primjer, neki sustavi koriste skalu od 0 do 100, a neki od -1 do 1 (Jain et al., 2008.).

Sam postupak odlučivanja može se povezati s uvođenjem pravila, odnosno politika sustava (na primjer, da se dopuste maksimalno tri pokušaja prepoznavanja uzorka). Općenito gledano, politike sustava moraju tražiti prikladan odnos između pogrešnog prihvaćanja i pogrešnog odbijanja korisnika u sustavu.

Budući da se svaki put kad korisnik ima interakciju sa senzorom uzima novi uzorak, ne postoji 100-postotna podudarnost s pohranjenim uzorkom.

U nastavku disertacije ukratko će se opisati biometrijske karakteristike korištene u istraživanju.

5.1. Biometrijske karakteristike

Pod pojmom biometrijska karakteristika podrazumijeva se fizička ili ponašajna karakteristika osobe na temelju koje se obavlja prepoznavanje. Fizičke su karakteristike prirođene karakteristike, poput karakteristika lica, otiska prsta, geometrije dlana, šarenice, mrežnice, termograma lica i tijela, uha, mirisa, DNK i sl. (Wayman et al., 2005.).

Ponašajne karakteristike jesu karakteristike koje je osoba tijekom vremena usvojila, odnosno naučila, poput potpisa, glasa, dinamike tipkanja, hoda i sl. (Wayman et al., 2005.).

U samim počecima izvedbe i upotrebe biometrijskih sustava prednost je davana fizičkim karakteristikama u odnosu na ponašajne karakteristike. Prevladavalo je mišljenje da fizičke značajke, u odnosu na ponašajne, posjeduju „uočljivost". Prema tome mišljenju prevladavalo je i uvjerenje da su fizičke karakteristike pouzdanije od ponašajnih jer imaju tendenciju manjih razlika unutar grupa nego što to imaju ponašajne karakteristike. Danas postoji desetak biometrijskih tehnologija koje se uvelike ili upotrebljavaju ili su gotovo pri kraju istraživanja i početku upotrebe.

5.1.1. Biometrijska karakteristika lica

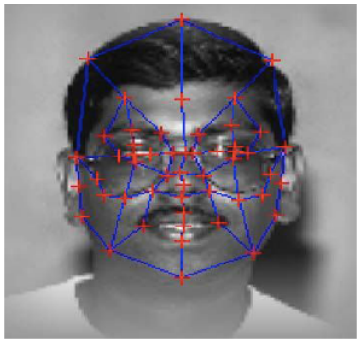
U svakodnevnom životu ljude se prepoznaje prema izgledu lica, koje, uz ostale tjelesne i ponašajne karakteristike, definira ono što se primarno doživljava kao izgled osobe. Odatle i inačica naziva osoba, odnosno lice. U klasičnim postupcima identifikacije, a prije svega u postupku prepoznavanja, identifikacija se temelji na izgledu lica. Izgled lica uvjetovan je i građom kostura glave, odnosno lica, rasporedom muskulature, kvalitetom kože, izgledom dijelova lica poput čela, očiju, nosa, usta i dr. Dakle, lice svakog pojedinog čovjeka po svojem izgledu i građi razlikuje se od lica svih drugih osoba; ono je individualno. Međutim, zbog vida čovjeka koji prepoznaje, psiholoških procesa vezanih uz percepciju, pamćenje i dosjećanje identifikacija prepoznavanjem vrlo je subjektivna, stoga se u postupku prepoznavanja ili pribavljanja osobnog opisa mogu dobiti nepouzdani podaci (Radmilović, 2008.).

Ljudsko je lice dinamičan objekt koji ima visok stupanj promjenljivosti svoje pojave, što čini detekciju lica i raspoznavanje osobe vrlo složenima. U klasičnoj identifikaciji poznata je identifikacija osoba putem fotografije. Osoba čiji je identitet potrebno utvrditi fotografira se

u istom mjerilu u kojem se nalazi fotografija osobe s kojom je se želi uspoređivati, a zatim se metodama linearnih i kutnih mjerenja uspoređuju razmaci između pojedinih dijelova lica, odnosno konstantnih točaka. Kad je riječ o računalnom, biometrijskom prepoznavanju lica, uglavnom se radi o usporedbi na temelju fotografije ili videosnimke. Lice se dijeli na oko 80 karakteristika, npr. razmak između očiju, dimenzije nosa, položaj i razmak između jagodičnih kostiju, dimenzije i oblik brade itd., po obilježjima koja ispunjavaju uvjete tražene za identifikacijska obilježja (Baksi i Singhal, 2014.).

Da bi prepoznavanje bilo na razini identifikacije, potrebno je utvrditi traženi broj podudarnosti (između 15 i 20 atributa). Budući da su odabrana obilježja konstantna i relativno nepromjenljiva, osobu se može prepoznati i nakon kirurških korekcija izgleda lica, promjene frizure i bojenja kose, nošenja naočala i slično.

U početnoj fazi prepoznavanja odraz lica skenira se u različitim mjerilima i zatim se po ključnim indikatorima ocjenjuju segmenti odraza i pod određenom vjerojatnošću određuje se radi li se o odrazu lica ili okoline. U drugoj se fazi određuje položaj glave, što mora prouzročiti određene korekcije pri prepoznavanju i zahtijeva korekcije *x*, *y* i *z* osi.



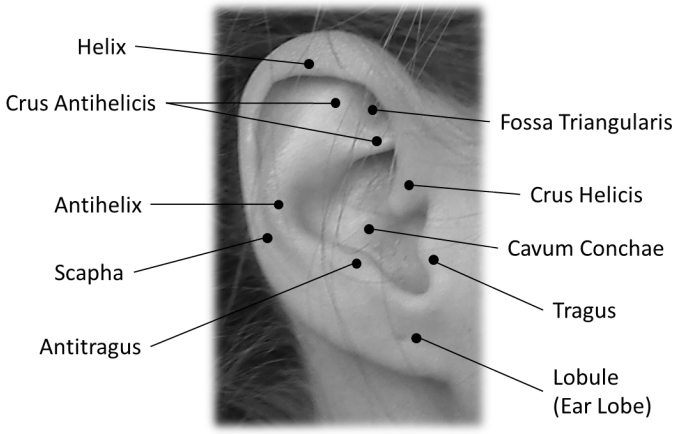
Slika 23. Atributi lica (Mesarević, 2007.)

Ova biometrija jedna je od relativno jeftinijih metoda jer ne zahtijeva skupu specijalnu opremu. Dovoljno je osobno računalo i videokamera. U praksi je dovoljno da osoba prođe pored kamere i da je sustav zabilježi, dok se prepoznavanje osobe obavlja s pomoću prepoznavanja oblika (Radmilović, 2008.).

Takvi sustavi služe za sprječavanje i otkrivanje kriminalaca i mogućih terorista. Većinom se upotrebljavaju u policiji i sličnim organizacijama.

5.1.2. Biometrijska karakteristika uha

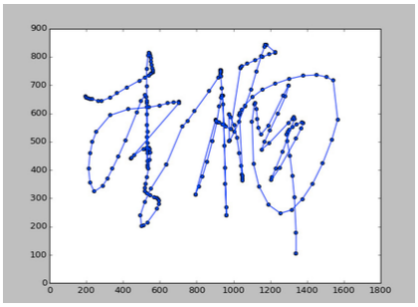
Kao i biometrija lica, uho je kao fizička karakteristika pogodna za beskontaktnu biometriju. Uho ima velik broj obilježja kao što je geometrija, oblik, veličina ili položaj te obilježja koja mogu poslužiti u prepoznavanju osoba. Prednosti uha u biometriji jesu te da je relativno stabilna biometrijska karakteristika jer se ne mijenja puno tijekom starenja. Isto tako, za razliku od pojedinih biometrijskih karakteristika kao što je lice, nije pod utjecajem fizičkih i emocionalnih stanja osobe te ima jednoličniju distribuciju boja. Zbog tih razloga biometrijski sustavi uha daju bolje rezultate u prepoznavanju osoba u odnosu na neke druge biometrijske sutave kod kojih to nije slučaj (Jain et al., 2008.). Potrebno je napomenuti i to da uši (lijevo i desno uho) nisu iste, odnosno nisu simetrične. Biometrija uha jest beskontaktna tehnika pa je korisnici dobro prihvaćaju, može se prikupiti i na daljinu, a za prikupljanje nije potrebna kooperativnost osobe. Ova biometrija također je jedna od relativno jeftinijih metoda jer ne zahtijeva skupu specijalnu opremu. Dovoljno je osobno računalo i videokamera. U praksi je dovoljno da osoba prođe pored kamere. U literaturi se također ističe da je uho sigurnija karakteristika (nego na primjer. lice) jer ga je vrlo teško povezati s nekom osobom pa je potrebna manja zaštita baze podataka s predlošcima. S druge strane, problem s karakteristikom uha jest taj da ju je teško opisati jer nije riječ o prirodnom načinu prepoznavanja osoba (kao što je lice ili glas) pa nedostaje vokabulara u riječniku pogodnih za detaljan opis. Zbog toga se biometrija uha zasniva na izdvajanju i analizi atributa s pomoću kojih se utvrđuju obilježja i vrši prepoznavanje osoba. Isto tako, nedostatak kod biometrije uha jest i nemogućnost ili otežanost prikupljanja atributa u slučajevima kad je uho prekriveno (npr. nakitom, kosom ili kapom) (Pug i Busch, 2012.). Uho je relativno nova biometrija te se upotrebljava u kontroli ulaza ili forenzici.



Slika 24. Anatomija uha (Pug i Busch, 2012.)

5.1.3. Biometrijska karakteristika potpisa

Činjenica da svaka osoba ima jedinstven rukopis te da je potpis neka vrsta *otiska prsta*, otvara mogućnost koja se može iskoristiti u identifikaciji osoba. Razvija se i mijenja tijekom vremena te je pod stalnim utjecajem fizičkih i emocionalnih stanja potpisivača. Potpisi nekih osoba često variraju, i to u tolikoj mjeri da su uzastopni otisci njihovih potpisa značajno različiti.



Slika 25. Primjer analize potpisa (Nan, 2016.)

Ova biometrija upotrebljava statičku, dinamičku ili kombiniranu analizu potpisa kako bi autenticirala osobu. Tehnologija se temelji na mjerenju brzine, pritiska i kuta koje upotrebljava osoba kada se potpisuje ili kada piše nespecificirani tekst (Li i Jain, 2009.).

Biometrijski potpis primjenjuje se u bankama i sličnim financijskim ustanovama. Jedan od smjerova prema kojima se ova tehnologija usredotočila jest i e-poslovanje, ali i druge primjene gdje je potpis prihvaćen kao metoda osobne autentikacije.

Potpis se razvija i mijenja tijekom vremena te je pod stalnim utjecajem fizičkih i emocionalnih stanja potpisivača. Potpisi nekih osoba često variraju, i to u tolikoj mjeri da se uzastopni otisci njihovih potpisa znatno razlikuju. Usporedba potpisa mjeri i vrednuje 60 različitih primarnih i više od 500 sekundarnih atributa za svaki potpis.

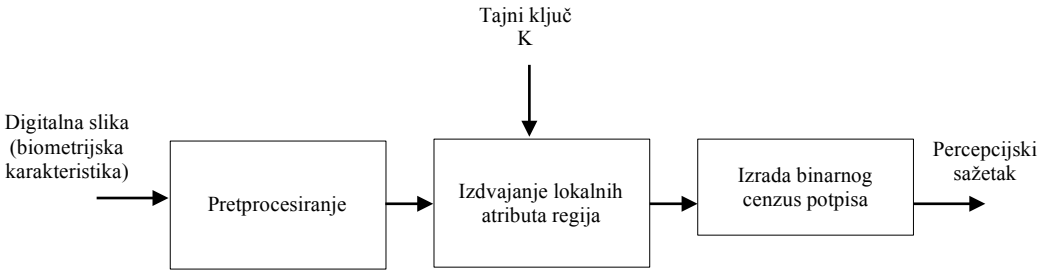
Identifikacijska točnost sustava temeljenih na metodi potpisa je prihvatljiva, iako postoji mogućnost krivotvorenja potpisa.

6. NOVORAZVIJENI ALGORITAM ZA IZRADU PERCEPCIJSKIH SAŽETAKA

Novorazvijeni algoritam za izradu percepcijskih sažetaka temelji se na izdvajanju i analizi atributa interesnih regija (engl. *Region of Interest* (ROI)), odnosno susjednih piksela (engl. *neighbourhood*) oko lokacija biometrijskih točaka na prethodno opisanim uzorcima, odnosno slikama biometrijskih karakteristika lica, uha i potpisa. Takve regije sadržavaju lokalne atribute čije se vrijednosti boje, odnosno intenziteta piksela, oblika ili tekstura opisuju vektorom.

Novorazvijeni algoritam za izradu percepcijskih sažetaka sastoji se od tri faze.

Faze novorazvijenog algoritma prikazane su na slici 26.



Slika 26. Faze novorazvijenog MCT algoritma

Prva faza algoritma započinje pretprocesiranjem. Pretprocesiranjem digitalnih slika moguće je popraviti određene artefakte na slici. Neki od elemenata za korekciju jesu greške nastale na senzoru (npr. mrtvi pikseli, greške zbog iskrivljenosti leće i sl.), greške u osvjetljenju, šumovi, geometrijske promjene ili promjene boje.

Najčešće operacije kod pretprocesiranja digitalnih slika jesu (Lv, 2013.):

- smanjenje prostorne dimenzije boja (engl. *Colour Space Dimension Reduction*): najčešće primjenjivana operacija nad slikama u algoritmima sažetka. Digitalne slike u boji pretvaraju se u slike sive skale (engl. *greyscale*) radi smanjivanja utroška vremena računanja za izdvajanje atributa;
- promjena veličine (engl. *resize*): slikama se visina i širina smanjuju na zadanu vrijednost. Time se dobiva dvostruka korist: smanjivanje utroška vremena računanja

za izdvajanje značajki čime se postiže bolja efikasnost algoritma; izdvojene značajke slika standardizirane veličine u su pravilu robusnije na geometrijske napade povezane s mijenjanjem veličina širine i visine slika;

- Filtriranje: učinkovit način da se popravi robusnost izdvojenih atributa slike na utjecaj šumova u slici. Neki od popularnih filtara kao što su medijan filter ili Gaussov filter učinkoviti su u otklanjanju šumova;
- normalizacije svjetline: svjetlina može varirati ovisno o različitom osvjetljenju prilikom snimanja. Upravo je zato važno da je se normalizira. Postoji mnogo različitih načina za normalizaciju, a najčešće korišteni jesu: normalizacija histogramom, globalni i adaptivni prag.

Druga faza algoritma odnosi se na izdvajanje lokalnih atributa odabranih regija odnosno susjedstva oko opisanih biometrijskih točaka. Lokalni atributi (engl. *local features*) neke slike jesu manji dijelovi te slike koji se, na temelju određenih svojstava, razlikuju od svoje okoline. Različitost ovisi o problemu koji se rješava pa se prema tome može definirati na različite načine. Često se u obzir uzimaju svojstva kao što su intenzitet, boja i tekstura. Atributi mogu biti predstavljeni u različitim oblicima. Tako primjerice atributi mogu biti obične točke (engl. *points*), kutovi (engl. *corners*), rubovi (engl. *edges*), grude (engl. *blobs*) ili regije (engl. *regions*).

Detektor atributa definira se kao način s pomoću kojeg se izdvajaju atributi. Detektori atributa oblikuju se ovisno o primjeni pa iz tog razloga postoji niz različitih detektora koji izračunavaju atribute ovisno o kontekstu.

Razlozi zbog kojih se lokalni atributi upotrebljavaju u obradi i analizi digitalne slike su mnogobrojni. Tuytelaars i Mikolajczyk (Tuytelaars i Mikolajczyk, 2008.) u svojem radu navode neke od njih:

- lokalni atributi mogu imati određenu semantičku interpretaciju u ograničenom kontekstu neke aplikacije (npr. na slikama snimljenima iz zraka detektirani rubovi često predstavljaju ceste);
- lokalnim atributima nastoje se detektirati stabilne točke (engl. *anchor points*) koje su dobro lokalizirane (tj. čiji se položaj i eventualne promjene položaja mogu odrediti s

visokom sigurnošću) i koje se mogu individualno identificirati, što znači da ih se može upotrebljavati za praćenje objekata na nizovima slika ili za kalibraciju kamere;

- skup lokalnih atributa detektiranih na jednoj slici može na robusan način predstavljati tu sliku te takva prezentacija slika može eliminirati potrebu za segmentacijom slike koja obično prethodi fazi prepoznavanja objekata i scena na njoj.

Tuytelaars i Mikolajczyk (Tuytelaars i Mikolajczyk, 2008.) ističu važnost određivanja namjene te navode tri kategorije upotrebe lokalnih atributa. Prva kategorija odnosi se na unaprijed poznat kontekst primjene. Na primjer, rubovi ceste na snimkama iz zraka predstavljat će ceste. Druga kategorija odnosi se na strogo određivanje pozicije lokalnih atributa. Na primjer, ako se primjenom nastoji riješiti problem kalibracije kamere ili 3D rekonstrukcije nekog objekta, lokalni atributi obično će biti dobro lokalizirane točke na razini piksela s točno definiranim pozicijama koje se uobičajeno nazivaju točke interesa (engl. *interest points*). Treća kategorija primjene jest prepoznavanje ili detekcija objekata na nekoj slici bez potrebe za njihovom segmentacijom. U tom slučaju točke interesa neće se promatrati zasebno, već će se promatrati i njihova okolina, tj. kontekst unutar kojega se nalaze. Tada se obično više ne govori o točkama interesa, već o regijama interesa (engl. *interest regions*).

Dobri atributi trebali bi imati sljedeća svojstva (Tuytelaars i Mikolajczyk, 2008.):

- ponovljivost (engl. *repeatability*): u nizu različitih slika sličnog sadržaja koje su snimljene u različitim uvjetima, idealan atribut trebao bi biti prisutan u svim slikama;
- karakterističnost ili prepoznatljivost (engl. *distinctivness*): atributi bi trebali imati što različitija svojstva kako bi se što lakše mogli raspoznavati. Drugim riječima, atribut bi trebao sadržavati što više jednoznačnih informacija;
- lokalitet (engl. *locality*): atribut bi trebao biti lokalan. Obično se definira susjedstvo nad kojim se promatra lokalnost atributa;
- brojnost (engl. *quantity*): broj detektiranih atributa na jednoj slici trebao bi biti dovoljno velik kako bi se detektirali atributi i na manjim objektima. Ipak, optimalan broj atributa ovisi o primjeni;
- preciznost (engl. *accuracy*): lokaciju lokalnih atributa potrebno je biti u mogućnosti precizno odrediti;

- učinkovitost (engl. *efficiency*): detekcija atributa ne bi trebala biti previše računski zahtjevna kako bi se mogla primijeniti i u vremenski kritičnim aplikacijama.

O primijenjenom detektoru ovisi koji će atributi biti pronađeni te kojeg oblika. Osim što se razlikuju u načinu izdvajanja lokalnih značajki (gradijenti, morfologija, geometrija i sl.), razlikuju se i po razini invarijantnosti (translacija, rotacija, skala, afine transformacije i sl.). Različite metode detektora atributa kao što su Harrisov detektor, SUSAN, SURF, FAST i dr. opisane su u brojnim radovima, no to nije predmet ove disertacije pa se neće posebno opisivati.

6.1. Atributi korištenih biometrijskih karakteristika

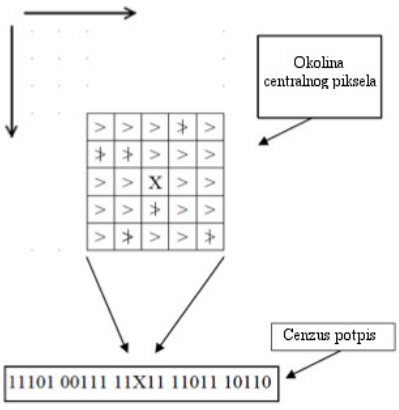
Atributi slika koji se analiziraju u novorazvijenom algoritmu nalaze se u regiji odnosno okolini (engl. *neighbourhood*) oko već određenih lokacija točaka na uzorcima biometrijskih karakteristika lica, uha i statičkog potpisa. Budući da su načini određivanja točaka kod tih biometrijskih karakteristika različiti, a u radu se upotrebljavaju za izradu percepcijskih sažetaka i predstavljaju tajni ključ K, odnosno lokaciju i redoslijed točaka iz kojih se izdvajaju atributi, bit će ukratko opisani u sljedećem poglavlju prije vrednovanja. Potrebno je napomenuti i to da je redoslijed za izdvajanje atributa isti kod svih biomterijskih karakteristika, odnosno početna je točka prva gornja biometrijska točka s lijeve strane, a sve ostale točke slijede desno dolje od početne, što u novorazvijenom algoritmu MCT predstavlja tajni ključ K. Kada se definira tajni ključ K, odnosno lokacija i redoslijed točaka na biometrijskom uzorku, izdvajaju se atributi odabranih regija, odnosno blokova susjednih piksela oko centralnog piksela koji predstavlja lokaciju biometrijske točke. Pri tome je bitno napomenuti da je promjenom lokacije i redosljeda biometrijskih točaka (tajnog ključa K) moguće napraviti više različitih percepcijskih sažetaka iz iste slike odnosno biometrijske karakteristike. Na taj način se postiže sigurnost jer je za usporedbu dva percepcijska sažetka potrebno poznavati tajni ključ K.

U novo razvijenom algoritmu izdvojeni atributi opisuju se vrijednošću gradijenta za svaki piksel. Nakon dobivanja vrijednosti atributa u trećem koraku algoritma kreće se izrada

binarnog cenzus potpisa. Za to se primjenjuje metoda modificirane cenzus transformacije koja će se dalje opisati zajedno s metodom cenzus transformacije.

6.2. Metoda cenzus transformacije

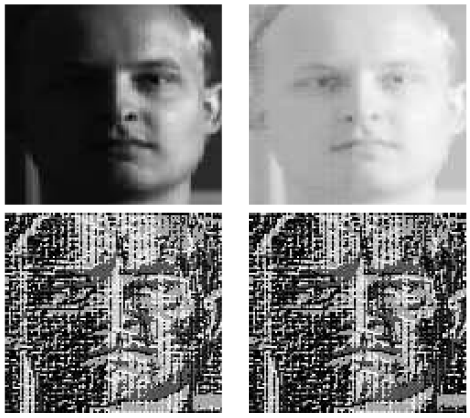
Godine 1994. Zabih i Woodfill (Zabih i Woodfill, 1994.) opisali su metodu za analizu digitalnih slika koju su nazvali cenzus transformacija (engl. *census transformation*). Za svaki centralni piksel računa se binarni *string* (cenzus potpis) na način da se intenzitet boje piksela uspoređuje s intenzitetom susjednih piksela. Za svaki susjedni piksel, određuje se je li njegov intenzitet boje manji ili od centralnog piskela ili nije. Najčešće se uzima blok od 3 x 3 susjedna piksela (engl. *neighborhood*) sa svojom strukturom (kernelom) te se na taj način može dobiti potpis (binarni vektor) dužine osam bitova odnosno 1 bajt ili blok od 5 x 5 susjednih piksela odnosno 3 bajta. Kod cenzus transformacije često se upotrebljava i skalar ranga koji predstavlja ukupan broj piksela čiji je intenzitet boje manji od intenziteta centralnog piksela.



Slika 27. Dobivanje binarnog cenzus potpisa
(Woodfil i Herzen, 1997.)

Metoda cenzus transformacije pokazala je određene prednosti u analizi slika. Kasnija istraživanja drugih autora pokazala su da je metoda otporna na promjene u svjetlini i kontrastu

slike što se pokazalo važnim u opisanim područjima istraživanja. Stein (Stein, 2004.) primjenjivao je cenzus transformaciju u uspoređivanju značajki slike. Muller i suradnici (Muller et al., 2011.), kao i Mohamed i Mertsching (Mohamed i Mertsching, 2012.) iskorištavaju metodu tako da upotrebljavaju atribute slike kako bi otkrili promjene koje su se dogodile pri modifikacijama slike. Ranftl i suradnici (Ranftl et al., 2012.) pokazali su robusnost metode u uvjetima promjene osvjetljenja. Froba i Ernst (Froba i Ernst, 2004.) u svojem radu opisuju metodu cenzus transformacije u kontekstu detekcije lica osoba. Na slici 28. prikazan je primjer robusnosti metode na različitu svjetlinu u prikazivanju lica. Primjer u drugom redu pokazuje da su lica jednaka bez obzira na različitu svjetlinu primjenom cenzus transformacije.



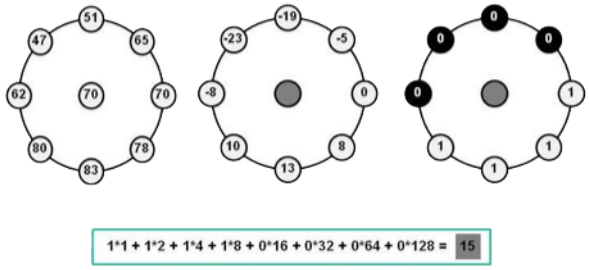
Slika 28. Robusnost cenzus transformacije na svjetlinu
(Froba i Ernst, 2004.)

Cenzus transformacija matematički se može opisati na sljedeći način (Froba i Ernst, 2004.): neka je s $\mathcal{N}(x)$ definirana okolina piksela x za koju vrijedi $x \notin \mathcal{N}(x)$. Cenzus transformacija tada generira binarni *string*, koji prikazuje koji piksel u $\mathcal{N}(x)$ ima manji intenzitet od $I(x)$ odnosno vrijednosti centralnog piksela. Ako se pretpostavlja da su vrijednosti uvijek nula ili pozitivne, tada je funkcija usporedbe cenzus transformacijom $\varsigma(I(x), I(x'))$ jednaka 1 ako je $I(x) < I(x')$ i ako $\otimes$ predstavlja operaciju povezivanja (ulančavanja). Cenzus transformacija tada se definira kako slijedi:

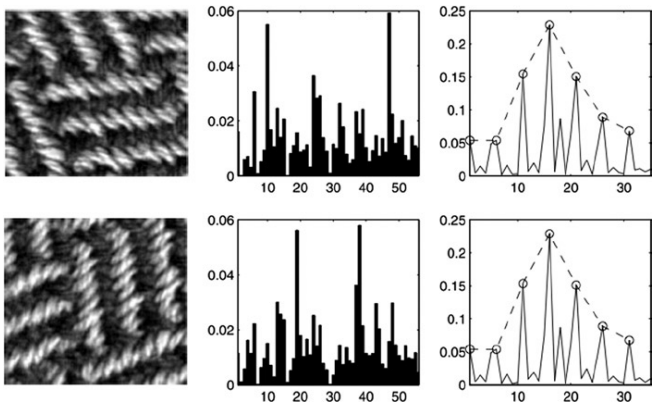
$$\mathcal{C}(\mathbf{x}) = \bigotimes_{\mathbf{y} \in \mathcal{N}} \zeta(\mathbf{I}(\mathbf{x}),\ \mathbf{I}(\mathbf{y})).$$

Važno je naglasiti da $C(x)$ nije koeficijet intenziteta ili sličnosti, nego svi bitovi imaju istu važnost. $C(x)$ u ovom slučaju više predstavlja indeks strukture kernela primijenjen na $\mathcal{N}(x)$ s centrom postavljenim na nulu. Tada svi pikseli u susjedstvu predstavljaju cenzus usporedbe s centralnim pikselom ovisno o svojoj lokaciji što je u određenim situacijama predstavljalo problem zbog nemogućnosti boljeg opisivanja kernela i računanja svih mogućih kombinacija.

Potrebno je napomenuti i to da se iste godine (objavljena je gotovo istodobno) pojavila metoda vrlo slična cenzus transformaciji, a koju su Ojala i suradnici (Ojala et al., 1994.) nazvali LBP (engl. *local binary patterns*) i koja je atribute piksela opisivala kroz LBP vrijednost i kasnije za njihovu usporedbu upotrebljavala dobivene histograme blokova slika (slika 30.). Te dvije metode razlikuju se i po redoslijedu dobivenih binarnih *stringova*. Kao i metoda cenzus transformacije, LBP metoda upotrebljavana je u područjima detekcije lica, prepoznavanja lica, pronalaženja slika u bazi ili detekcije kretnji.

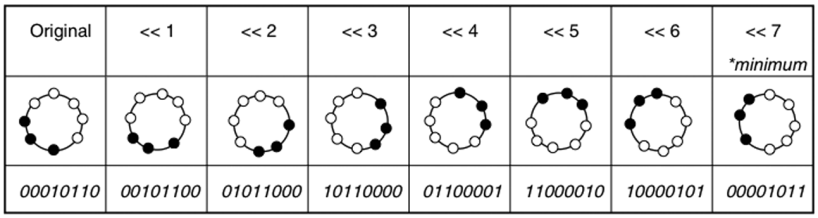


Slika 29. LPB metoda (Pietikäinen et al., 2011.)



Slika 30. Usporedba histograma tekstura slike LBP metodom (Pietikäinen et al., 2011.)

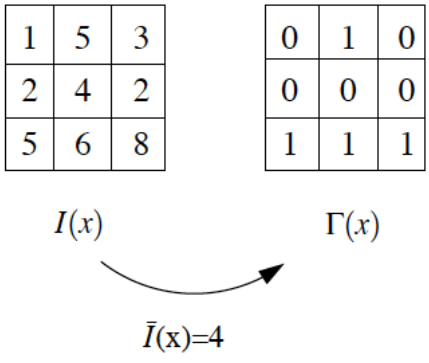
Iz LPB metode razvijaju se i različite poboljšane verzije metode (ILBP, LTP, TPLBP, FPLBP i dr.), među kojima je značajnija RILBP metoda (engl. *rotation invariant LBP*), koju karakterizira robusnost na modifikacije rotacijom. Primjer je dan na slici 31.



Slika 31. ILBP metoda i invarijantnost na rotaciju (Pietikäinen et al., 2011.)

6.3. Metoda modificirane cenzus transformacije

Metoda koju su Zabih i Woodfill (Zabih i Woodfill, 1996.) nazvali modificiranom cenzus transformacijom (engl. *Modified Census trasform* (MCT)) pokušala je unaprijediti metodu cenzus transformacije. Metoda upotrebljava usporedbu intenziteta svakog piksela unutar 3 x 3 bloka na način da ih uspoređuje s prosječnom vrijednošću intenziteta svih piksela iz strukture kernel. Na temelju usporedbe je li intenzitet piksela veći od prosječnog intenziteta ($\bar{I}(x)$) ili nije, generira se binarni vektor. Binarni vektor može se izračunati za svaki piksel unutar bloka uključujući i centralni piksel što daje 9-bitni cenzus potpis (slika 32.).

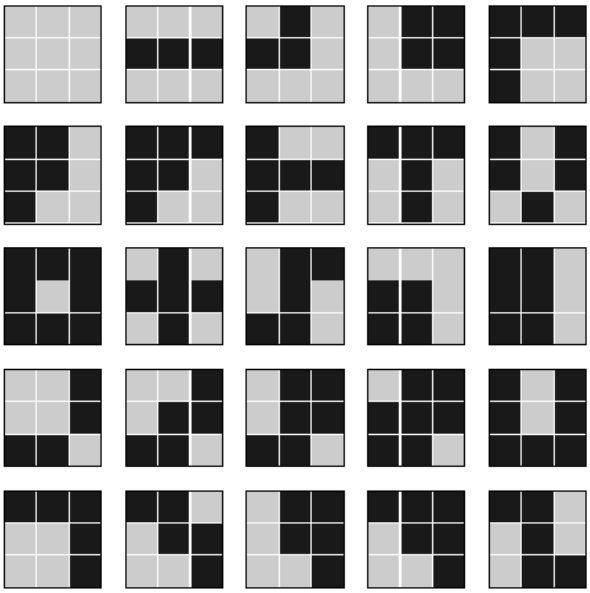


Slika 32. Generiranje binarnog vektora MCT metodom (Just et al, 2006.)

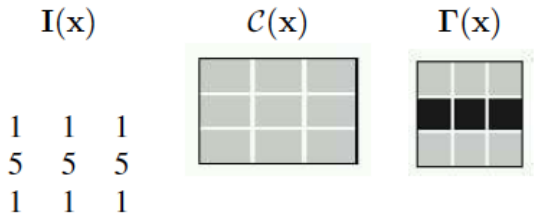
Modificirana cenzus transformacija ($\Gamma(x)$) matematički se može opisati na sljedeći način: neka je s $\mathcal{N}'(x)$ definirana okolina piksela x za koju vrijedi $\mathcal{N}'(x) = \mathcal{N}(x) \cup x$. Prosječna vrijednost intenziteta definira se kao $\bar{I}(x$. Tada je modificirana cenzus transformacija $\Gamma(x)$ jednaka (Froba i Ernst, 2004.):

$$\mathbf{\Gamma}(\mathbf{x}) = \bigotimes_{\mathbf{y}\in\mathcal{N}'} \zeta(\bar{\mathbf{I}}(\mathbf{x}),\ \mathbf{I}(\mathbf{y})).$$

Kako je prikazano na slici 33., ishod metode modificirane cenzus transformacije može ovisiti o mogućim uzorcima bloka 3 x 3 piksela, odnosno o njihovim varijacijama (2^9 -1) što ukupno čini 511 mogućih uzoraka, za razliku od metode cenzus transformacije, kojom je moguće generirati samo 2^8 odnosno 256 uzoraka zbog izostavljanja centralnog piksela. Uzorak omogućuje bolje prepoznavanje linija, rubova ili kutova u slici. Takvim pristupom moguće je generirati unikatne cenzus potpise. Istraživanja su pokazala poboljšanja u prepoznavanju određenih objekata na slici u odnosu na metodu cenzus transformacije (slika 40.) Na slici 34. prikazano je da se metodom cenzus transformacije $C(x)$ ne može prepoznati linija u drugom retku bloka, što nije prepreka metodi modificirane cenzus transformacije $\Gamma(x)$.

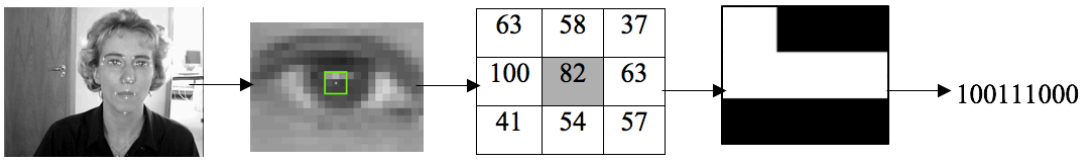


Slika 33. MCT za 25 od 511 mogućih kombinacija uzoraka za blok 3 x 3 piksela (Froba i Ernst, 2004.)



Slika 34. Primjer usporedbe CT i MCT metode
(Froba i Ernst, 2004.)

U trećoj se fazi primjenom prethodno opisane metode modificirane cenzus transformacije dobije cenzus potpis za svaki blok 3 x 3 oko biometrijske točke što je prikazano na slici 35. Cenzus potpis u ovom je slučaju jedna vrsta binarnog ograničavanja pragom (engl. *thresholding*) gdje se vrijednosti gradijenta piksela manje od $\bar{I}(x)$ preslikavaju u binarnu vrijednost 0, a veće vrijednosti u binarnu vrijednost 1. Segmentacija s pomoću praga predstavlja grupu metoda temeljenih na usporedbi osvjetljenosti piksela. Njegova je osnovna primjena odvajanje objekta od pozadine ako pozadina ima ujednačenost osvjetljenost koja se razlikuje od objekta. Ovakav način segmentacije može se primijeniti na primjer kod izdvajanja pisanog ili tiskanog teksta, analize nekih biomedicinskih slika, prepoznavanja tipa zrakoplova koji leti itd. (Lazarević, 2014.). Svi cenzus potpisi odabranih biometrijskih točaka na kraju se spoje u konačni percepcijski sažetak u binarnom obliku. Potrebno je napomenuti i da dužina konačnog percepcijskog sažetka ovisi o broju biometrijskih točaka te da se svaka regija oko biometrijske točke opisuje 9-bitnim binarnim cenzus potpisom.



$\bar{I}(x)$=61,6667

Slika 35. Izrada cenzus potpisa regije oko biometrijske točke s pomoću metode modificirane cenzus transformacije

Koraci u novorazvijenom algoritmu (MCT algoritam) jesu:

1. pretprocesiranje ulazne slike (pretvaranje u intenzitetsku sivu sliku (engl. *grayscale*), filter zamagljivanja)
2. odabir lokacija i redoslijeda biometrijskih točaka (tajni ključ *K*),
3. izdvajanje vrijednosti atributa iz regije, odnosno devet blokova s 3 x 3 piksela oko centralnog piksela jedne biometrijske točke (81 piksel),
4. provjera integriteta za svaku biometrijsku točku, odnosno provjera je li srednja vrijednost gradijenta pojedinog bloka $\bar{I}(x)$=0,
5. binarno ograničavanje metodom modificirane cenzus transformacije ovisno o tome je li vrijednost gradijenta 3 x 3 bloka veća ili manja od srednje vrijednosti svih blokova $\bar{I}(x)$ i izrada 9-bitnog binarnog cenzus potpisa za svaku biometrijsku točku,
6. spajanje svih pojedinačnih cenzus potpisa u konačni percepcijski sažetak.

7. VREDNOVANJE ALGORITAMA ZA IZRADU PERCEPCIJSKIH SAŽETAKA

Prema Bloomu (Bloom, 1956.) evaluacija ili vrednovanje je prosuđivanje vrijednosti za neku svrhu. Prosuđivanje se temelji na upotrebi kriterija i standarda, a može biti kvalitativno i kvantitativno.

Vrednovanje se sastoji se od triju etapa. U prvoj etapi određuju se kriteriji učinkovitosti, u drugoj etapi mjere se rezultati dovođenjem u odnos s utvrđenim kriterijima, a u trećoj se etapi uzročno-posljedičnom analizom otklanjaju uočeni nedostaci.

Vrednovanje se u mnogim sustavima provodi s pomoću povratnih informacija koje pokazuju odstupanje od planiranoga. Za postizanje učinkovitog i pouzdanog vrednovanja korisnicima treba sustav koji će ih obavijestiti u kojem bi se sljedećem trenutku mogao pojaviti neki problem u slučaju da odmah ne poduzmu određene mjere (Bloom, 1956.).

Postoje mnoge druge slične definicije i objašnjenja vrednovanja (evaluacije) u literaturi. Iako se svaka definicija i svako objašnjenje donekle razlikuju, postoji nekoliko razloga za primjenu vrednovanja koji su zajednički svima:

(1) dobivanje povratnih informacija,

(2) uspoređivanje dobivenoga i očekivanoga,

(3) mjerenje i prosuđivanje (vrednovanje) rezultata,

(4) poboljšanje i praćenje novih zamisli,

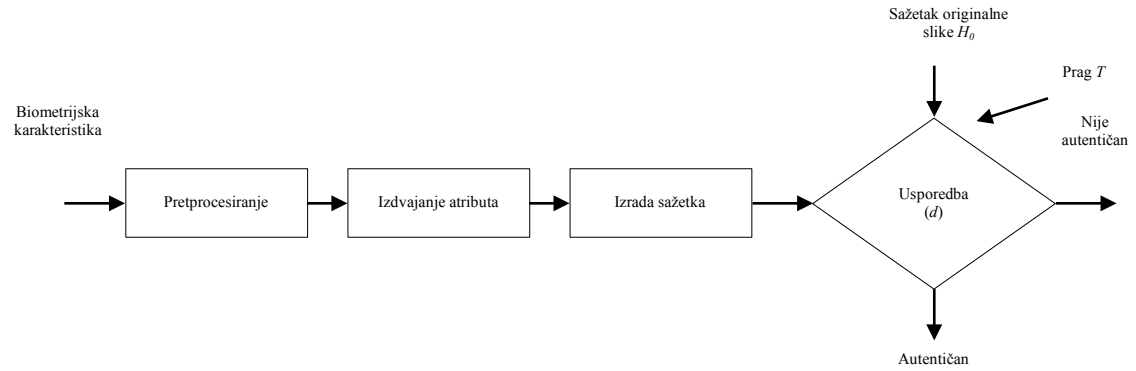
(5) prepoznavanje novih zamisli – prognostika.

7.1. Istraživanje

Kako je već spomenuto, cilj ove disertacije jest razviti novi algoritam za izradu percepcijskih sažetaka, koji se temelji na izdvajanju lokalnih atributa biometrijskih karakteristika metodom modificirane cenzus transformacije (MCT) te njegovo vrednovanje robusnosti i točnosti u odnosu na do sada najčešće korištene algoritme radi ispitivanja njegove primjene u biometrijskim sustavima autentikacije. Upravo radi postavljenog cilja i testiranja hipoteze, faze u istraživanju su uključivale: razvoj novog algoritma (MCT), implementaciju svih percepcijskih sažetaka pomoću opisanih algoritama te na kraju njihovu usporedbu, odnosno vrednovanja robusnosti i točnosti (tablica 2.). Razvoj i implementacija algoritama za izradu, usporedbu i vednovanje algoritama percepcijskih sažetaka bile su izvedene u MATLAB (MATrix LABoratory) programskom alatu za izračun i vizualizaciju na računalu sa i5 procesorom i 8Gb RAM memorije.

Tablica 2. Faze u istraživanju

Dizajn novog i implementacija postojećih algoritma	**Usporedba percepcijskih sažetaka**	**Vrednovanje algoritama**
Pretprocesiranje	Mjerenje sličnosti (normalizirana Hammingova udaljenost, Damerau-Levenshtein)	Test robusnosti
Izdvajanje atributa	Odluka o autentičnosti ($d<T$, $d>T$)	Test točnosti
Izrada sažetka		



Slika 36. Prve dvije faze u istraživanju

Kako je već ranije u disertaciji spomenuto, istraživanje će se provesti radi provjere mogućnosti primjene percepcijskih sažetaka u biometrijskim sustavima autentikacije. Autentikacija u biometriji označava usporedbu (1 : 1), odnosno pohranjeni predložak uspoređuje se s prikupljenim uzorkom na senzoru te se na temelju postavljenog praga (engl. *treshold*) odlučuje o autentičnosti korisnika. Što je veće podudaranje, veći je i rezultat podudaranja (engl. *match score*). Ako rezultat prijeđe prag, odnosno postavljenu numeričku vrijednost podudaranja sa predloškom, osoba je označena kao autentična. Određivanje praga ovisi o samoj primjeni sustava, ali općenito biometrijski sustavi autentikacije zahtjevaju veće podudaranje radi postizanja veće sigurnosti u prepoznavanju korisnika. U slučaju biometrijske identifikacije kod koje se provjerava nalazi li se korisnik u bazi ili ne, usporedba je (1:N) odnosno uzorak se uspoređuje sa svim pohranjenim predlošcima u bazi, te prag obično nije postavljen visoko.

Percepcijski sažetci, da bi bili upotrebljivi u takvim sustavima, trebali bi pokazati dvije osobine – robusnost na manipulacije koje uzrokuju promjene na slici koje bi onemogućile diskriminaciju kod njihove usporedbe te osjetljivost na napade modifikacijom kojima će se promijeniti sadržaj slike odnosno narušiti integritet. Primjenom manipulacija trebali bi biti sposobni prepoznati slične slike, a primjenom modifikacija trebali bi moći uočiti promjene. Isto tako, morali bi točno moći razlikovati dvije potpuno različite slike odnosno

omogućiti diskriminaciju. U istraživanju to će se ispitivati testom robusnosti i testom točnosti dalje opisanom u radu.

7.1.1. Istraživačke pretpostavke

Kod postojećih algoritama, analizom rada algoritama i analizom literature (Zauner, 2010., Hadmi et. al., 2012., Kozat et al., 2004., Weng et al., 2012.), a kod novorazvijenog MCT algoritma predistraživanjem, vezano za napade, krenulo se od nekoliko istraživačkih pretpostavki. Od ukupno šest opisanih algoritama koji se temelje na različitim i u disertaciji ranije opisanim metodama, četiri analiziraju globalne atribute slika, a samo dva (uključujući i novorazvijeni algoritam) analiziraju lokalne atribute slika. Pretpostavka je bila da će algoritmi koji analiziraju lokalne atribute slika biti precizniji u odnosu na algoritme koji u svom radu koriste globalne atribute slika kod malicioznih napada jer će bolje uočavati promjene na slikama. Istovremeno nedostatak algoritama koji analiziraju globalne atribute može biti i ne uočavanje promjena manjih vrijednosti parametara u negeometrijskim napadima. Isto tako, algoritmi koji analiziraju lokalne atribute slika trebali bi pokazivati bolje rezultate jer analiziraju manji broj atributa na slici za razliku od algoritama koji u svom radu koriste globalne atribute slika jer oni analiziraju i atribute koji nisu od velike važnosti za utvrđivanje sličnosti, a koji se smatraju viškom (npr. pozadina). Nadalje, algoritmi koji u svom radu koriste i analiziraju vrijednost intenziteta boje (kao što je i novorazvijeni MCT algoritam) mogli bi imati problema kod negeometrijskih napada kao što je šum, pogotovo ako u fazi pretprocesiranja ne koriste filtere. Slično je i sa algoritmima koji temelje se na izdvajanju atributa s pomoću otkrivanja elemenata kao što su rubovi, kutovi ili krivulje u slici. Tu bi algoritmi koji analiziraju frekvencije u slikama trebali imati bolje rezultate. Isto tako, analizom literature, uočeno je da postojeći algoritmi nisu robusni na geometrijske napade, što je važna značajka za autentikaciju u biometrijskim sustavima.

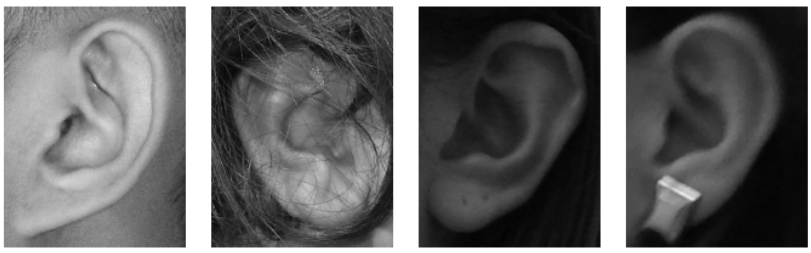
7.1.2. Podaktovni skup

U istraživanju su korištene tri biometrijske karakteristike – lice, uho i statički potpis. Ove karakteristike odabrane su radi nekoliko razloga. Prvi razlog je aktualnost istraživanja tih biometrijskih karakteristika radi autentikacije korisnika ne samo u biometrijskim sustavima nego na primjer i u sustavima prepoznavanja korisnika mobilnih uređaja (Oravec M. et al., 2016.). Prema istraživanju Biometrics Institute (Biometrics Institute, 2015.) upotreba biometrijskih karakteristika u autentikaciji korisnika mobilnih uređaja poput pametnih telefona ili tableta u velikom je porastu. Drugi razlog je što se one u biometrijskim sustavima klasificiraju kao fizičke (lice i uho) i ponašajne (statički potpis), s time da lice spada u biometrijske karakteristike koje se mijenjaju tijekom vremena, a uho i statički potpis se ne mijenjaju tijekom vremena što može utjecati na atribute za izradu percepcijskih sažetaka. Treći razlog je što se biometrijske karakteristike lica i uha mogu kombinirati u multimodalnim biometrijskim sustavima ili kod autentikacije na mobilnim uređajima (Napi M. et al., 2017.). Četvrti razlog je različita složenost i količina atributa u uzorcima odnosno digitalnim slikama biometrijskih karakteristika. Iz biometrijske karakteristike lica može se izdvojiti najveća količina atributa za analizu, dok kod biometrijske karakterstike statičkog potpisa ta količina najmanja. Isto tako, zbog različitih utjecaja, koji su opisani kasnije u disertaciji, biometrijska karakteristika lica ima promjenjivije odnosno nestabilnije atribute u odnosu na biometrijsku karakteristiku uha ili potpisa.

Kod biometrijske karakteristike lica koristila se znanstvena baza BioID, koja se nalazi na *web*-sjedištu https://www.bioid.com/About/BioID-Face-Database. Baza je namijenjena znanstvenicima koji se bave algoritmima za detekciju lica te je pogodna za ispitivanje i komparaciju algoritama. Testni set u bazi prikupljen je u stvarnim situacijama i različitim uvjetima kao što su osvjetljenje, poza, pozadina i veličina. Baza sadržava 1521 sliku s rezolucijom 384 x 286 piksela. Svaka slika prikazuje frontalni pogled na lice jedne od 23 različitih osoba.

Kod biometrijske karakteristike uha koristila se javno dostupna biometrijska baza WPUT-DB (WPUT-DB Biometrics Ear Database). Baza sadržava 2071 sliku karakteristike uha prikupljenu od 501 različite osobe svih godina. Za svaku osobu prikupljeno je od četiri do

osam slika uha uzetih različitim danima, u različitim uvjetima osvjetljenja i s dodanim nakitom. Primjeri slika iz baze WPUT-BD prikazani su na slici 37.



Slika 37. Primjeri uzoraka uha iz baze WPUT-DB

Testirani uzorci biometrijske karakteristike statičkog potpisa dio su testnog seta biometrijske baze ICFHR 4NsigComp s natjecanja forenzičke verifikacije potpisa iz 2012. godine (ICFHR 4NsigComp). Cilj natjecanja bila je procjena učinkovitosti automatiziranih procesa prepoznavanja originalnih i krivotvorenih potpisa osoba. Baza sadržava 79 originalnih i 194 krivotvorena potpisa.

U fazi vrednovanja algoritama, odnosno pri testu robusnosti koristio se testni set sastavljen od originalne biometrijske karakteristike iz opisanih baza, te njezinih deformiranih verzija (*intra* set) za svaki korišteni napad što je opisano ispod u tekstu. Ukupno se u istraživanju napravilo 882 percepcijska sažetka i njihove usporedbe.

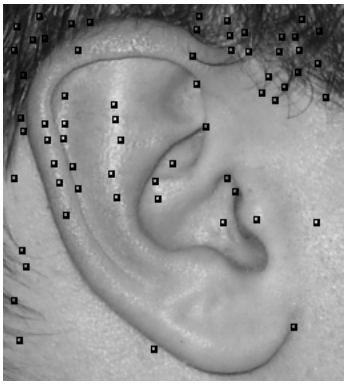
7.1.3. Implementacija algoritama

U istraživanju se novorazvijeni MCT algoritam uspoređivao sa još 5 algoritama koji se u literaturi označavaju kao standardni najčešće korišteni ("*state of the art*") algoritmi. Sljedeći algoritmi upotrijebljeni su u istraživanju: algoritam temeljen na metodi diskretne kosinusove transformacije (DCT ili pHash) (Zeng, 2013.), algoritam temeljen na metodi diskretne wavelet transformacije (DWT) (Venkatesan et al., 2000.), algoritam temeljen na detekciji točaka vizualno značajnih atributa (VFPH) (Monga i Evans, 2006.), algoritam temeljen na Marr-Hildreth metodi (Zauner, 2010.) i algoritam temeljen na metodi prosječne vrijednosti bloka (engl. Block Mean Value) (Yang et al., 2006.).

Iako su u poglavlju 2. navedeni algoritmi detaljno teorijski opisani, u tablici ispod će se ukratko opisati njihova implementacija kroz faze pretprocesiranja i izdvajanja atributa navedenih slika biometrijskih karakteristika da bi se dobio konačni percepcijski sažetak svake slike potreban za daljnu fazu istraživanja odnosno uporedbu percepcijskih sažetaka. Vrijednosti parametara u svakoj fazi preuzete su iz navedenih radova radi bolje usporedivosti rezultata sa novorazvijenim algoritmom.

Kako se već napomenulo razvoj novog i implementacija algoritama za izradu, usporedbu i vednovanje algoritama percepcijskih sažetaka napravljen je u MATLAB (MATrix LABoratory) programskom okruženju za izračun i vizualizaciju na računalu sa i5 procesorom i 8Gb RAM memorije. Implementacija algoritma temeljenog na metodi diskretne wavelet transformacije (DWT) i algoritma temeljenog na detekciji točaka vizualno značajnih atributa (VFPH) napravljena je prema primjeru MATLAB alata Image Hashing Toolbox kojeg je moguće naći na poveznici http://users.ece.utexas.edu/~bevans/projects/hashing/toolbox/index.html. Za obradu slika korišten je alat i funkcije u sklopu MATLAB dodatka Image Processing Toolbox.

Pretprocesiranje je dio svakog algoritma korištenog u istraživanju. Općenito, namjena pretprocesiranja je priprema slika radi izdvajanja što kvalitetnijih atributa za percepcijski sažetak. Iako neki od opisanih algoritama (Marr Hildreth) uključuju i neke posebne operacije kao što je *uporaba filtera* da bi poboljšali izdvajanje atributa u slučajevima pojave šumova ili zamagljivanja kod slika, svi algoritmi su uključivali operacije: *smanjenje dimenzijalnosti boje* odnosno pretvaranje u sivu intenzitetsku (engl. *grayscale*) sliku - da bi se olakšalo računanje kod izdvajanja atributa odnosno da bi transformacija bila brža i efikasnija; *promjena veličine* - također da bi se olakšalo računanje kod izdvajanja atributa te u nekim algoritmima postigla bolja otpornost kod promjena omjera visine i širine slike.



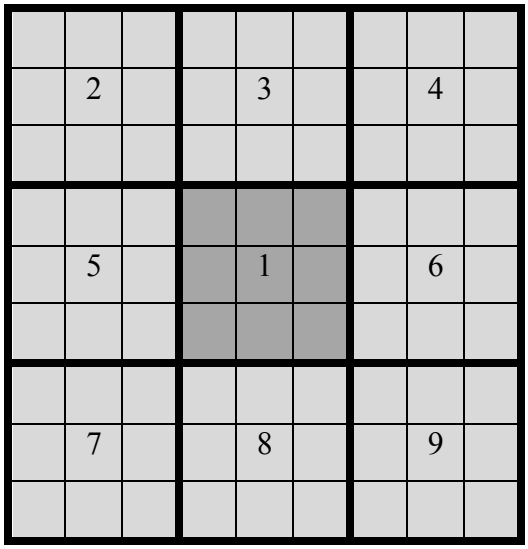
Slika 38. Izdvajanje lokalnih atributa na uzorku
biometrijske karakteristike uha s pomoću MFVP algoritma

Tablica 3. Implementacija algoritama sa vrijednostima parametara

Algoritam (implementacija prema radu)	**Pretprocesiranje**	**Izdvajanje atributa**	**Izrada percepcijskog sažetka**	**Veličina percepcijskog sažetka**
DCT (Zeng, 2013.); (Krawetz, 2011.)	veličina 32x32 piksela; siva intenzitetska slika (engl. *grayscale*)	DCT transformacija – blok u gornjem-lijevom kutu 8x8 piksela	$h_i = \begin{cases} 0, C_i < m \\ 1, C_i \geq m \end{cases}$	64 bita
MH (Zauner, 2010.)	siva intenzitetska slika (engl. *grayscale*); Canny-Deriche filter (1.0)	Laplacian of Gaussian (LoG) ($\sigma = 2$)	Normalizacija slike (0-1); binarno ograničavanje pragom T	72 bita
BMV (Yang et al., 2006.); (Zauner, 2010.)	siva intenzitetska slika (engl. *grayscale*); veličina 192x192 piksela	blokovi – 16x16 piksela; medijan intenziteta slike; srednja vrijednost intenziteta bloka	$h(i) = \begin{cases} 0\,, M_i < M_d \\ 1\,, M_i \geq M_d \end{cases}$	144 bita
MFVP (Monga i Evans, 2006.)	siva intenzitetska slika (engl. *grayscale*); veličina 256x256 piksela	traženje preklapajuće pravokutne regije – 64 točaka atributa; *wavelet* transformacija; traženje maksime	binarizacija vektora detektiranih atributa; tajni ključ K	64 bita

DWT (Venkatesan et al., 2000.)	siva intenzitetska slika (engl. *grayscale*); veličina 256x256 piksela	DWT dekompozicija; tajni ključ *K* podijela na pravokutnike *M=150;* određivanje vektora atributa	kvantizacija vektora; binarizacija sažetka Reed-Mullerovim dekoderom grešaka $h = D(x) \in \{0,1\}^n$	150 bita
MCT (novorazvijeni algoritam)	siva intenzitetska slika (engl. *grayscale*); Gaussov filter (1.0)	Određivanje lokacija biometrijskih točaka; tajni ključ *K*; ROI sa 9 blokova (3x3 piksela) oko svake biometrijske točke	binarno ograničavanje blokova $\bar{I}(x)$ metodom modificirane cenzus transformacije	ovisno o biometrijskoj karakteristici i broju biometrijskih točaka; 9 bitni cenzus potpis (180 bitova lice, 108 bitova uho i 108 bitova potpis)

Za MCT algoritam treba se napomenuti da se upotrebom bloka od 3 x 3 piksela ne mogu obuhvatiti relevantni atributi dovoljno precizni za autentikaciju regije. Iz tog razloga u disertaciji je za izradu cenzus potpisa upotrijebljena regija s više blokova oko biometrijske točke. Umjesto bloka od 3 x 3 piksela oko centralne biometrijske točke upotrijebljena je regija od devet blokova veličine 3 x 3 piksela, odnosno svaka biometrijska točka opisana je s pomoću 81 vektora atributa (slika 39.). Za izradu 9-bitnog cenzus potpisa gradijent pojedinog bloka uspoređivao se s prosječnom vrijednošću gradijenta svih blokova. Kod biometrijske karakteristike lica s 20 odabranih točaka duljina percepcijskog sažetka iznosi 180 bitova, odnosno 20 točaka s 9 bitova za cenzus potpis jedne točke. Kod biometrijske karakteristike uha i biometrijske karakteristike potpisa duljina konačnog percepcijskog sažetka iznosi 108 bitova.



Slika 39. Regija od devet blokova (3 x 3 piksela) za svaku biometrijsku točku

7.1.4. Određivanje lokacija atributa kod novorazvijenog MCT algoritma

S obzirom na to da novi MCT algoritam izdvaja i analizira lokalne atribute interesnih regija slika odnosno biometrijskih karakteristika oko biometrijskih točaka, prije testa robusnosti potrebno je posebno opisati u vrednovanju korištene atribute za svaku biometrijsku karakteristiku posebno zbog specifičnosti određivanja istih.

7.1.4.1. Određivanje lokacija atributa na uzorcima biometrijske karakteristike lica

Označavanje lokacija točaka na svakoj slici u bazi bio je dio projekta FGnet (Crowley – FGnet) te su iste ručno označene prema stvarnim obilježjima osoba značajnima za detekciju lica. Lice svake osobe na slikama u bazi označeno je s 20 karakterističnih točaka kako je prikazano na slici 40. Označavanje počinje s lokacijom zjenice oka, a završava s lokacijom vrha brade.

Slika 40. Označene biometrijske točake lica u BioID bazi (Crowley – FGnet)

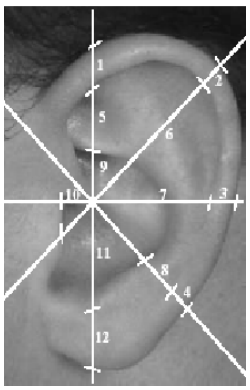
Lokacije su označene pozicijom *x* i *y* u koordinatnom sustavu te su spremljene u tekstualnu datoteku čiji je ispis prikazan na slici 41.

version: 1
n_points: 20
{
159.128 108.541
230.854 109.176
164.841 179.633
223.237 178.998
132.469 93.9421
183.883 94.5768
211.177 95.2116
254.974 91.4031
129.295 109.176
144.529 109.811
176.901 107.272
216.89 107.272
246.088 110.445
261.957 109.811
196.578 139.009
184.518 147.261
207.369 145.991
195.943 175.189
193.404 193.597
192.769 229.143
}

Slika 41. Izgled datoteke s koordinatama (x,y) označenih biometrijskih točaka lica u bazi BioID

7.1.4.2. Određivanje lokacija atributa na uzorcima biometrijske karakteristike uha

Iako kod uha, kao i kod biometrijske karakteristike lica, postoji velik broj algoritama za određivanje lokacija točaka koje se upotrebljavaju u autentikaciji, a opisane su u brojnim radovima Jaina i suradnika (Jain et al., 2008.), za potrebe ove disertacije primijenjena je metoda koju je razvio i opisao Iannarelli (Abaza et al., 2013.). Metoda se temelji na antropometriji uha, odnosno na ručnom određivanju 12 oznaka (Iannarellijev sustav) na 2D slikama uha što je prikazano na slici 42. u nastavku. Uho se podijeli na osam dijelova iscrtavanjem pravaca (okomito, vodoravno i pod kutom od 45 °) koji sjecište imaju u točki na vrhu targusa uha. Na mjestima gdje se nalazi sjecište tih pravaca i linija vanjskih dijelova uha, postavi se oznaka. Budući da se tijekom vremena uho znatno ne mijenja, Iannarellijeva metoda smatra se pouzdanom i dugi se niz godina upotrebljava u forenzici i biometrijskim sustavima.



Slika 42. Označavanje uha Iannarellijevom metodom (Abaza et al., 2013.)

Primjer određivanja lokacija i označavanje lokacija atributa u alatu MATLab dan je u kodu 7.1.

```
figure;
imshow(I);
hold on
[cx,cy]=ginput(1)
r=400
pos = [cx-r+1 cy-r+1 r*2 r*2];
rectangle('Position',pos,'Curvature',[1 1]);
x1 = [-r, 0, -r*cosd(45), -r*cosd(45); r, 0, r*cosd(45), r*cosd(45)]+cx+1;
y1 = [0, -r, -r*sind(45), r*sind(45); 0, r, r*sind(45), -r*sind(45)]+cy+1;
plot(x1,y1,'Color','r');
[x,y]=ginput(12)
plot(x,y,'+','MarkerEdgeColor','w')
```

Kod 7.1. Određivanje lokacija atributa na uzorcima biometrijske karakteristike uha – implementacija u alatu MATLab

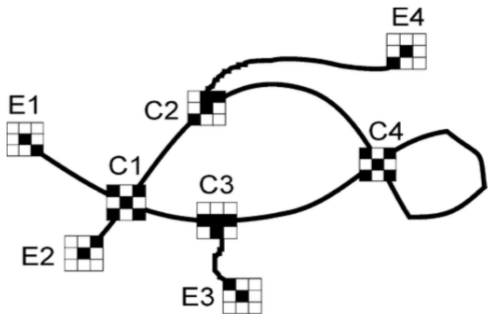
7.1.4.3. Određivanje lokacija atributa na uzorcima biometrijske karakteristike potpisa

Kod biometrijske karakteristike potpisa razlikuju se statički i dinamički potpisi. Prvi analiziraju digitaliziranu sliku potpisa s papira te ne zahtijevaju da osoba bude fizički prisutna u trenutku autentikacije, dok drugi zahtijevaju potpis u stvarnom vremenu koji se daje s pomoću digitalnog uređaja (npr. tableta i specijalne olovke) što znači da osoba mora biti prisutna u trenutku autentikacije.

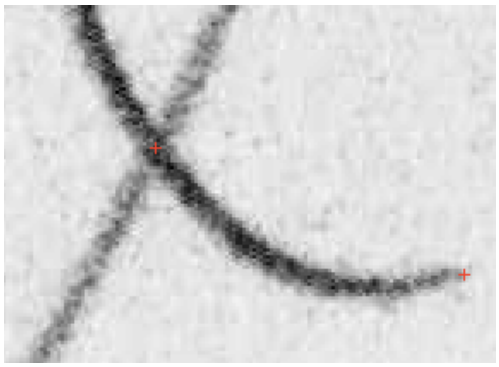
Atributi kod statičkih potpisa odnose se na samu geometriju potpisa, dok dinamički sadržavaju atribute kao što su geometrija potpisa, brzina, putanja, nagib, jačina pritiska i sl.

U istraživanju percepcijskih sažetaka biometrijske karakteristike potpisa lokacije točaka određene su atributom poteza. Potez je definiran kao neprekidna linija povučena od trenutka kada osoba spusti olovku na površinu (papir) do trenutka kada digne olovku s površine. Iako je atribut broja poteza i broja podizanja olovke karakterističan za dinamičke biometrijske karakteristike potpisa, u disertaciji se upotrijebljava radi vizualne uočljivosti. Osim početne i završne točke poteza u određivanju ostalih lokacija točaka, za izradu percepcijskih sažetaka primjenjuje se metoda koju su opisali Baltzakis i Papamarkos

(Baltzakis i Papamarkos, 2001.), odnosno u obzir se uzimaju i lokacije presjecanja linija poteza (engl. *crossover*) (slika 43.)



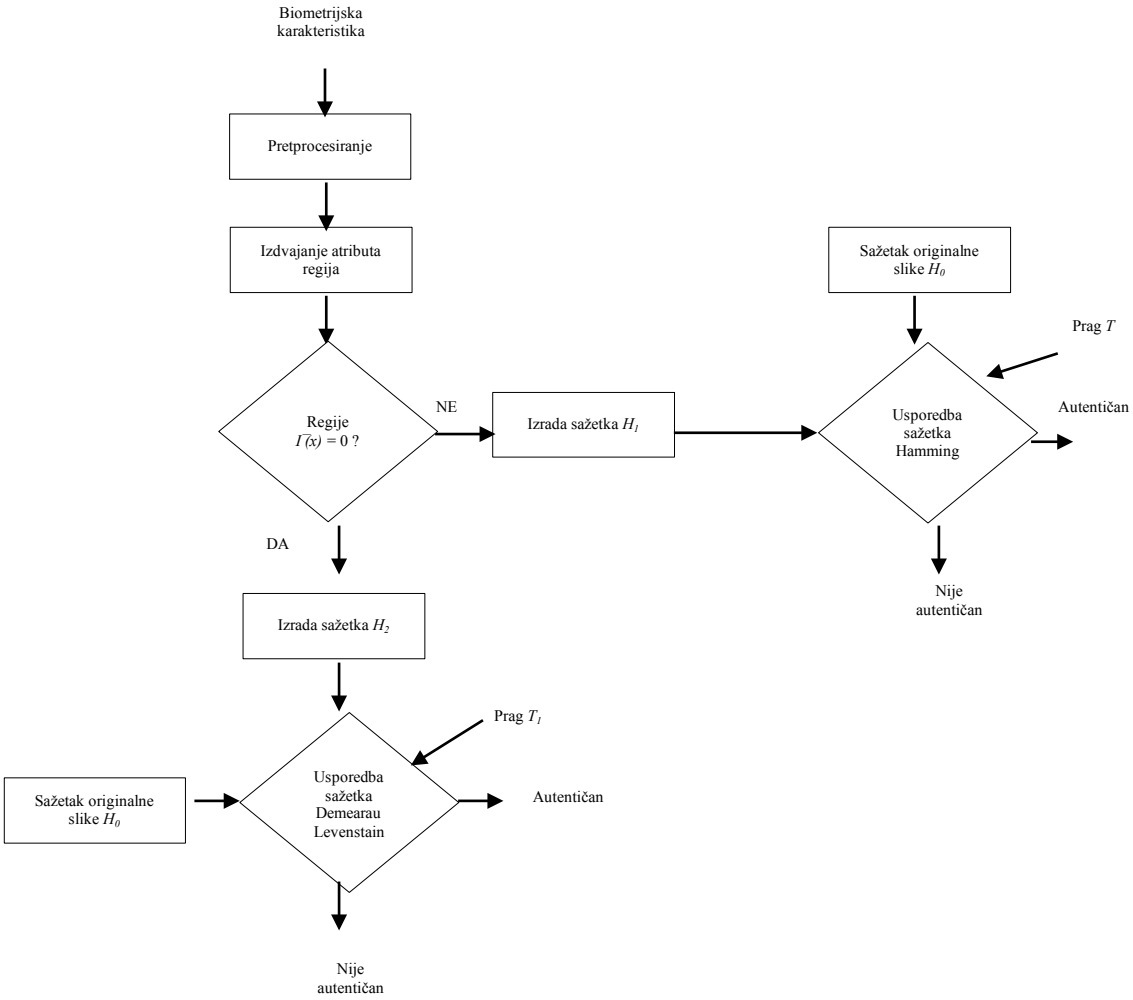
Slika 43. Određivanje lokacija atributa biometrijske karakteristike potpisa (Baltzakis H., Papamarkos, 2001.)



Slika 44. Određivanje točaka za izradu percepcijskog sažetka biometrijske karakteristike potpisa na kraju i presjecištu linija poteza

7.1.5. Dodatne faze u istraživanju za novorazvijeni MCT algoritam

Potrebno je istaknuti da je tijekom vrednovanja uočena jedna za algoritme za izradu percepcijskih sažetaka specifična, a za biometrijske sustave uobičajena situacija, koja se opisuje u sljedećem poglavlju, a to je nedostatak atributa za analizu u odnosu na originalnu sliku. Takvi su uzorci u biometrijskim sustavima odbačeni zbog loše kvalitete, a kod algoritama za izradu percepcijskih sažetaka dijelovi koji nedostaju označeni su kao prazan prostor (nula) što dovodi do netočnih rezultata pri njihovoj usporedbi.



Slika 45. Dodatne faze u vrednovanju novorazvijenog MCT algoritma

U novorazvijenom algoritmu taj problem može se riješiti tako da se ispitivanjem prosječne vrijednosti gradijenta bloka može uočiti nedostatak atributa oko pojedine biometrijske točke te takve regije označiti kao obrisane (slika 45.). U tom slučaju percepcijski sažetak moguće je izraditi bez tih regija, samo što je tada rezultat manja duljina sažetka. Budući da svi algoritmi za izradu percepcijskog sažetka opisani u disertaciji upotrebljavaju Hammingovu udaljenost kao metodu za mjerenje sličnosti, usporedba takvih sažetaka različite duljine ne bi bila moguća. Hammingova udaljenost mjeri udaljenost odnosno različitost elemenata samo kada se uspoređuju dva sažetka jednake duljine. Damerau-Levenshteinovom udaljenošću (engl. *Damerau-Levenshtein distance*) mogu se mjeriti sažetci različite duljine što je opisano i u poglavlju 4.2. ove disertacije. Pritom se javlja potreba za uvođenjem drugog praga T_1, kojim se određuje prihvatljiva vrijednost udaljenosti između dvaju percepcijskih sažetaka koji nisu jednake duljine. Prednosti takvog pristupa opisane su i vidljive na rezultatima u sljedećem poglavlju, kod napada brisanjem na biometrijske uzorke biometrijskih karakteristika.

7.2. Test robusnosti

Robusnost će se definirati kao mjera otpornosti algoritma na male, namjerne promjene atributa odnosno manipulacije i modifikacije nad digitalnim slikama. Dobar algoritam za percepcijski sažetak trebao bi biti robusan na takve napade. Ispitivanje robusnosti provodi se kako bi se odredilo kako male promjene testnih uvjeta utječu na rezultat. Važan su dio razvoja algoritma jer pomažu otkriti optimalne uvjete izvedbe te upućuju na to što je potrebno nadzirati. Tijekom testiranja mijenjaju se testni uvjeti unutar granica i prati se kvantitativna promjena rezultata.

Test robusnosti odnosi se na usporedbu percepcijskih sažetaka originalnih slika s njihovim deformiranim slikama. Kao što se već istaknulo u uvodu disertacije, deformacija podrazumijeva manipulaciju i modifikaciju digitalne slike. Manipulacija predstavlja operaciju nad nekom slikom, kojom se ona vizulano ne mijenja. Nakon takvih operacija pretpostavlja se da se i percepcijski sažetak takve slike neće znatno promijeniti. Modifikacija predstavlja operaciju nad slikom, kojom se ista vizualno mijenja. Nakon takvih operacija pretpostavlja se da će se i percepcijski sažetak takve slike znatno promijeniti jer se takvim napadima mijenja sadržaj ili struktura odnosno atributi slike. Na taj način ispitat će se robusnost metode radi autentikacije slika, odnosno mjerit će se sličnost sa sažetkom originalne slike H_0 (1 : 1) uz postavljeni prag T (slika 44.). Manja vrijednost udaljenosti d prikazana u tablicama i grafikonima u nastavku predstavlja bolji rezultat. Što je rezultat bliže 0, slike su sličnije.

7.2.1. Napadi na biometrijske karakteristike

U nastavku disertacije opisuju se napadi, odnosno testni uvjeti u kojima se ispituje robusnost algoritma. Potrebno je napomenuti i da su ti napadi odabrani zato što se pojavljuju kao problem kod prepoznavanja i očitavanja uzoraka u biometrijskim sustavima kako je već ranije spomenuto u radu, a vrlo često ih koriste autori i u ispitivanju robusnosti algoritama za izradu percepcijskih sažetaka.

Napadi manipulacijom i modifikacijom u istraživanju podijeljeni su u tri kategorije - ***geometrijski, negeometrijski i zlonamjerni***, kako je prikazano u tablici 4.

Tako podijeljeni napadi trebali bi u vrednovanju testirati algoritme sa tri aspekta. Prvi aspekt je robusnost na negeometrijske napade. Negeometrijski napadi kao što je promijena svjetline ili kompresija ne bi trebali bitno utjecati na sličnost percepcijskih sažetaka s obzirom da se sadržaj slike ili struktura bitno ne mijenja. Negeometrijski napadi u biometrijskim sustavima često se javljaju kao problem pojave šumova na uzorcima pri očitanja na senzoru, pri kompresiji slika kod prijenosa komunikacijskim kanalom ili kod pohrane biometrijskih uzoraka u bazu. (Alaswad A. O. et al., 2014.). Isto tako mogu biti rezultat vanjskih utjecaja, kao što su vlaga, prljavština i temperatura, ili nemogućnosti fokusiranja kamere kod prikupljanja biometrijske karakteristike. Zbog toga, točnost biometrijskih sustava uvelike ovisi o osjetljivosti ulaznih prikupljenih uzoraka na senzoru. Loše prikupljeni uzorak rezultirati će smanjenom točnosti prepoznavanja (slika 46.).

Drugi aspekt je robusnost na geometrijske napade. Geometrijski napadi su zanimljivi jer se rotacijom ili translacijom, napadnuta slika ljudskom oku vizualno ne mijenja iako je njezina digitalna prezentacija promijenjena, a dosta su česti u biometrijskim sustavima. Na slici 46. vidljivo je i da zbog pomaka i rotacije biometrijske karakteristike prsta što predstavlja geometrijski napad, postoji otežano čitanje atributa za autentikaciju korisnika. Isto tako, zbog nedovoljnog pritiska prsta na senzor nedostaje dio atributa što predstavlja treću kategoriju napada – zlonamjerni napadi. Nedostatak atributa velik je problem u biometrijskim sustavima jer bi se takvi nepotpuni uzorci često odbacivali zbog nedovoljne kvalitete. Osim toga treći aspekt predstavljaju i zlonamjerni napadi kao što je namjerno brisanje ili dodavanje manjih i većih dijelova slike da se zavara biometrijski sustav. Takve napade, algoritmi bi trebali uspješno otkriti da bi bili upotrebljivi u autentikaciji.

Navedeni napadi korišteni su u testu robusnosti, a u biometrijskim sustavima javljaju se u svim dijelovima sustava od prikupljanja, prijenosa, obrade i pohrane biometrijskih karakteristika koji su opisani u poglavlju 5.

Slika 46. Otežano čitanje atributa zbog položaja i necjelovitosti biometrijske karakteristike (Jain A.K. et al., 2008.)

Ukupno je testirano 8 napada koji su prikazani u tablici 4. Za svaki napad označen je parametar odnosno vrijednost promjene u odnosu na originalnu sliku. Za sve biometrijske karakteristike (lice, uho i potpis) generirane su ukupno 882 deformirane slike prema vrijednosti parametra promjene napada u odnosu na originalnu sliku. Time se dobio tzv. *intra* set slika koje su uključene u test robusnosti. Kako su se u testu koristile slike 3 biometrijske karakteristike koje su deformirane sa ukupno 8 napada tako se kreiralo 3 *intra* setova slika sa po 294 slike – 1 originalna i 293 deformirane verzije. Na slici 47. ispod prikazan je dio *intra* seta od 6 slika biometrijske karakteristike lica u napadu svjetlinom sa vrijednostima parametara od – 30 % do + 30 % koje su se uspoređivale sa originalnom slikom. Za obradu slika odnosno promijenu vrijednosti svih napada korištene su funkcije u sklopu MATLAB alata Image Processing Toolbox.

Slika 47. *Intra* set slika deformiranih slika napadom svjetlinom na biometrijsku karekteristiku lica sa vrijednostima – 30 % do + 30 %

U tablicama u nastavku prikazane su *minimalne*, *maksimalne* i *prosječne udaljenosti* za sve biometrijske karakteristike u testu. Minimalne i maksimalne udaljenosti predstavljaju optimalni raspon vrijednosti parametra u kojem pojedini algoritam pokazuje robusnost na određene napade. Prosječna udaljenost može se uzeti kao vrijednost praga *T* za pojedini algoritam i određeni napad kod odluke o autentičnosti. Ako je udaljenost *d* dobivena usporedbom dvaju sažetaka manja od vrijednosti praga *T*, slike će biti označene kao autentične. Ako je udaljenost *d* veća od praga *T*, slike će biti označene kao neautentične. U tablicama je u zadnjem stupcu (+/-) također označena razlika vrijednosti rezultata novorazvijenog MCT algoritma u odnosu na najbolji rezultat do sada razvijenog algoritma u testu.

Ono što se mora istaknuti je da je kod testa robusnosti fokus na promjeni testnih uvjeta, a ne toliko na sam rezultat odnosno vrijednost udaljenosti *d.* Kako se već napomenulo, test robusnosti bi trebao pokazati otpornost testiranih algoritama na napade manipulacijom i modifikacijom sa različitim vrijednostima parametara napada. U takvim uvjetima test bi, kod dobrih algoritama trebao pokazati da je ponašanje algoritma dosljedno, da su odstupanja logična i u korelaciji s promjenama vrijednosti parametara napada ili da napad nema utjecaja na utvrđivanje sličnosti. U drugom slučaju, test će kod loših algoritama pokazati da ponašanje algoritma nije dosljedno u korelaciji s promjenama vrijednosti parametara ili da se ne može utvrditi sličnost kod slika bez obzira na prividno dobar rezultat.

Tablica 4. Napadi u testu robusnosti

Napad	Parametar/vrijednost	Kategorija napada
Svjetlina	- 30 % - + 30 %, 10 %	Negeometrijski
Gaussov šum	σ = 0 - 20, σ = 5	
Binarni šum (Salt&Pepper)	0 – 0,005, 0,001	
Kompresija	10 – 90 %, 10 %	
Rotacija	-30 % - 30 %, 10 %	Geometrijski
Translacija (vertikalno)	- 15- + 15 piksela, 5 piksela	
Skaliranje	90 – 10 %, 10 %	
Brisanje	1 – 4 bloka	Zlonamjerni

7.2.1.1. Negeometrijski napadi

Negeometrijski napadi predstavljaju napade koji ne mijenjaju strukturnu informaciju na slici, na primjer oblike, nego se odnose na smetnje u slici, npr. pojavu šumova ili na promjenu vrijednosti boje odnosno gradijenta. Za potrebe istraživanja odabrana su četiri takva napada: svjetlina, Gaussov šum, binarni šum (Salt&Pepper) i JPEG kompresija.

7.2.1.1.1. Napad svjetlinom

Podešavanje svjetline na slici jedna je od najčešćih i najjednostavnijih operacija. U testu su upotrijebljene vrijednosti od – 30 % do + 30 % u odnosu na postavke svjetline originalne slike. Iz dobivenih rezultata vidljivo je da su svi algoritmi robusni na promjene svjetline. Odstupanja u rezultatu od percepcijskog sažetka originalne slike su minimalna (0,0000 – 0,0999) za sve biometrijske karakteristike što označuje ispravno utvrđivanje sličnosti slika. Uočljivo je da rezultati algoritama ovise o testiranoj biometrijskoj karakteristici te da svi algoritmi nemaju dosljedno ponašanje. Promjene rezultata prema vrijednostima parametara nisu u korelaciji kod svih algoritama što je prikazano na slikama u nastavku. Najbolji primjer jesu algoritmi DCT, MH i DWT koji, iako su ispravno utvrdili

sličnost kod biometrijske karakteristike lica, nemaju dosljedno ponašanje i logična (očekivana) odstupanja kod malih promjena svjetline. Kod biometrijske karakteristike uha i potpisa njihovo je ponašanje konzistentno, a odstupanja su logična prema vijednostima parametara ili uopće nemaju utjecaj na rezultate što je prikazano na grafikonima 2. i 3. Najveću udaljenost (0,0999) pokazuje DWT algoritam kod biometrijske karakteristike uha za vrijednost parametra od + 20 % svjetline, a promjenom vrijednosti parametra za + 10 % (+ 30 % svjetline) pokazuje manju udaljenost (0,0836).

Tablica 5. Napad svjetlinom za biometrijsku karakteristiku lica s parametrom od – 30 % do + 30 %

Postotak	**DCT**	**VFPH**	**MH**	**BMV**	**DWT**	**MCT**
-30	0,0469	0,0159	0,0000	0,0000	0,0339	0,0056 **(-0,0056)**
-20	0,0469	0,0159	0,0000	0,0000	0,0286	0,0111 **(-0,0111)**
-10	0,0313	0,0159	0,0469	0,0000	0,0282	0,0111 **(-0,0111)**
0	0,0000	0,0000	0,0000	0,0000	0,0000	**0,0000**
10	0,0156	0,0159	0,0469	0,0000	0,0566	0,0111 **(-0,0045)**
20	0,0156	0,0159	0,0469	0,0312	0,0812	0,0056 **(-0,0111)**
30	0,0313	0,0159	0,0469	0,0625	0,0910	0,0111 **(+0,0048)**

Tablica 6. Napad svjetlinom

Lice

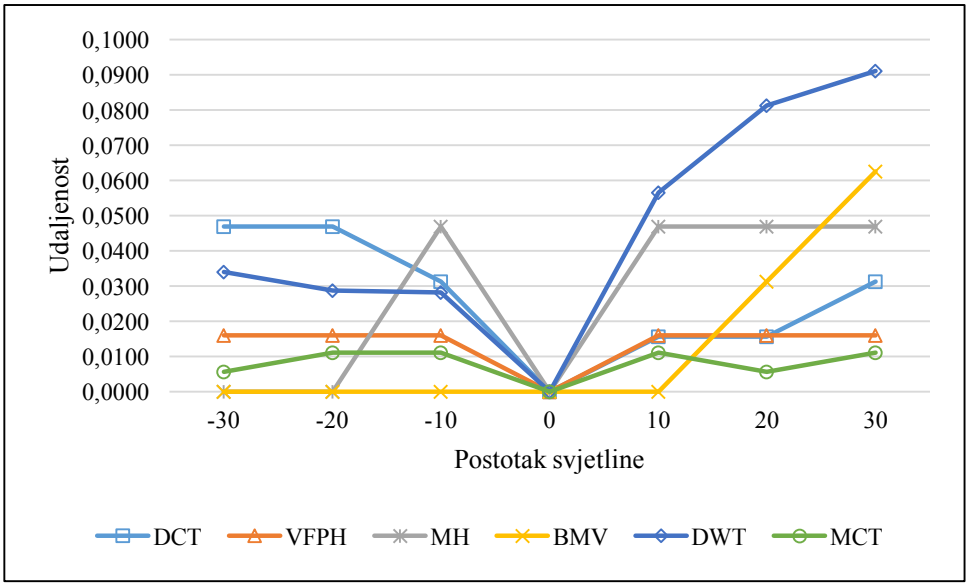
	DCT	VFPH	MH	BMV	DWT	MCT	(+/-)
MIN.	0,0156	0,0159	0,0000	0,0000	0,0282	0,0000	**(0,0000)**
MAKS.	0,0469	0,0159	0,0469	0,0625	0,0910	0,0111	**(+0,0048)**
PROSJEČNA	0,0313	0,0159	0,0313	0,0156	0,0533	0,0055	**(+0,0101)**

Uho

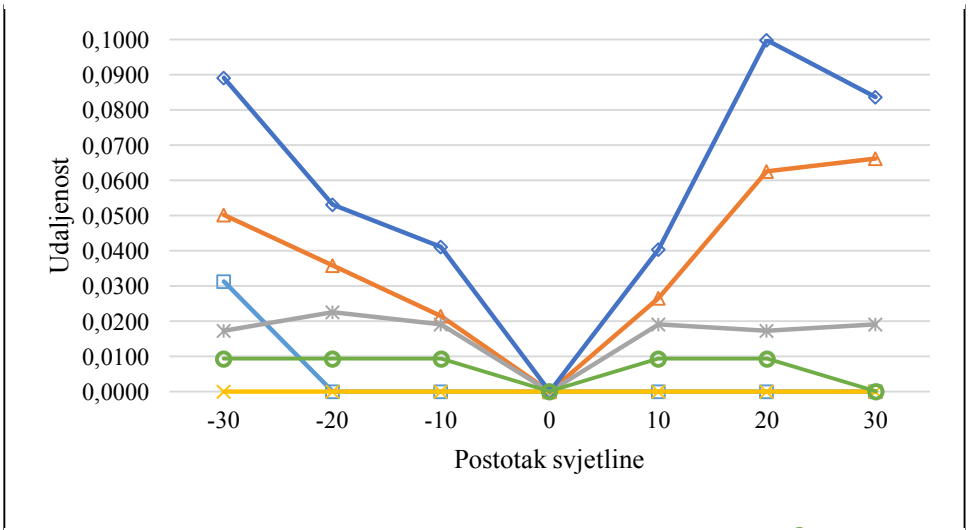
	DCT	VFPH	MH	BMV	DWT	MCT	(+/-)
MIN.	0,0000	0,0215	0,0173	0,0000	0,0404	0,0000	**(0,0000)**
MAKS.	0,0313	0,0662	0,0225	0,0000	0,0999	0,0093	**(-0,0093)**
PROSJEČNA	0,0052	0,0438	0,0190	0,0000	0,0679	0,0078	**(-0,0078)**

Potpis

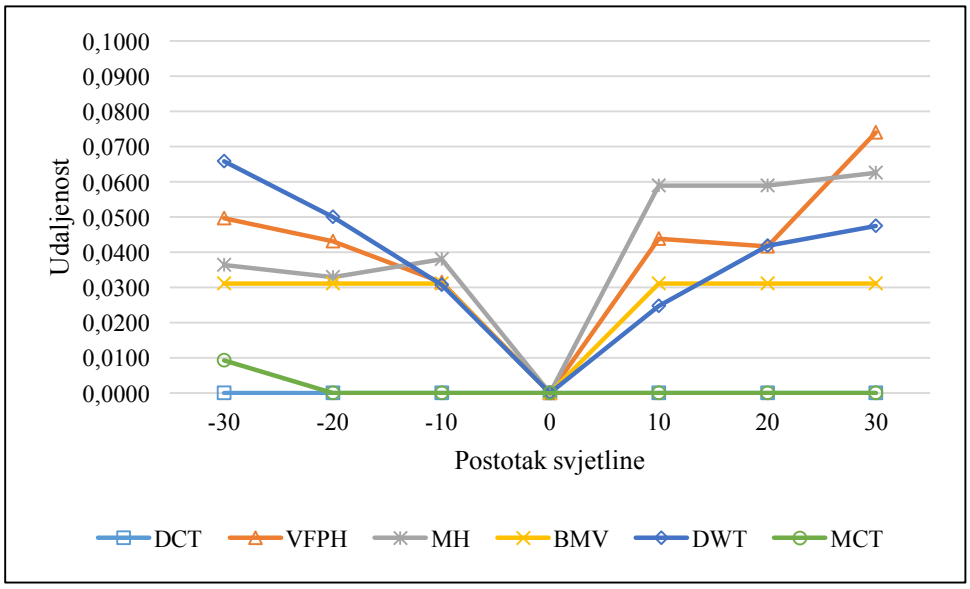
	DCT	VFPH	MH	BMV	DWT	MCT	(+/-)
MIN.	0,0000	0,0314	0,0329	0,0312	0,0247	0,0000	**(0,0000)**
MAKS.	0,0000	0,0496	0,0625	0,0312	0,0658	0,0093	**(-0,0093)**
PROSJEČNA	0,0000	0,0429	0,0480	0,0312	0,0435	0,0016	**(-0,0016)**



Grafikon 1. Napad svjetlinom na biometrijsku karakteristiku lica



Grafikon 2. Napad svjetlinom na biometrijsku karakteristiku uha



Grafikon 3. Napad svjetlinom na biometrijsku karakteristiku potpisa

7.2.1.1.2. Napad Gaussov šum

Šum se opisuje kao neželjena smetnja koja se preklapa s korisnom informacijom te koja ima tendenciju da prekrije njezin sadržaj. Može ga se predstaviti kao slučajnu varijablu sa svojom srednjom vrijednošću, standardnom devijacijom i varijancom.
Šum se dijeli (Schowengerdt):

- ns fotoelektronički (termalni, fotonski),
- na impulsni (*salt and pepper*) i
- na strukturirani (periodični nestacionarni, periodični stacionarni, aperiodični).

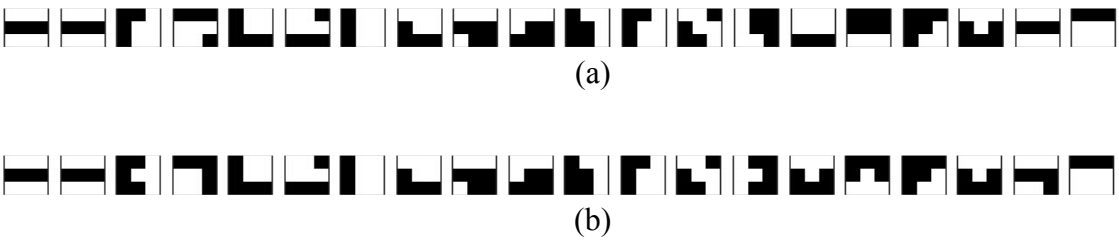
Šum predstavlja slučajne (stohastičke) varijacije svjetline ili boje u slici nastale u senzoru i elektroničkom sklopu digitalne kamere ili skenera.

Šumovi u digitalnoj slici pojavljuju se pri prikupljanju uzorka kod slabog osvjetljenja ili visoke temperature okoline, pri prolasku podataka kroz šumoviti kanal pri prijenosu ili kao pogreške koje nastaju pri pohranjivanju podataka i sl.

Za potrebe ove disertacije testnim slikama dodan je Gaussov bijeli šum sa srednjom vrijednošću 0 i konstantnom standardnom devijacijom kao i varijancom. Testiran je napad na biometrijske karakteristike lica, uha i potpisa sa standardnim vrijednostima devijacije šuma $\sigma = 5$, $\sigma = 10$, $\sigma = 15$ i $\sigma = 20$. Na slici 48. dan je primjer usporedbe originalne slike biometrijske karakteristike lica i slike nakon napada Gaussovim šumom ($\sigma = 15$).

(a) originalna slika (b) Gaussov šum ($\sigma = 15$)

Slika 48. Napad Gaussovim šumom kod biometrijske karakteristike lica



(a)

(b)

Slika 49. Usporedba MCT uzoraka (a) originalne slike biometrijske karakteristike lica i (b) slike na kojoj je izvršen napad Gaussovim šumom ($\boldsymbol{\sigma} = 20$)

Kako novorazvijeni MCT algoritam analizira vrijednost intenziteta (boje) 0 - 255 kod sivih intenzitetskih slika (engl. *grayscale*), a pri napadu Gaussovim šumom pikseli mijenjaju vrijednosti boje piksela, to ima velik utjecaj i na cenzus potpis svake regije oko biometrijske točke što je prikazano na slici 49. Kako je vrijednost napada dosta velika ($\sigma = 20$), tako je 6 od ukupnih 20 cenzus potpisa (prikazanih grafički MCT uzorcima na slici) percepcijskog sažetka originalne slike i napadnute slike različito.

Tablica 7. Napad Gaussov šum

Lice

	DCT	VFPH	MH	BMV	DWT	MCT	(+/-)
MIN.	0,0156	0,0000	0,0469	0,0000	0,0392	0,1000	**(-0,1000)**
MAKS.	0,0312	0,0159	0,0469	0,0000	0,0502	0,2278	**(-0,2278)**
PROSJEČNA	0,0234	0,0040	0,0469	0,0000	0,0475	0,1778	**(-0,1778)**

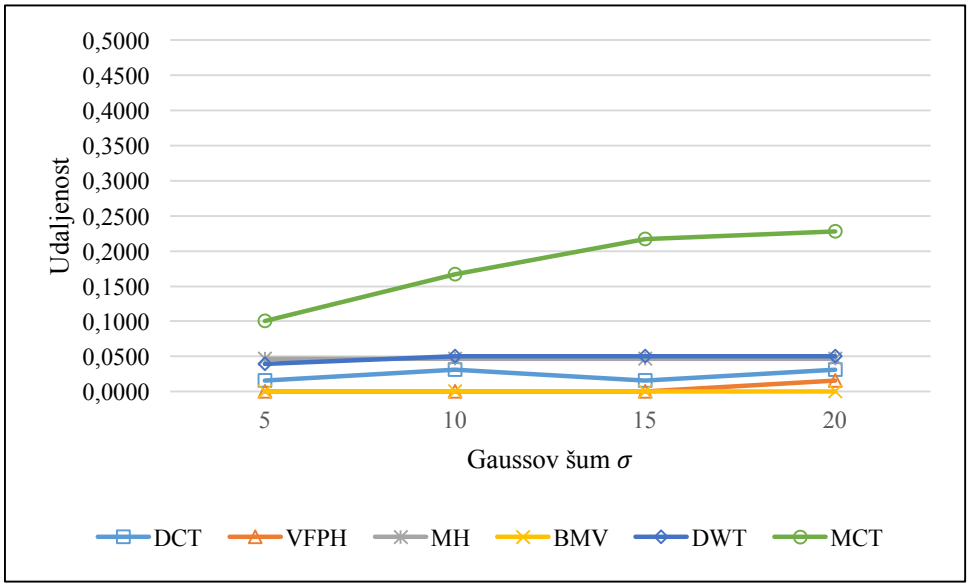
Uho

	DCT	VFPH	MH	BMV	DWT	MCT	(+/-)
MIN.	0,0000	0,0840	0,0659	0,0000	0,0000	0,0278	**(-0,2278)**
MAKS.	0,0312	0,2516	0,1927	0,0312	0,0140	0,1389	**(-0,1077)**
PROSJEČNA	0,0156	0,1418	0,1367	0,0078	0,0070	0,0949	**(-0,0871)**

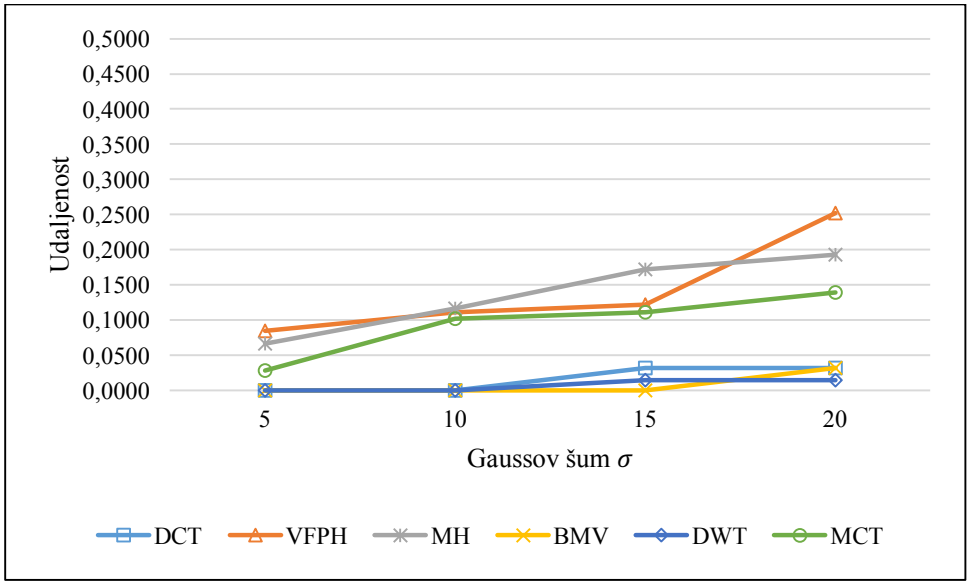
Potpis

	DCT	VFPH	MH	BMV	DWT	MCT	(+/-)
MIN.	0,0000	0,0909	0,1875	0,0000	0,0080	0,0926	**(-0,0926)**
MAKS.	0,0625	0,2928	0,2916	0,0278	0,0214	0,2685	**(-0,2471)**
PROSJEČNA	0,0234	0,1963	0,2534	0,0139	0,0134	0,1829	**(-0,1695)**

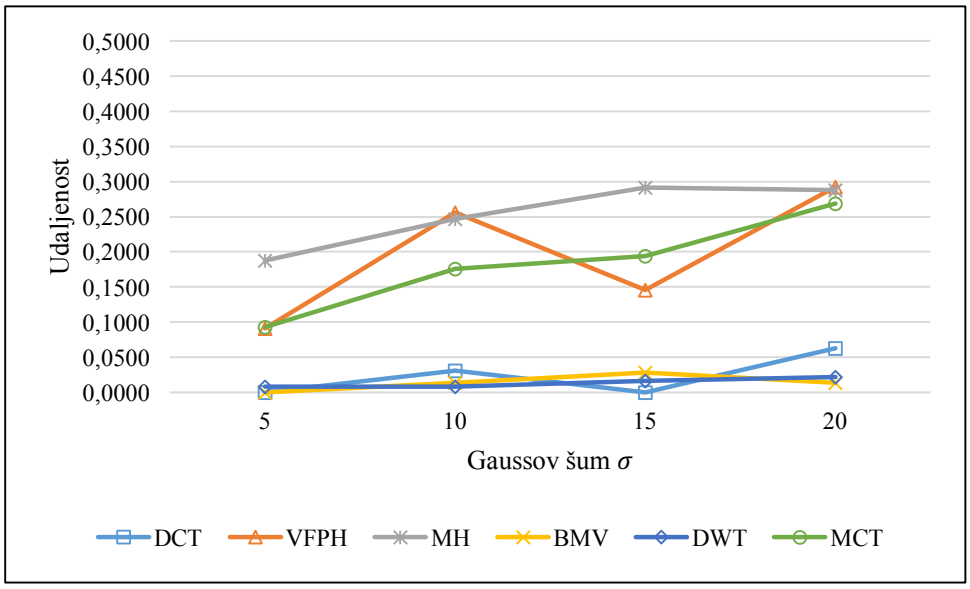
Iz dobivenih rezultata vidljivo je da nisu svi algoritmi robusni na napad Gaussovim šumom. Udaljenosti od percepcijskog sažetka originalne slike velike su u usporedbi s drugim negeometrijskim napadima (0,0000 – 0,2928). Algoritmi koji su u istraživanju najmanje robusni na taj napad jesu VFPH, MH, ali i novorazvijeni MCT algoritam. Najveća udaljenost zabilježena je kod biometrijske karakteristike potpisa (VFPH = 0,2928; MH = 0,2916; MCT = 0,2685). Uočljivo je i da rezultati algoritama ne ovise u tolikoj mjeri o testiranoj biometrijskoj karakteristici te da svi algoritmi imaju konzistentno ponašanje. Iznimka je jedino VFPH algoritam kod biometrijske karakteristike potpisa što je vidljivo na grafikonu 4.



Grafikon 4. Napad Gaussovim šumom na biometrijsku karakteristiku lica



Grafikon 5. Napad Gaussovim šumom na biometrijsku karakteristiku uha



Grafikon 6. Napad Gaussovim šumom na biometrijsku karakteristiku potpisa

7.2.1.1.3. Napad binarnim šumom

Binarni šum (engl. *Salt&Pepper*) poznat je kao impulsni šum. Nastaje kod iznenadnih smetnji tijekom prijenosa, a manifestira se pojavom šuma u obliku nasumičnih crnih ili bijelih točaka (piksela) na slici. Ako se s r ($0 < r < 1$) označi vjerojatnost pojave smetnje na slici, tada se s $r/2$ mogu označiti bijele (sol, engl. *salt*) odnosno crne (papar, engl. *pepper*) piksele kao šum. Za potrebe disertacije dodana vrijednost r u rasponu je od 0,01 do 0,05 za svaku digitalnu sliku, odnosno biometrijsku karakteristiku.

Tablica 8. Napad binarnim šumom

Lice

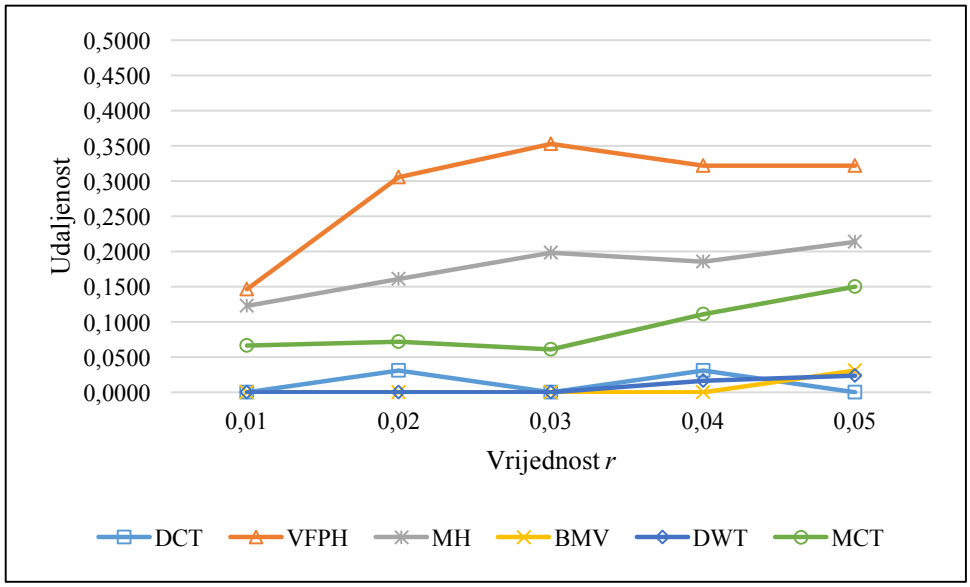
	DCT	VFPH	MH	BMV	DWT	MCT	(+/-)
MIN.	0,0000	0,1468	0,1232	0,0000	0,0000	0,0611	**(-0,0611)**
MAKS.	0,0312	0,3533	0,2135	0,0312	0,0236	0,1500	**(-0,1264)**
PROSJEČNA	0,0125	0,2899	0,1763	0,0062	0,0081	0,0922	**(-0,0841)**

Uho

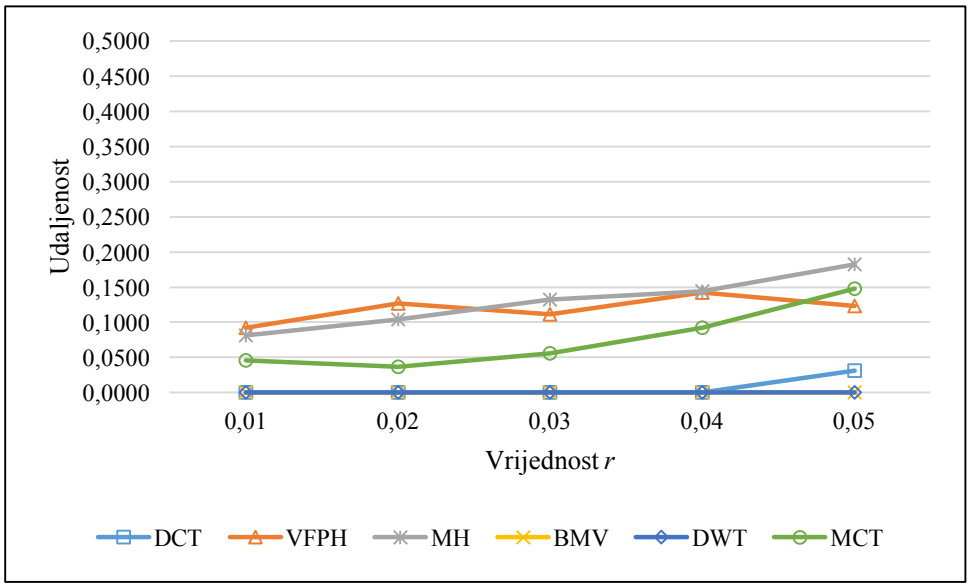
	DCT	VFPH	MH	BMV	DWT	MCT	(+/-)
MIN.	0,0000	0,0920	0,0815	0,0000	0,0000	0,0370	**(-0,0370)**
MAKS.	0,0312	0,1422	0,1822	0,0000	0,0000	0,1481	**(-0,1481)**
PROSJEČNA	0,0062	0,1191	0,1287	0,0000	0,0000	0,0759	**(-0,0759)**

Potpis

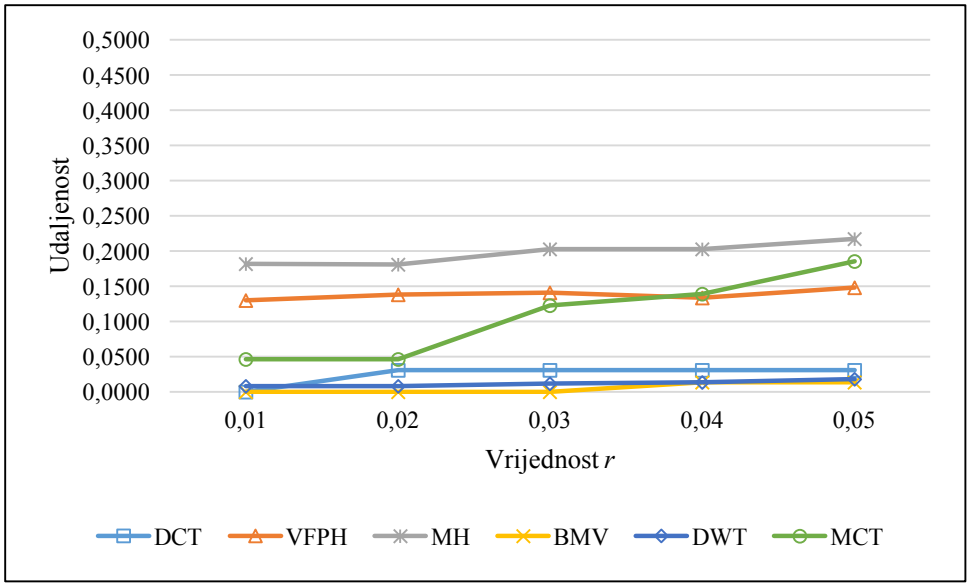
	DCT	VFPH	MH	BMV	DWT	MCT	(+/-)
MIN.	0,0000	0,1299	0,1805	0,0000	0,0080	0,0463	**(-0,0463)**
MAKS.	0,0312	0,1485	0,2170	0,0139	0,0180	0,1852	**(-0,1672)**
PROSJEČNA	0,0250	0,1380	0,1972	0,0056	0,0118	0,1078	**(-0,0960)**



Grafikon 7. Napad binarnim šumom na biometrijsku karakteristiku lica



Grafikon 8. Napad binarnim šumom na biometrijsku karakteristiku uha



Grafikon 9. Napad binarnim šumom na biometrijsku karakteristiku potpisa

Iz dobivenih rezultata robusnosti na napad binarnim šumom vidljivo je da su algoritami za izradu percepcijskih sažetaka u većoj ili manjoj mjeri osjetljivi, odnosno da nisu robusni. Najlošije rezultate u istraživanju postižu algoritmi VFPH (0,3533) i MH (0,2170), koji u testu nemaju dosljedno ponašanje i logična (očekivana) odstupanja kod malih promjena vrijednosti šuma *r*. Algoritmi koji se temelje na analizi atributa blokova, DCT i BMV u ovom istraživanju pokazuju veliku robusnost. Novorazvijeni MCT algoritam u ovom testiranju

također pokazuje veliku robusnost, ali samo u određenom rasponu vrijednosti binarnog šuma (r = 0,01 – 0,04). Za najveću vrijednost odnosno parametar r od 0,005 algoritam pokazuje lošije rezultate. Testiranjem se također pokazuje da robusnost algoritama na napad binarnim šumom ne ovisi o odabranoj biometrijskoj karakteristici.

7.2.1.1.4. Napad JPEG kompresijom

JPEG je najčešći format za pohranu slika kojim se koriste današnji digitalni fotoaparati. Posebno je dizajniran kako bi se smanjila veličina slika fotografskog tipa. Predstavlja dobar kompromis između kvalitete slike i veličine datoteke, a slike ovog formata pogodne su za upotrebu u svakodnevnim aplikacijama (Andabak i Gaura, 2010.). Sažimanje ili kompresija slike omogućava smanjenje veličine datoteke pri pohrani. Digitalna se slika pohranjuje kao i svaka druga računalna datoteka, no zbog velike količine podataka razvijeni su različiti sustavi za smanjivanje datoteke pri pohrani. Takvo smanjivanje datoteke naziva se kompresija ili sažimanje. Prilikom kompresije ne mijenja se broj piksela koji tvore sliku, već se samo mijenja način na koji se slika priprema za pohranu. Neki od tih procesa ne utječu na kvalitetu slike, a neki utječu. Slika se dakle može kompresirati bez gubitaka (engl. *lossless*) i uz gubitke (engl. *lossy*). JPEG format slike pri kompresiji koristi se metodom s gubicima. Metoda kompresije s gubicima radi na principu da su neke informacije na slici manje važne ili da su izvan granica ljudskog vizualnog sustava te se takve informacije na vrlo pametan način uklanjaju. Tako obrađena slika još uvijek ima dovoljno informacija za kvalitetnu rekonstrukciju slike. Te metode ponekad se nazivaju perceptivnima bez gubitaka, što znači da se do određene točke rekonstruirana slika neće razlikovati od orginala zato što su razlike neupadljive. U istraživanju za potrebe disertacije upotrijebljena je JPEG kompresija s gubitkom u rasponu od 10 do 90 %. Kod slika s 90-postotnom kompresijom bila je najlošija kvaliteta slike, odnosno došlo je do najvećeg gubitka, ali i najvećeg stupnja kompresije, a u slučaju 10-postotne kompresije dobivena je najbolja kvaliteta slike, odnosno došlo je do najmanjeg gubitka kod kompresije. Primjer vizulane usporedbe slike i slike s JPEG kompresijom prikazan je na slici 48.

(a) originalna slika (b) JPEG kompresija (90 %)

Slika 50. Napad JPEG kompresijom na biometrijsku karakteristiku lica

Veličina datoteka biometrijskih karakteristika prikazana je u tablici 7. Kod stupnja JPEG kompresije veličina datoteke za biometrijsku karakteristiku potpisa iznosi samo 6 Kb.

Tablica 9. Veličina datoteka u Kb za sve biometrijske karakteristike kod JPEG kompresije

Stupanj JPEG kompresije	**Lice (veličina u Kb)**	**Uho (veličina u Kb)**	**Potpis (veličina u Kb)**
10 %	35	75	23
20 %	28	55	18
30 %	23	43	15
...	...	...	...
90 %	7	12	6

Tablica 10. Napad JPEG kompresijom

Lice

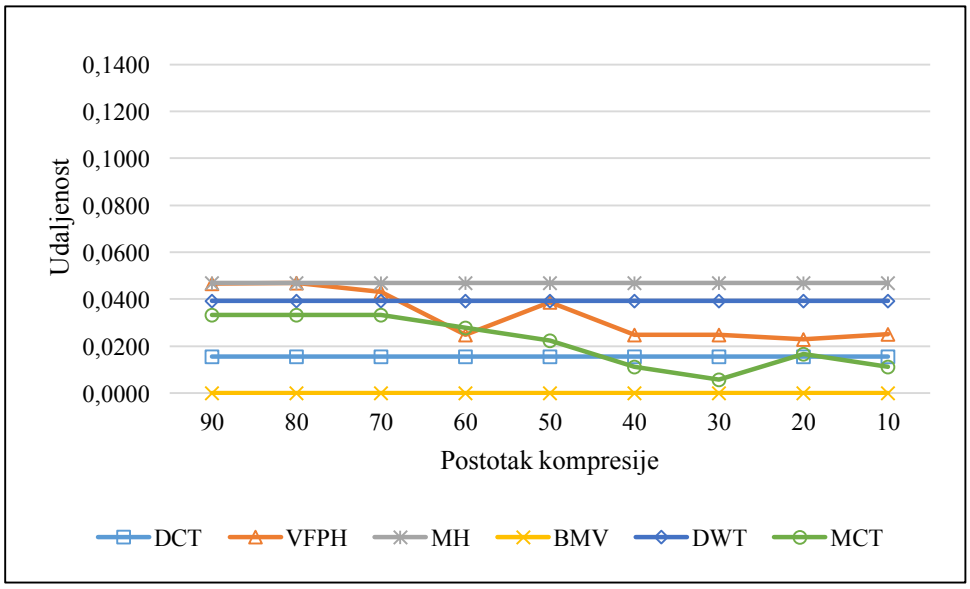
	DCT	VFPH	MH	BMV	DWT	MCT	(+/-)
MIN.	0,0156	0,0230	0,0469	0,0000	0,0392	0,0056	**(-0,0056)**
MAKS.	0,0156	0,0470	0,0469	0,0000	0,0392	0,0333	**(-0,0333)**
PROSJEČNA	0,0156	0,0331	0,0469	0,0000	0,0392	0,0216	**(-0,0216)**

Uho

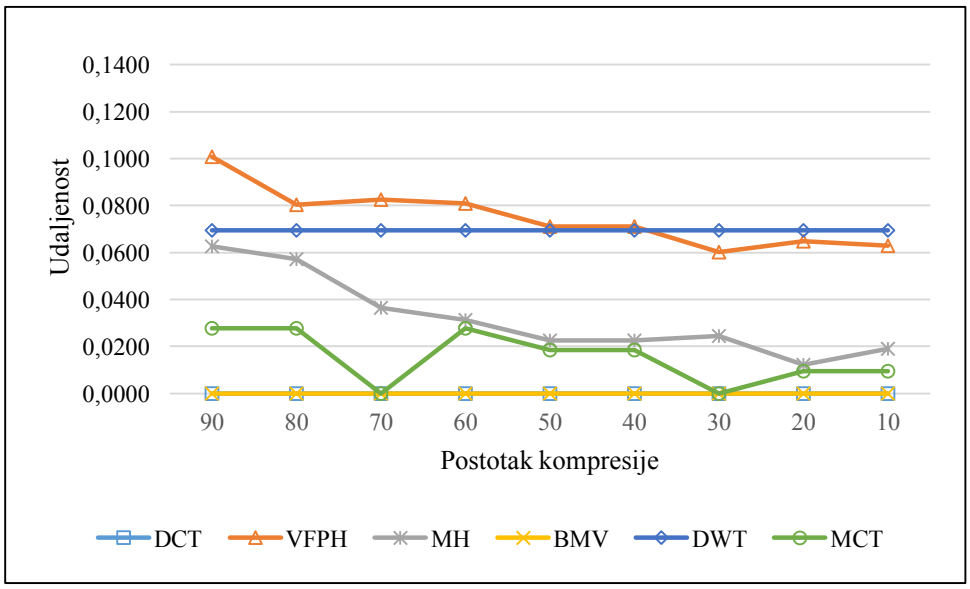
	DCT	VFPH	MH	BMV	DWT	MCT	(+/-)
MIN.	0,0000	0,0601	0,0121	0,0000	0,0694	0,0000	**(0,0000)**
MAKS.	0,0000	0,1007	0,0625	0,0000	0,0694	0,0278	**(-0,0278)**
PROSJEČNA	0,0000	0,0749	0,0320	0,0000	0,0694	0,0154	**(-0,0154)**

Potpis

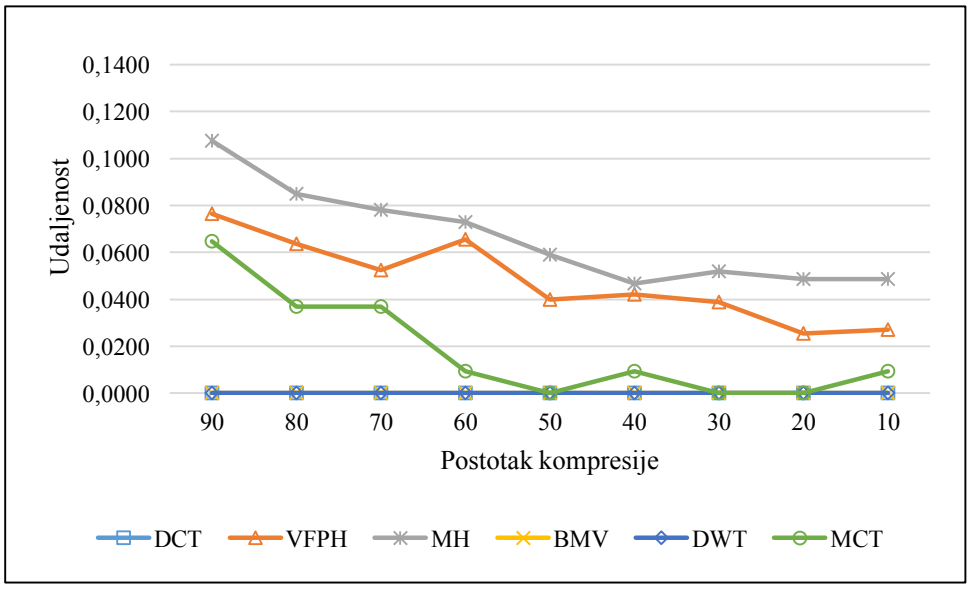
	DCT	VFPH	MH	BMV	DWT	MCT	(+/-)
MIN.	0,0000	0,0255	0,0468	0,0000	0,0000	0,0000	**(0,0000)**
MAKS.	0,0000	0,0765	0,1076	0,0000	0,0000	0,0648	**(-0,0648)**
PROSJEČNA	0,0000	0,0480	0,0665	0,0000	0,0000	0,0185	**(-0,0185)**



Grafikon 10. Napad JPEG kompresijom na biometrijsku karakteristiku lica



Grafikon 11. Napad JPEG kompresijom na biometrijsku karakteristiku uha



Grafikon 12. Napad JPEG kompresijom na biometrijsku karakteristiku potpisa

Rezultati testiranja algoritama pokazuju veliku robusnost na napad JPEG kompresijom što je i prikazano na grafikonima 10., 11. i 12. To pokazuju i rezultati kod kojih je maksimalna udaljenost iznosila (0,1076) kod MH algoritma za biometrijsku karakteristiku potpisa pri vrijednosti parametra kompresije od čak 90 %. Svi algoritmi u testu imaju dosljedno ponašanje i logična (očekivana) odstupanja kod malih promjena vrijednosti parametra odnosno stupnja kompresije bez obzira na odabranu biometrijsku karakteristiku.

7.2.1.2. Geometrijski napadi

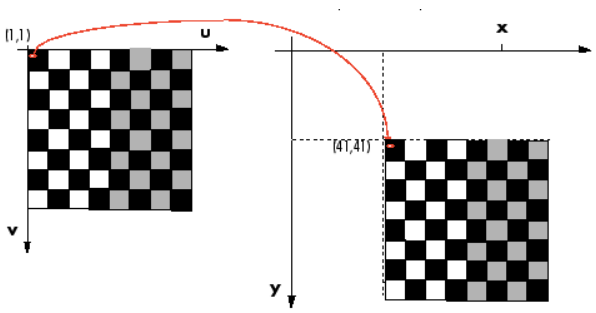
Geometrijska transformacija jest funkcija koja preslikava originalnu točku ili vektor u njezinu sliku. U računalnoj grafici upotrebljavaju se dvodimenzionalne (2D) i trodimenzionalne (3D) geometrijske transformacije. U disertaciji se radi ispitivanja robusnosti percepcijskih sažetaka na takve geometrijske promjene slika upotrebljavaju najčešće transformacije, odnosno izrezivanje, rotacija i skaliranje. Vrijednosti novih elemenata slika kod geometrijskih transformacija dobivene su bilinearnom interpolacijom. Bilinearna interpolacija (engl. *bilinear interpolation*) jest vrsta interpolacije kod koje se vrijednost novog slikovnog elementa izračunava na temelju vrijednosti četiriju susjednih piksela: lijevog, desnog, gornjeg i donjeg. Na taj način kreiraju se vrijednosti slikovnih elemenata u točkama izvan rešetke.

Kod geometrijskih transformacija piksel se s pozicije (x, y) pomiče na poziciju (x_1, y_1). Ovdje je bit transformacija koordinata slike što se može zapisati kako slijedi:

$$x_1 = \begin{bmatrix} x_1 \\ y_1 \end{bmatrix} = g(x) = \begin{bmatrix} x \\ y \end{bmatrix}$$

7.2.1.2.1. Napad translacijom

Najjednostavnija od svih geometrijskih operacija jest translacija, koja nastaje kada se čitava slika pomakne za dani vektor (x_0, y_0). Sve točke, odnosno pikseli pomiču se u istom smjeru i za istu udaljenost. Smjer vektora određuje smjer translacije. Dužina vektora određuje koliko će se točke pomaknuti. Doslovan prijevod latinske riječi *translatio* znači prijenos. Na slici 51. dan je primjer translacije piksela na digitalnoj slici.



Slika 51. Operacija translacije piksela na novu lokaciju (MathWork)

Tablica 11. Napad translacijom

Lice

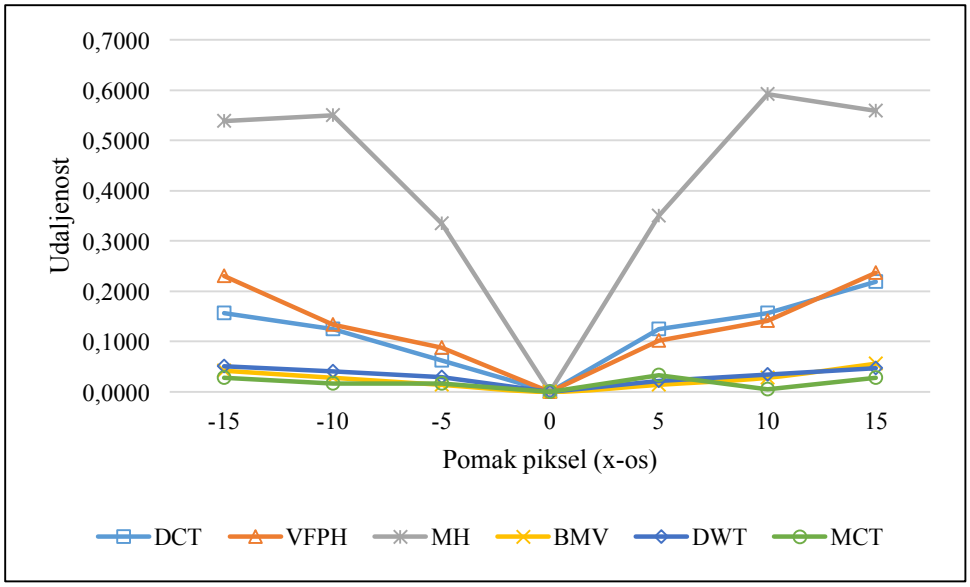
	DCT	VFPH	MH	BMV	DWT	MCT	(+/-)
MIN.	0,0625	0,0875	0,3350	0,0139	0,0221	0,0056	**(+0,0083)**
MAKS.	0,3506	0,2366	0,5920	0,0556	0,0506	0,0333	**(+0,0173)**
PROSJEČNA	0,1730	0,1551	0,4875	0,0301	0,0374	0,0213	**(+0,0088)**

Uho

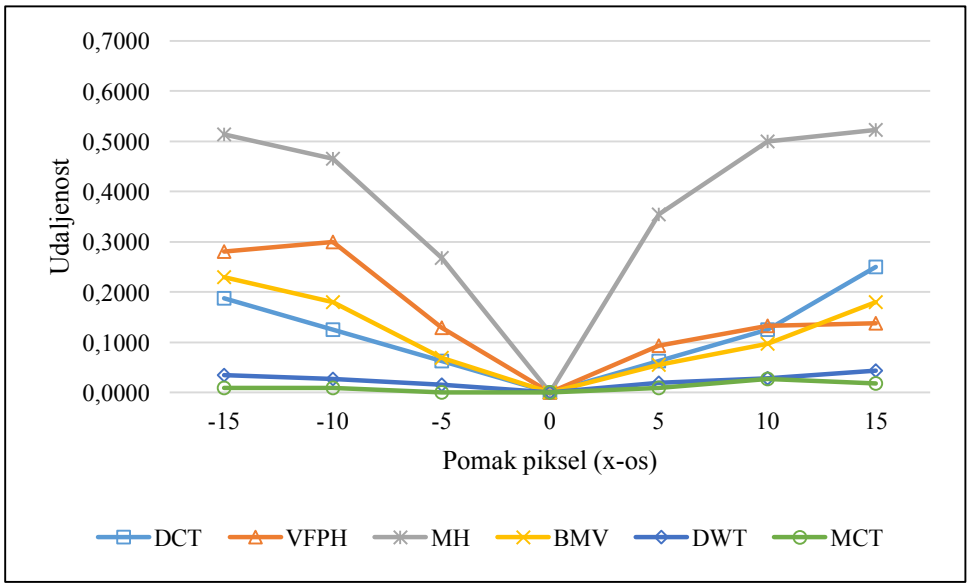
	DCT	VFPH	MH	BMV	DWT	MCT	(+/-)
MIN.	0,0625	0,0930	0,2673	0,0556	0,0152	0,0000	**(+0,0152)**
MAKS.	0,2500	0,3004	0,5225	0,2292	0,0440	0,0278	**(+0,0162)**
PROSJEČNA	0,1354	0,1790	0,4372	0,1354	0,0282	0,0124	**(+0,0158)**

Potpis

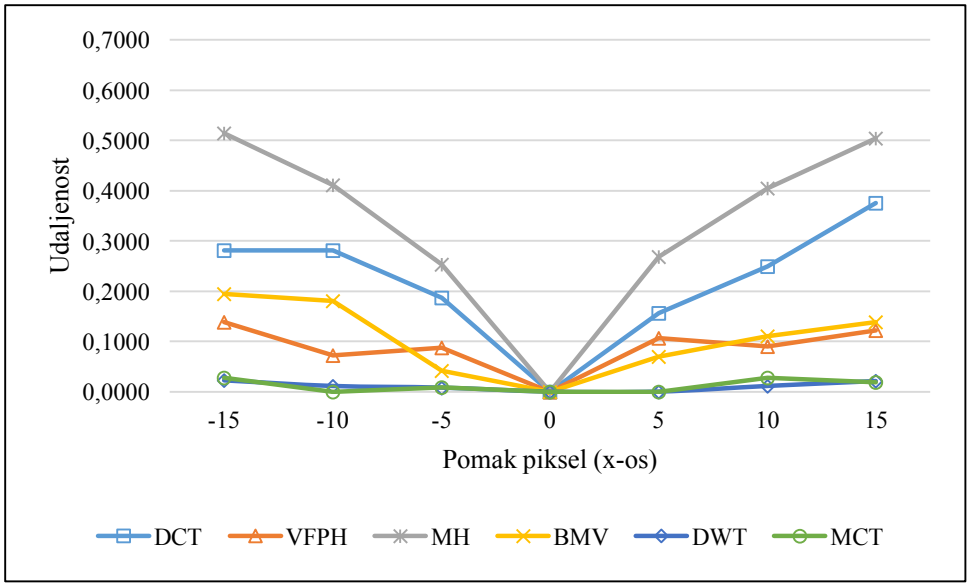
	DCT	VFPH	MH	BMV	DWT	MCT	(+/-)
MIN.	0,1562	0,0722	0,2534	0,0417	0,0000	0,0000	**(+0,0000)**
MAKS.	0,3750	0,1381	0,5138	0,1944	0,0226	0,0278	**(+0,0052)**
PROSJEČNA	0,2552	0,1028	0,3926	0,1227	0,0124	0,0139	**(-0,0015)**



Slika 52. Napad translacijom na biometrijsku karakteristiku lica



Grafikon 13. Napad translacijom na biometrijsku karakteristiku uha



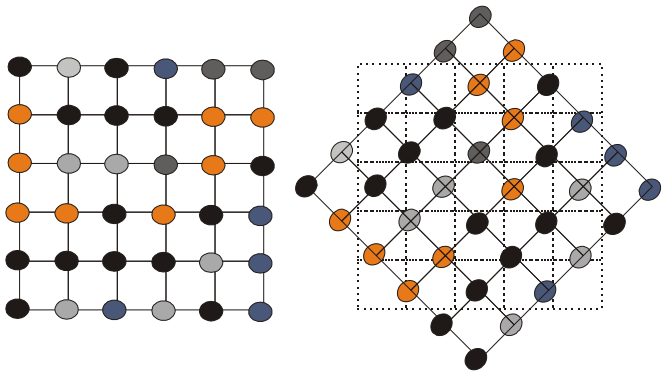
Grafikon 14. Napad translacijom na biometrijsku karakteristiku potpisa

Kod napada translacijom najlošiji rezultat ima MH algoritam (0,5920), i to za biometrijsku karakteristiku lica. Potrebno je naglasiti i to da kod maksimalnih vrijednosti parametra u napadu (+ - 15 piksela) MH algoritam daje rezultate koji u pravilu označavaju potpuno različite slike. Testiranjem se pokazalo i da DCT i VFPH algoritmi također bilježe

lošije rezultate maksimalnih udaljenosti i to kod svih biometrijskih karakteristika iako se radi o malim pomacima u translaciji (DCT = 0,3506; 0,2500; 0,3750) / (VFPH = 0,2366; 0,3004; 0,1381). Najrobusniji algoritam u testiranju ovog napada jest novorazvijeni MCT algoritam koji, bez obzira na biometrijsku karakteristiku, bilježi maksimalne udaljenosti od 0,0226 do 0,0333. Iako su dobiveni rezultati loši, odnosno udaljenosti su između percepcijskih sažetaka velike, svi algoritmi u testu imaju dosljedno ponašanje i logična (očekivana) odstupanja kod promjena vrijednosti parametra translacije.

7.2.1.2.2. Napad rotacijom

Rotacija je geometrijska transformacija kojom se (x_1, y_1) element originalne slike rotira u (x_2, y_2) element druge slike koristeći se određenim kutom α. Problem rotacije kod slika javlja se pri skeniranju ili uzimanju uzoraka biometrijskih karakteristika u biometrijskim sustavima, a operacija rotiranja primjenjuje se kako bi se poboljšao vizualni izgled slike u fazi pretprocesiranja slika. U disertaciji je zbog istraživanja robusnosti algoritama upotrijebljena rotacija slika oko centralne točke u opsegu od $\alpha = -30°$ do $\alpha = +30°$ u odnosu na originalnu sliku. Problem kod napada rotacije jest taj da elementi slike nisu na istom mjestu u rešetki u odnosu na originalnu sliku te se pri rotiranju osim pozicije mijenjaju i njihove vrijednosti boje što je prikazano na slici 53. i slici 54., pa je zbog toga potrebno provesti interpolaciju slike.



Slika 53. Rotacija elemenata slike za α = – 45 °

```
%rotacija
I = imrotate(I,30, 'crop','bilinear')
sz = size(I) / 2;
x=round(x)
y=round(y)
orig_x = x - sz(2);
orig_y = y - sz(1);
rot_mat=[cosd(-30), sind(-30); -sind(-30), cosd(-30)];
old_orig = [orig_x orig_y];
%nove koordinate
new_orig =old_orig * rot_mat;
new_x=new_orig(: , 1) + sz(2);
new_y=new_orig(:,2) + sz(1);
```

Kod 7.2. Operacija rotacije 30 ° i određivanje koordinata u MCT algoritmu – implementacija u alatu MATLab

177	182	187
179	181	181
182	177	172

MCT cenzus potpis **001110110**

160	161	160
147	155	158
134	143	155

MCT cenzus potpis **000110111**

Slika 54. Promjena MCT cenzus potpisa zbog promjene vrijednosti intenziteta piksela u regiji oko biometrijske točke uha kod rotacije slike od 30 ◦

Slika 54. prikazuje utjecaj geometrijskog napada rotacijom od 30° na novorazvijeni MCT algoritam. Kako algoritam analizira vrijednost intenziteta (boje) 0 - 255 kod sivih intenzitetskih slika (engl. *grayscale*), pri rotiranju slike osim pozicije piksela mijenjaju se i njihova vrijednosti boje. Pri tome se, kako je navedeno, koristila bilinearna interpolacija (engl. *bilinear interpolation*). Vrijednost novog slikovnog elementa izračunala se na temelju vrijednosti četiriju susjednih piksela: lijevog, desnog, gornjeg i donjeg, što je i prikazano na slici. Međutim, iako je stupanj rotacije slika prilično velik, nove vrijednosti intenziteta piksela kod biometrijskih karakteristika (lica i uha) nisu previše utjecale na vrijednost MCT cenzus potpisa originalne i rotirane slike (BER = 2) u odnosu na druge algoritme, što je prikazano u tablicama i grafikonima ispod.

Tablica 12. Napad rotacijom

Lice

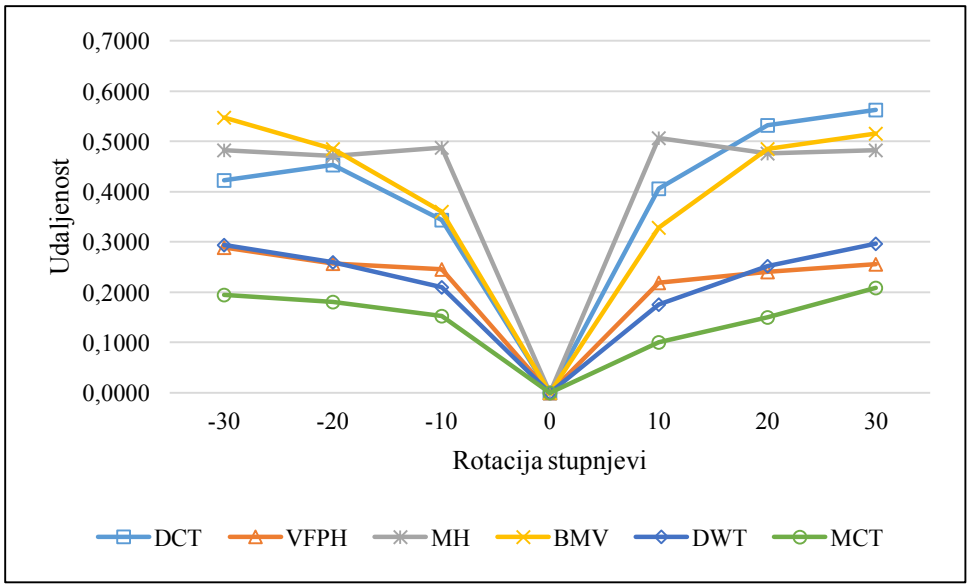
	DCT	VFPH	MH	BMV	DWT	MCT	(+/-)
MIN.	0,3438	0,2182	0,4705	0,3281	0,1760	0,1000	**(+0,0760)**
MAKS.	0,5625	0,2884	0,5069	0,5469	0,2970	0,2083	**(+0,0801)**
PROSJEČNA	0,4532	0,2510	0,4844	0,4531	0,2479	0,1644	**(+0,0835)**

Uho

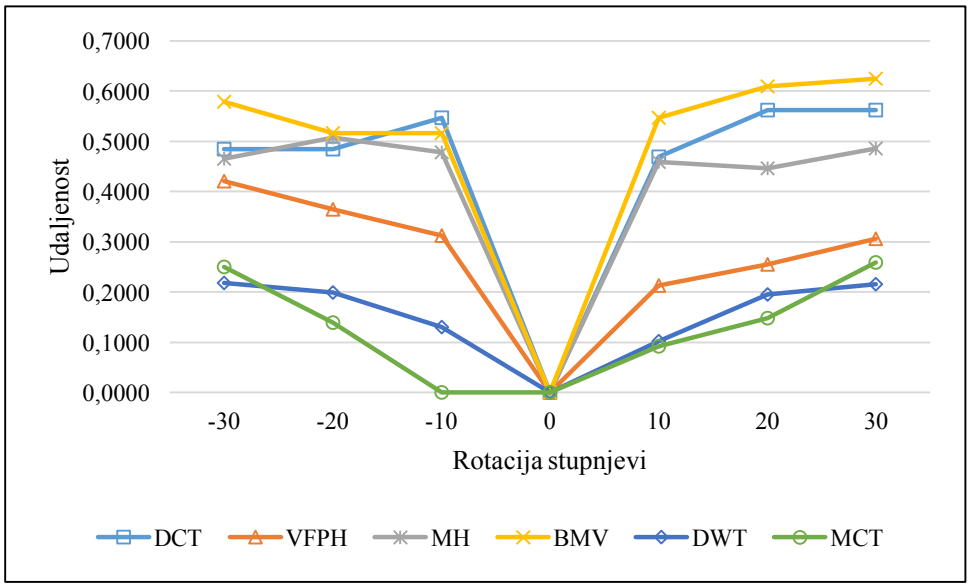
	DCT	VFPH	MH	BMV	DWT	MCT	(+/-)
MIN.	0,4687	0,2133	0,4461	0,5156	0,1029	0,0000	**(+0,1029)**
MAKS.	0,5625	0,4210	0,5069	0,6250	0,2179	0,2593	**(-0,0414)**
PROSJEČNA	0,5182	0,3123	0,4733	0,5651	0,1769	0,1297	**(+0,0472)**

Potpis

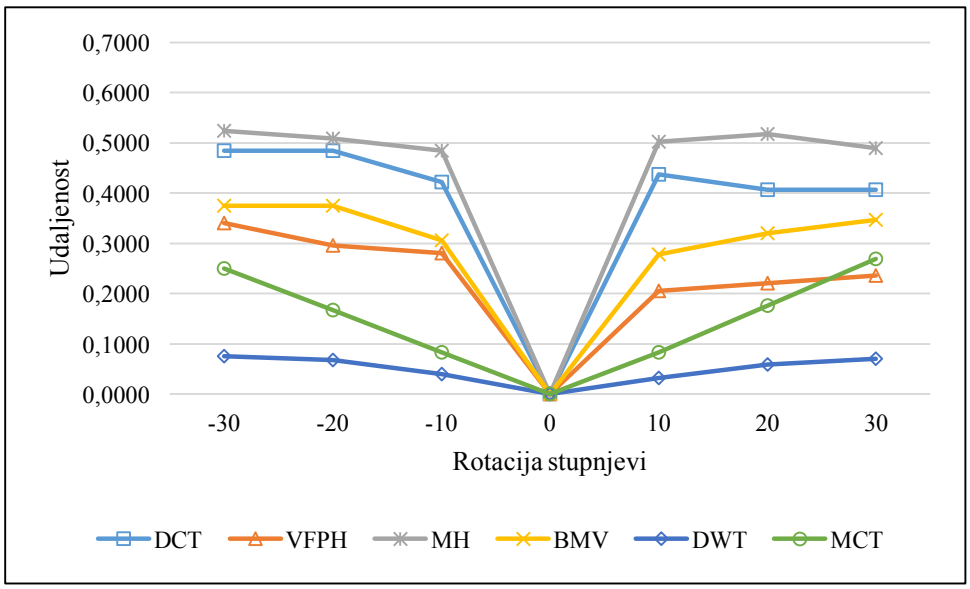
	DCT	VFPH	MH	BMV	DWT	MCT	(+/-)
MIN.	0,4062	0,2052	0,4843	0,2778	0,0321	0,0833	**(-0,0512)**
MAKS.	0,4843	0,3407	0,5243	0,3750	0,0762	0,2685	**(-0,1923)**
PROSJEČNA	0,4401	0,2633	0,5043	0,3333	0,0577	0,1713	**(-0,1136)**



Grafikon 15. Napad rotacijom na biometrijsku karakteristiku lica



Grafikon 16. Napad rotacijom na biometrijsku karakteristiku uha

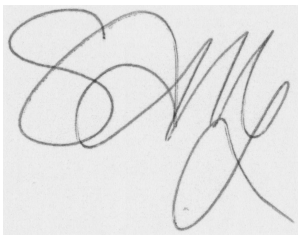


Grafikon 17. Napad rotacijom na biometrijsku karakteristiku potpisa

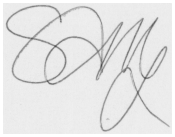
Slično kao i kod napada translacijom, algoritmi pokazuju loše rezultate u odnosu na druge u istraživanju testirane napade što je prikazano na prethodnim grafikonima. Tako najlošiji rezultat, odnosno najveću udaljenost bilježi MVB algoritam (0,6250) za biometrijsku karakteristiku uha. DCT algoritam za dvije od triju testiranih biometrijskih karakteristika (lice i uho) ima maksimalnu udaljenost od 0,5625. Neovisno o biometrijskoj karakteristici, i ostali algoritmi imaju loše rezultate i maksimalu udaljenost (VFPH = 0,4210; MH = 0,5243; DWT = 0,3750). Novorazvijeni MCT algoritam robusan je na samo mali stupanj rotacije od + –10 % (0,0833), ali s povećanjem stupnja rotacije povećava se i udaljenost iako je ona ukupno najmanja u odnosu na druge testirane algoritme. Testiranjem se pokazalo i da rotacija kod DWT algoritma nema prevelik utjecaj kod biometrijske karakteristike potpisa gdje je zabilježena maksimalna udaljenost samo 0,07.

7.2.1.2.3. Napad skaliranjem

Operacijom skaliranja fizička veličina slike povećava se ili smanjuje. Skaliranjem se mijenja broj piksela originalne slike, odnosno količina informacije na slici. U disertaciji je robusnost na napad skaliranjem ispitana na način da se slika smanjivala za omjer 0,01 – 0,05. Kako je već ranije spomenuto, nove vrijednosti piksela na slici dobivene su bilinearnom interpolacijom. Na slici 54. dan je primjer skaliranja.



(a) originalna slika



(b) napad skaliranjem 0,03

Slika 55. Napad skaliranjem na biometrijsku karakteristiku potpisa

Tablica 13. Napad skaliranjem

Lice

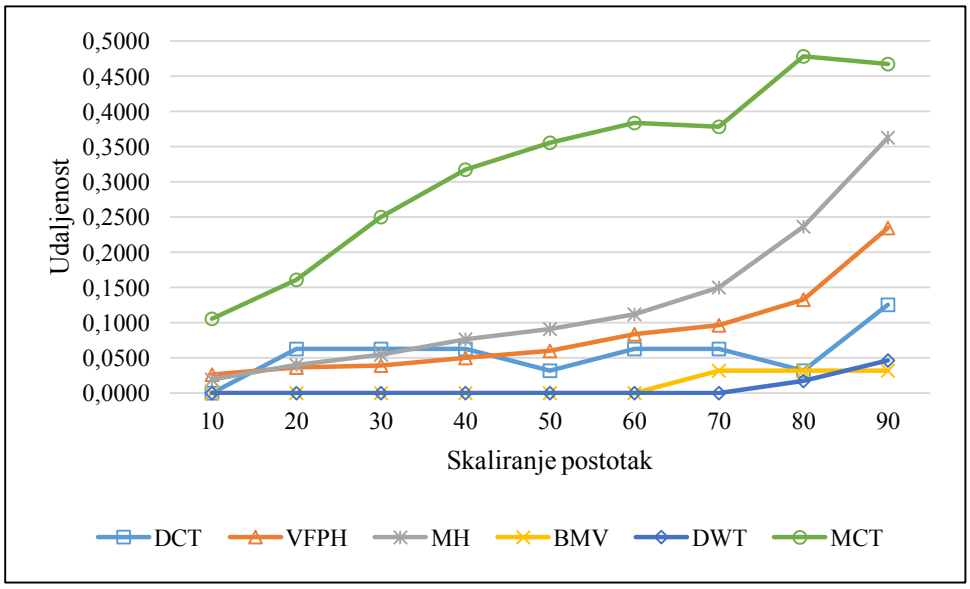
	DCT	VFPH	MH	BMV	DWT	MCT	(+/-)
MIN.	0,0000	0,0257	0,0191	0,0000	0,0000	0,1056	**(-0,1056)**
MAKS.	0,1250	0,2342	0,3628	0,0312	0,0461	0,4778	**(-0,4466)**
PROSJEČNA	0,0556	0,0841	0,1265	0,0104	0,0070	0,3216	**(-0,3146)**

Uho

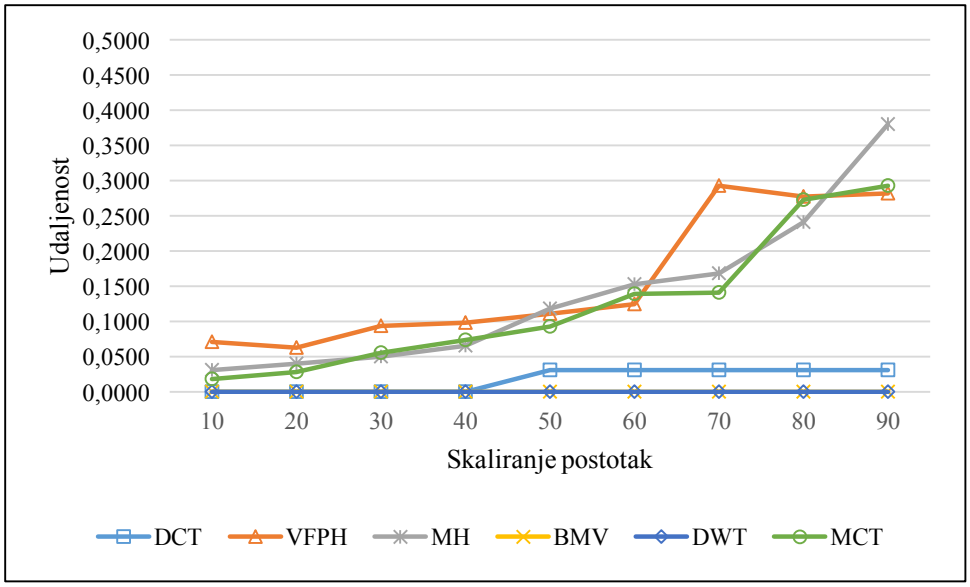
	DCT	VFPH	MH	BMV	DWT	MCT	(+/-)
MIN.	0,0000	0,0625	0,0312	0,0000	0,0000	0,0185	**(-0,0185)**
MAKS.	0,0312	0,2933	0,3802	0,0000	0,0000	0,2929	**(-0,2929)**
PROSJEČNA	0,0173	0,1570	0,1387	0,0000	0,0000	0,1238	**(-0,1238)**

Potpis

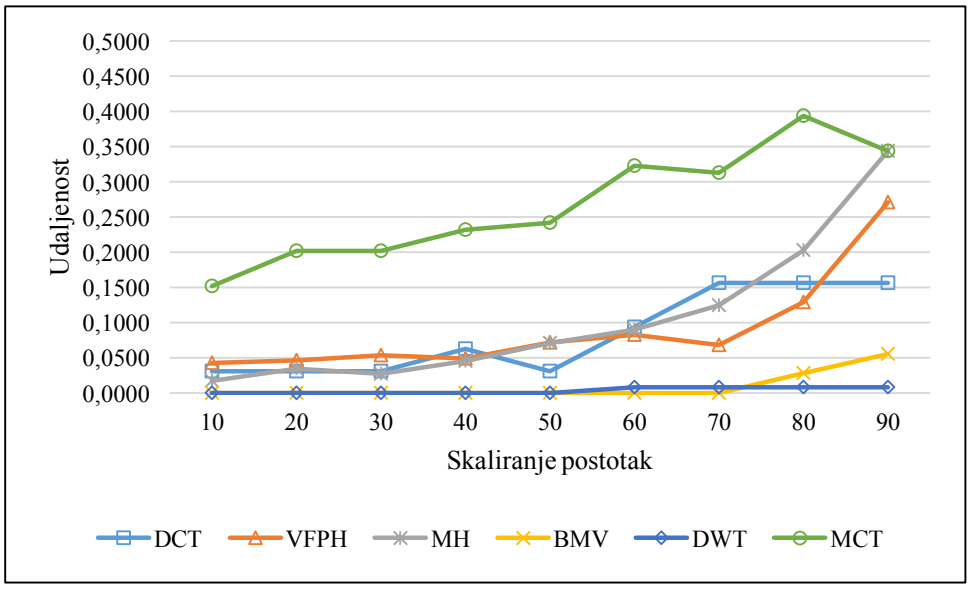
	DCT	VFPH	MH	BMV	DWT	MCT	(+/-)
MIN.	0,0312	0,0424	0,0173	0,0000	0,0000	0,1515	**(-0,1515)**
MAKS.	0,1562	0,2713	0,3437	0,0556	0,0080	0,3939	**(-0,3859)**
PROSJEČNA	0,0833	0,0906	0,1064	0,0093	0,0036	0,2671	**(-0,2635)**



Grafikon 18. Napad skaliranjem na biometrijsku karakteristiku lica



Grafikon 19. Napad skaliranjem na biometrijsku karakteristiku uha



Grafikon 20. Napad skaliranjem na biometrijsku karakteristiku potpisa

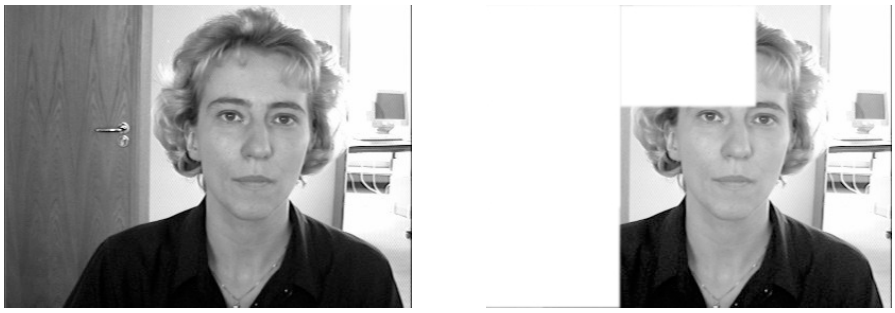
```
%velicina skalirane slike
[nretci nstupci]=size(I)
%velicina originalne slike
[retci stupci]=size(II)
%nove koordinate
newx = (x/retci)*nretci;
newy = (y/stupci)*nstupci;
imshow(I)
zoom(2)
hold on
plot(newx,newy,'+','MarkerEdgeColor','r')
```

Kod 7.3. Određivanje koordinata u skaliranim slikama u MCT algoritmu - implementacija u alatu MATLab

Od svih testiranih algoritama najmanju robusnost na napad skaliranjem pokazuje novorazvijeni MCT algoritam. Najveća odnosno maksimalna udaljenost zabilježena je kod biometrijske karakteristike lica (0,4778). Podjednako loše rezultate zabilježili su VFPH (0,2933) i MH (0,3802) algoritam, dok su se MVB (0,0556) i DWT (0,0461) algoritam pokazali najrobusnijima, odnosno na njih opisani napad gotovo nije imao ikakav utjecaj. Bez obzira na rezultate svi algoritmi u testu imaju dosljedno ponašanje i logična (očekivana) odstupanja kod promjena vrijednosti parametra skaliranja.

7.2.1.2.4. Napad brisanjem

Vizualno slične slike trebale bi imati sličnu strukturu. Općenito govoreći, ljudsko oko može razlikovati slike uspoređujući njihovu strukturu. Ako je na slici izvršena promjena brisanjem ili dodavanjem elemenata, narušena je struktura slike. Kod digitalnih slika, kao i u biometrijskim sustavima, nedostatak ili višak informacija može se manifestirati kao zlonamjerna radnja odnosno napad, ali može biti i posljedica pogrešaka u prijenosu ili pohrani podataka. Radi ispitivanja robusnosti algoritama percepcijskih sažetaka na takve promjene prvo je na testne slike izvršen napad brisanjem elemenata. Svaka testna slika podijeljena je na devet blokova, a izbrisani su blokovi 1 – 4 od lijeve strane slike prema sredini što je dovoljno za ispitivanje robusnosti. Brisanjem više od četiriju blokova ne bi se dobili pouzdani rezultati s obzirom na činjenicu da bi se time izbrisalo više od polovice strukture slike.



(a) originalna slika (b) napad brisanjem (promjena četiriju blokova)

Slika 56. Napad brisanjem na biometrijsku karakteristiku lica

Tablica 14. Napad brisanjem

Lice

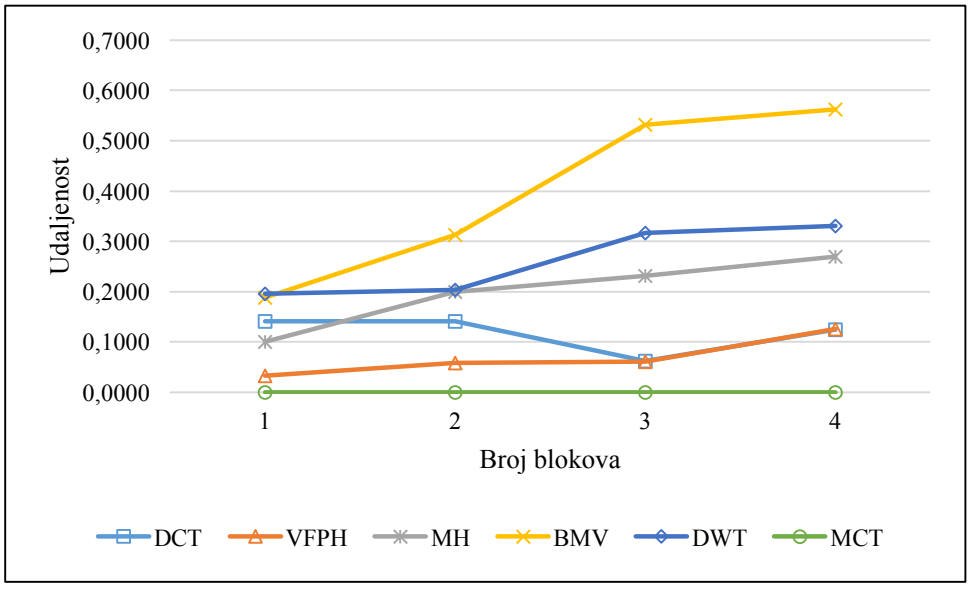
	DCT	VFPH	MH	BMV	DWT	MCT	(+/-)
MIN.	0,0625	0,0324	0,1007	0,1875	0,1956	0,0000	**(+0,0324)**
MAKS.	0,1406	0,1261	0,2691	0,5625	0,3304	0,0000	**(+0,1261)**
PROSJEČNA	0,1172	0,0693	0,2001	0,3984	0,2615	0,0000	**(+0,0693)**

Uho

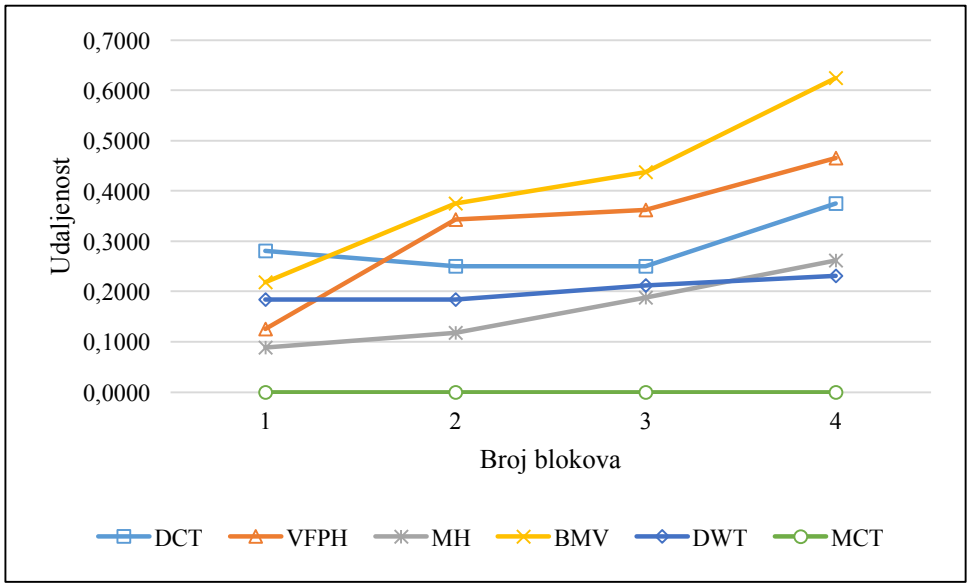
	DCT	VFPH	MH	BMV	DWT	MCT	(+/-)
MIN.	0,2500	0,1255	0,0885	0,2188	0,1841	0,0000	**(+0,0885)**
MAKS.	0,3750	0,4649	0,2621	0,6250	0,2311	0,0000	**(+0,2311)**
PROSJEČNA	0,2891	0,3239	0,1640	0,4141	0,2029	0,0000	**(+0,1640)**

Potpis

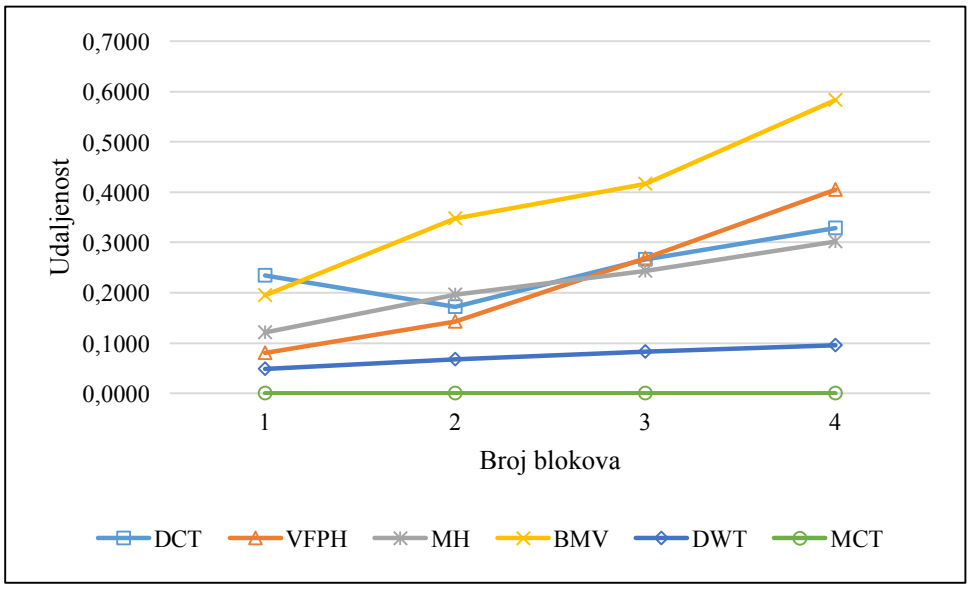
	DCT	VFPH	MH	BMV	DWT	MCT	(+/-)
MIN.	0,1718	0,0804	0,1215	0,1944	0,0487	0,0000	**(+0,0804)**
MAKS.	0,3281	0,4049	0,3020	0,5833	0,0962	0,0000	**(+0,0962)**
PROSJEČNA	0,2500	0,2243	0,2157	0,3854	0,0736	0,0000	**(+0,0736)**



Grafikon 21. Napad brisanjem na biometrijsku karakteristiku lica



Grafikon 22. Napad brisanjem na biometrijsku karakteristiku uha



Grafikon 23. Napad brisanjem na biometrijsku karakteristiku potpisa

Najmanju robusnost na napad brisanjem blokova u testu pokazuje MVB algoritam (0,6250) i to za biometrijsku karakteristiku uha. Slične rezultate pokazuje i za biometrijsku karakteristiku lica (0,5625) te za biometrijsku karakteristiku potpisa (0,5833). Ostali algoritmi također pokazuju lošije rezultate VFPH (0,4649), MH (0,3020), DCT (0,3750) i DWT (0,3304). Potrebno je da DWT algoritam kod biometrijske karakteristike potpisa pokazuje

veliku robusnost te da je zabilježena maksimalna udaljenost od samo 0,0962. Kako je ranije opisano, napad brisanjem nema utjecaj na novorazvijeni MCT algoritam. Bez obzira na rezultate većina algoritama u testu ima dosljedno ponašanje i logična (očekivana) odstupanja kod promjena vrijednosti parametra brisanja, odnosno što je veći dio slike izbrisan, zabilježene su udaljenosti veće.

Jedna od bitnih značajki novorazvijenog MCT algoritma je da se dodatnim fazama algoritama našao nov način za uspoređivanje percepcijskih sažetaka koji nisu jednake duljine Damerau-Levenshteinovom metodom što u prethodnim istraživanjima koji su se bavili percepcijskim sažetcima nije bilo moguće. Naime, tijekom vrednovanja uočena je jedna za algoritme za izradu percepcijskih sažetaka specifična, a za biometrijske sustave uobičajena situacija, a to je nedostatak atributa za analizu u odnosu na originalnu sliku. Takvi uzorci u biometrijskim sustavima bili bi odbačeni zbog loše kvalitete, a kod algoritama za izradu percepcijskih sažetaka dijelovi koji nedostaju bili bi označeni su kao prazan prostor (nula) što bi dovelo do netočnih rezultata pri njihovoj usporedbi. U tom slučaju percepcijski sažetak moguće je izraditi bez tih regija, samo što je tada rezultat manja duljina sažetka. Budući da svi algoritmi za izradu percepcijskog sažetka opisani u disertaciji upotrebljavaju Hammingovu udaljenost kao metodu za mjerenje sličnosti, usporedba takvih sažetaka različite duljine ne bi bila moguća. Hammingova udaljenost mjeri udaljenost odnosno različitost elemenata samo kada se uspoređuju dva sažetka jednake duljine. Damerau-Levenshteinovom udaljenošću (engl. *Damerau-Levenshtein distance*) mogu se mjeriti sažetci različite duljine što je opisano i u poglavlju 4.2. ove disertacije. Pritom se javlja potreba za uvođenjem drugog praga T_1, kojim se određuje prihvatljiva vrijednost udaljenosti između dvaju percepcijskih sažetaka koji nisu jednake duljine.

Da bi detaljnije ispitali taj dio novorazvijenog MCT algoritma, napravio se novi dodatni testni *intra* set slika biometrijske karakteristike lica (n = 100) gdje su se nasumično brisali dijelovi slika odnosno regije na slikama (slika 57.). Svaka slika iz testnog seta odnosno njihovi percepcijski sažetci uspoređivali su se sa percepcijskim sažetkom originalne slike iz baze. Važno je napomenuti da su obrisani blokovi na slici bili veličine od 9x9 piksela do 81x81 piksela. Maksimalni broj takvih nasumično obisanih blokova bio je 10. Položaj i broj obrisanih blokova bio je nasumično određen. Implementacija dodatnih faza u algoritmu također je napravljena u programskom paketu MATLAB.

Slika 57. Biometrijska karakteristika lica sa nasumično obrisanim blokovima

Kako je ranije opisano novorazvijeni MCT algoritam na slikama biometrijske karakteristike lica izdvaja i analizira regiju oko 20 biometrijskih točaka. Kako se u testnom setu nalazilo i slika sa obrisanim blokovima koji nisu bili dio izdvojenih i analiziranih regija oko biometrijskih točaka rezultat je za takve slike normaliziranom Hammingovom udaljenošću iznosio 0 što je i očekivano. Kako su analizirane regije oko svake biometrijske točke u novorazvijenom MCT algoritmu bile veličine ukupno 81 piksel (9 blokova od 3x3 piksela) što je prikazano na slici 39., na nekim slikama iz testnog seta te regije su bile samo djelomično obrisane (slika 57.). U takvim slučajevima novorazvijeni MCT algoritma nije prepoznao da se radi o djelomično obrisanim regijama te je takve piksele označavao kao BER (engl. *bit error rate*) kod normalizirane Hammingove udaljenosti u odnosu na originalnu sliku odnosno njezin percepcijski sažetak. Kod testnih slika gdje je algoritam primjenom modificirane cenzus transformacije prepoznao da je cijela regija oko biometrijske točke obrisana, takvu je regiju označio kao obrisanu biometrijsku točku (slika 58.). Takvi percepcijski sažetci uspoređivani su Damerau-Levenshteinovom udaljenošću sa percepcijskim sažetkom originalne slike zbog različitih dužina percepcijskih sažetaka što je opisano u poglavlju 4.2. ove disertacije. U tablici 15. prikazana je Damerau-Levenshtein udaljenost za svaku u potpunosti obrisanu biometrijsku točku odnosno regiju oko nje. Treba se napomenuti da su sve takve slike u testu bile uspješno detektirane. Ako na slikama iz testnog seta nije bilo brisanja samo dijela piksela u regiji oko biometrijske točke, ostale regije bile su istovjetne regijama originalne slike, te je njihova normalizirana Hammingova udaljenost bila 0 (BER = 0) te su kao takve prikazane na grafikonu 24. ispod. Slika 59. prikazuje primjer usporedbe percepcijskog sažetka originalne slike sa percepcijskim sažetkom gdje su u potpunosti obrisane prve dvije biometrijske točke odnosno regije oko njih, a četvrta biometrijska točka je

obrisana samo djelomično (BER = 4). U tom slučaju normalizirana Hammingova udaljenost za preostali dio percepcijskog sažetka iznosi 0,0888.

Tablica 15. Damerau-Levenshteinova udaljenost prema broju obrisanih biometrijskih točaka

Broj obrisanih biometrijskih točaka	**Damerau-Levenshteinova udaljenost**
1	9
2	18
3	27
4	36
5	45
6	54

…

110101100 011100001 101110101 111101011 11010101 101010101 101010101

(a)

000000000 000000000 101110101 111101011 11010101 101010101 101010101

(b)

Damerau-Levenshtein = 18; BER = 0; normalizirana Hammingova udaljenost = 0,0000

Slika 58. Percepcijski sažetci (a) orginalne slike i (b) slike na kojoj su obrisane prve dvije biometrijske točke

110101100 011100001 101110101 111101011 11010101 101010101 101010101

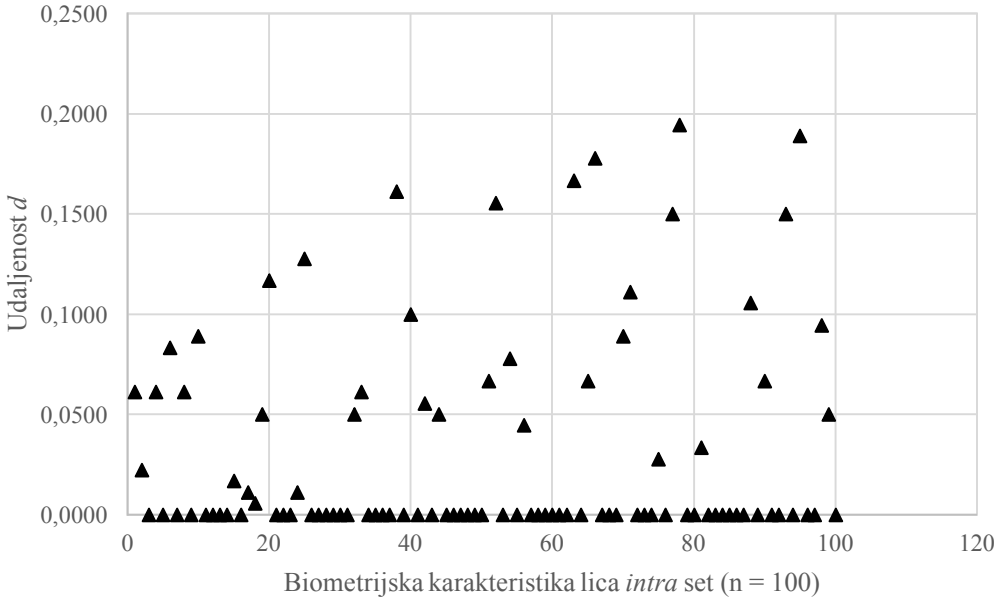
(a)

000000000 000000000 101110101 0000 01011 11010101 101010101 101010101

(b)

Damerau-Levenshtein = 22; BER = 4; normalizirana Hammingova udaljenost = 0,0888

Slika 59. Percepcijski sažetci (a) orginalne slike i (b) slike na kojoj su obrisane prve dvije biometrijske točke i četvrta djelomično BER = 4



Grafikon 24. Distribucija rezultata MCT algoritma za nasumično obrisane blokove

Grafikon 24. prikazuje distribuciju rezultata MCT algoritma za testirani *intra* set (n = 100) biometrijske karakteristike lica sa nasumično obrisanim blokovima. Kako se i očekivalo, većina testiranih slika ima normaliziranu Hammingovu udaljenost *d* jednaku 0. Prvi razlog je taj što, kako je već navedeno, nasumično obrisani blokovi na tim slikama nisu bili u blizini regija oko odabranih biometrijskih točaka te su, pošto na slikama nije bilo nikakvih drugih napada, percepcijski sažetci orginalne slike i percepcijski sažetci takvih slika

bili jednaki (BER = 0). Drugi razlog je taj što je algoritam uspješno detektirao u potpunosti obrisane biometrijske točke i njihove okolne regije (Damerau-Levenshtein udaljenost = 9, 18, 27) te je, pošto je ostatak percepcijskog sažetka bio u potpunosti jednak percepcijskom sažetku originalne slike, normalizirana Hammingova udaljenost *d* iznosila također 0. Ostale slike u distribuciji imaju rezultat udaljenosti od minimalnih 0,01111 do maksimalnih 0,19444, zbog djelomično obrisanih regija oko biometrijskih točaka. No, gledano u postocima to je rezultat između 80,56 i 99,98% točnosti.

Testom robusnosti pokazalo se da za sve biometrijske karakteristike i prema postavljenim kriterijima važnosti, novorazvijeni MCT algoritam u odnosu na ostale vrednovane algoritme daje najbolje rezultate u dvije od tri kategorije testiranih napada (geometrijski i maliciozni) čime je djelomično potvrđen prvi dio u postavljenoj hipotezi disertacije, a koji se odnosi na robusnost algoritma, pogotovo za potrebe u sustavima biometrijske autentikacije. Iako je tijekom testa robusnosti primijećeno da rezultati ovise i o odabranoj biometrijskoj karakteristici, ukupno gledano, novorazvijeni algoritam pokazuje veliku robusnost u odnosu na druge algoritme kod geometrijskih napada (rotacije i translacije) i kod malicioznog napada brisanjem. Jedine nedostatke robusnosti MCT algoritam pokazuje kod napada skaliranjem i to kod biometrijskih karakteristika lica i potpisa, i djelomično kod negeometrijskih napada binarnim i Gaussovim šumom što je donekle i očekivano s obzirom na činjenicu da se tim napadima mijenja vrijednost gradijenta (boje) piksela pojedinih regija odnosno piksela na slici, a koje novorazvijeni algoritam uzima u obzir pri svojem radu. No, kako se tijekom istraživanja literature došlo do novih spoznaja, u nastavku disertacije prikazano je moguće rješenje za poboljšanje rezultata novorazvijenog algoritma kod takvih napada. Kao još jedno od mogućih rješenja je i kombinacija novorazvijenog algoritma sa nekim već postojećim algoritmima za izradu percepcijskih sažetaka koji pokazuju veću robusnost na geometrijske napade, što bi također poboljšalo rezultat.

Iz dobivenih rezultata testa robusnosti može se zaključiti da bi novorazvijeni MCT algoritam u ovakvom obliku, bio najprikladniji u slučajevima provjere uzoraka biometrijskih karakteristika koji su označeni zbog nedovoljne kvalitete te koje bi postojeći biometrijski sustavi odbacivali kao neispravne zbog nedostatka dijelova slike, loše prezentacije ili njihovog položaja (rotacija) odnosno gdje god dolazi do otežanog čitanja atributa na senzoru.

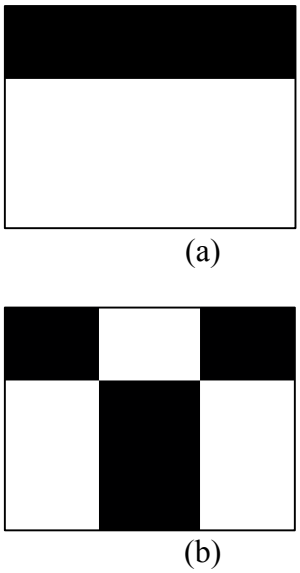
Isto tako testom robusnosti je uočeno da se, kod pojedinih algoritama, kao jedini relevantni pokazatelj ne može uzeti samo robusnost algoritma na pojedine napade. Neki od njih (BMV i DWT), iako u testu robusnosti pokazuju veliku robusnost na negeometrijske napade, rezultati pokazuju da zapravo ne uočavaju male promjene vrijednosti napada te time generiraju veliki broj pogrešaka.

7.3. Poboljšanje MCT algoritma za napad Gaussovim i binarnim šumom

Kako su rezultati istraživanja pokazali, novorazvijeni MCT algoritam ne pokazuje veliku robusnost na napade Gaussovim i binarnim šumom, odnosno u slučajevima kad se mijenja vrijednost gradijenta promatranog bloka što može predstavljati problem. Problem je djelomično moguće riješiti primjenom nekog linearnog filtra (npr. Wienerov filtar) u fazi pretprocesiranja slike čija su namjena smanjenje i eliminacija šumova u slici. Nadalje, za percepcijske sažetke prikladno je rješenje primjena metode zamjene, koju su predložili autori Chen i suradnici (Chen et al., 2013.) i Ojala i suradnici (Ojala et al., 2002.).

U njihovim radovima primijećeno je da se *podstringovi* u redcima blokova (Y) veličine 3 x 3 piksela u slici pojavljuju u obliku $Y = \{y_1 = (000), y_2 = (001), y_3 = (010), y_4 = (011), y_5 = (100), y_6 = (101), y_7 = (110), y_8 = (111)\}$. Isto tako, primijećeno je i da se statistički u analizi blokova slika najčešće javljaju oblici $y_1 = (000)$ i $y_8 = (111)$, a koji označuju glatke površine ili linije odnosno rubove.

Ako se promatraju *stringovi* blokova piksela u ovoj disertaciji dobiveni metodom modificirane cenzus transformacije piksela oko centralnih biometrijskih točaka, može se primijetiti sličnost. Na slici 55. prikazani su uzorak (a) originalne slike karakteristike lica i uzorak (b) slike na kojoj je izvršen napad Gaussovim šumom ($\sigma = 10$). Vidljivo je da se uzorci razlikuju, odnosno izračunana normalizirana Hammingova udaljenost u ovom slučaju iznosi 0,3333 što usporedbom percepcijskih sažetaka označava da su uzorci potpuno različiti. Analizom *podstringova y* po redcima blokova i uzorka za biometrijske točke može se primijetiti da se kod uzorka slike na kojoj je izvršen napad Gaussovim šumom razlikuju oni kod kojih se pojavljuju *podstringovi* $y_3 = (010)$ i $y_6 = (101)$. Ako se pretpostavi da su to *stringovi* dobiveni od piksela u sredini na kojima se pojavljuje šum, jednostavnom metodom zamjene *podstringova* $y_3 = (010)$ s $y_0 = (000)$ i $y_6 = (101)$ s $y_8 = (111)$, rezultat algoritma može se drastično poboljšati (0,0000).



(a)

(b)

Slika 60. Usporedba MCT uzorka (a) originalne slike i (b) slike na kojoj je izvršen napad Gaussovim šumom

7.4. Mjerenje točnosti algoritama

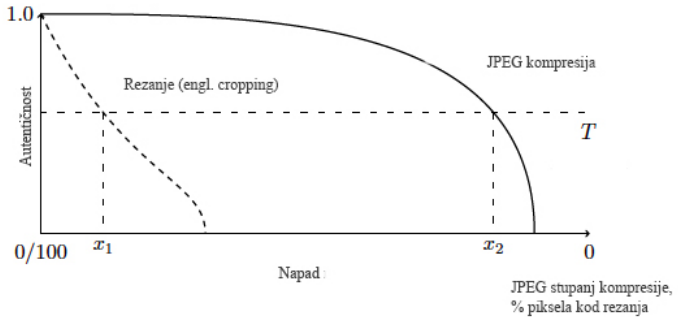
Točnost algoritma percepcijskih sažetaka moguće je prikazati mjerenjem pogrešaka u radu algoritama. No, tijekom pregleda literature u području istraživanja percepcijskih sažetaka nije se naišlo na standardne metode za mjerenje pogrešaka. Pojedini autori kao što je Zauner (Zauner, 2010.) ili Weng (Weng, 2012.) primjećuju da algoritmi za izradu percepcijskh sažetaka pokazuju sličnost s algoritmima koji se upotrebljavaju u biometrijskoj autentikaciji, stoga u radovima za mjerenje pogrešaka upotrebljavaju one koji se upotrebljavaju i za provjeru točnosti u biometrijskim sustavima, a to su stopa ispravne detekcije (engl. *true positive (TP)*) odnosno P_d (vjerojatnost ispravne detekcije) i stopa lažne detekcije (engl. *false positive (FP)*) odnosno P_f (vjerojatnost lažne detekcije). Kada se usporede vrijednosti percepcijskog sažetka dviju slika, udaljenost d između njih može se mjeriti s postavljenim pragom T što je opisano u prethodnom potpoglavlju. Tada je moguće rješenje:

R_o – te su dvije slike različite;

R_1 – te su dvije slike slične.

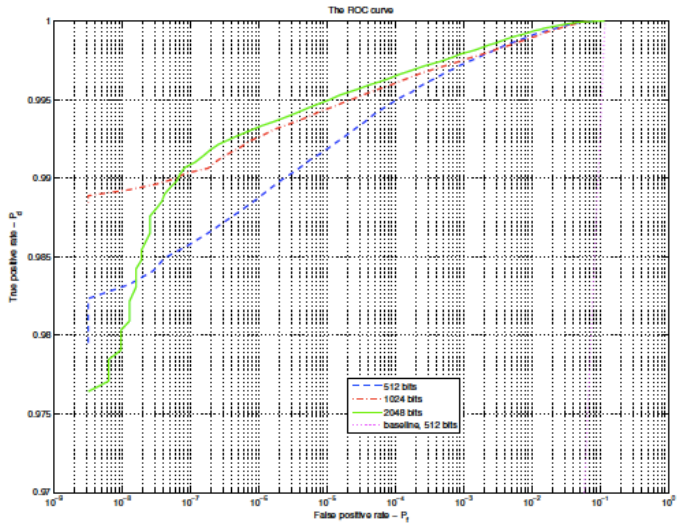
Rješenje R_o jest odabir ako je $d > T$. Inače je odabir R_1. Budući da rješenje ovisi o pragu T, njegov je odabir vrlo važan. Ako je vrijednost praga T postavljena prenisko, sve slične slike bit će označene kao različite i obrnuto: ako je vrijednost praga T postavljena previše visoko, sve različite slike bit će označene kao slične.

U radovima u kojima se opisuju u vrednovanju upotrijebljeni algoritmi, vrijednosti praga T različito su postavljene. Tako Zauner (Zauner, 2010.) za DCT algoritam vrijednost praga postavlja na visokih 0,4000, odnosno sve slike čiji je rezultat usporedbe percepcijskih sažetaka ispod te vrijednosti označene su kao slične. Monga i suradnici (Monga et al., 2006.) za VFPH algoritam u vrednovanju upotrijebljenom alatu (Hashing toolbox) za prag T upotrebljavaju vrijednost 0,2000, a za DWT algoritam niskih 0,0800. Ističu da postavljanje vrijednosti praga T ovisi o namjeni odabranih algoritama te odabranim napadima na slike. Tako Zauner opisuje i da utvrđivanje autentičnosti slika kod različitih napada modifikacijom i manipulacijom (npr. JPEG kompresijom i rezanjem (engl. *cropping*)) na sliku uz jednako postavljeni prag nije isto što je prikazano na slici 61.



Slika 61. Odnos napada i autentičnosti kod različitih napada uz isto postavljen prag T (obrada prema Zauner, 2010.)

Isto tako, potrebno je istaknuti da se točnost u slučaju identifikacije, odnosno usporedbe (1 : N) kada se testirani uzorak uspoređuje s *N* predložaka u bazi, može prikazati kao odnos između P_d i P_f s pomoću ROC (engl. *receiver operating characteristic*) krivulje (slika 62.). U dvodimenzionalnom grafikonu stopa ispravnih detekcija P_d prikazana je na osi *y*, a stopa lažnih detekcija P_f na osi *x*. Tipična ROC krivulja ima visoku vrijednost P_d, a nisku vrijednost P_f. Za postavljanje ispravne vrijednosti praga *T* potrebno je definirati i pojam stope lažno negative detekcije (engl. *false negative (FN)*) odnosno P_m (vjerovatnost lažno negativne detekcije). Prema definiciji P_m = 1-P_d.



Slika 62. ROC krivulja za testirane algoritme (Weng, 2012.)

Tada se može definirati i točka EER (engl. *equal error rate*) gdje je $P_m = P_f$. (Weng, 2012.).

Budući da u disertaciji nije upotrijebljena identifikacija, odnosno usporedba (1 : *N*) za uzorke biometrijskih karakteristika, već samo autentikacija odnosno usporedba (1 : 1), vrijednost praga *T* u testu točnosti postavljena je na 0,1500 odnosno 85%. Takva vrijednost postavljenog praga obično je značajka biometrijskih sustava za autentikaciju u kojima je cilj dobiti što bolji rezultat kako bi i utvrđivanje autentičnosti odnosno prepoznavanje osoba bilo što preciznije (Jain, 2005.). Svi rezultati usporedbe dvaju percepcijskih sažetaka ispod te vrijednosti (bliže 0) bili su označeni kao autentični i utvrđena je sličnost njihovih slika. Tijekom testiranja točnosti primijećeno je i da pojedini algoritmi pokazuju velik broj lažno pozitivnih i lažno negativnih detekcija u određenim situacijama što najbolje pokazuje primjer s biometrijskim karakteristikama lica koje su upotrijebljene u testu. Primjer je dodavanje

objekta u pozadini testiranom uzorku biometrijske karakteristike lica (što je prikazano na slici 63.).

Slika 63. Promjena pozadine na slici biometrijske karakteristike lica

DCT algoritam daje rezultat od 0,09375, dok MH algoritam daje rezultat od 0,2100. DWT algoritam pokazuje rezultat od 0,1122, a VFPH 0,1155. BMV algoritam dao je rezultat 0,2639. Iz dobivenih rezultata vidljivo je da bi DCT, DWT i VFPH algoritmi, uz postavljeni prag $T = 0{,}1500$ percepcijske sažetke označili kao autentične, dok bi ih MH algoritam i BMV algoritam označili kao neautentične. Na novorazvijeni MCT algoritam promjena pozadine ne utječe što je vidljivo iz dobivenog rezultata (0,0000).

U drugom primjeru uklonjena je pozadina slike da bi se dobilo segmentirano lice osobe (slika 64.) Dobiveni rezultati usporedbe percepcijsih sažetaka s pomoću testiranih algoritama u tom primjeru (DCT (0,4531), MH (0,4513), BMV (0,4444), DWT (0,2202) i VFPH (0,4169)) pokazuju da su svi algoritmi pokazali da te dvije slike nisu slične, odnosno ne bi utvrdili autentičnost. Na novorazvijeni MCT algoritam takva promjena također ne utječe što je vidljivo iz dobivenog rezultata (0,0000) pod uvjetom da biometrijske točke budu na istim lokacijama, bez obzira na veličinu slike.

Slika 64. Segmentirano lice bez pozadine kod biometrijske karakteristike lica

Iz testa točnosti vidljivo je da testirani algoritmi kod ovakvih situacija generiraju velik broj pogrešaka. Pogreške u njihovu radu javljaju se najčešće jer analiziraju velik broj atributa koji su nepotrebni odnosno višak kao što je pozadina, a također ne mogu prepoznati male promjene na slikama što je čest slučaj u biometrijskoj autentikaciji. Drugi razlog jest taj što se temelje na različitim metodama. Tako četiri algoritma (DCT, MH, BMV, DWT) analiziraju globalne atribute slika, a samo dva (VFPH i novorazvijeni MCT algoritam) analiziraju lokalne atribute slika. Rezultati istraživanja pokazali su veću točnost novorazvijenog MCT algoritama u odnosu na ostale algoritme jer se pri njegovu radu upotrebljavaju lokalni atributi slika s precizno odabranim specifičnim regijama na slici čime je potvrđen i drugi dio postavljene hipoteze. Test točnosti također pokazuje da bi samo novorazvijeni MCT algoritam bio prikladan za upotrebu u području biometrije odnosno biometrijske autentikacije, a ostali algoritmi, iako u testu robusnosti uz određene kriterije pokazuju zadovoljavajuće rezultate, u testu točnosti pokazuju velik broj pogrešaka u pojedinim situacijama.

Potrebno je istaknuti i to da su svi algoritmi uspješno utvdili različitost slika u trećem primjeru kad je upotrijebljena slika iz prethodno opisane BioID baze s uzorcima biometrijske karakteristike lica druge osobe uz istu testnu pozadinu (slika 65.).

Slika 65. Biometrijska karakteristika lica druge osobe s istom pozadinom

Rezultati algoritama u toj situaciji (DWT 0,2103; VFPH 0,2753; BMV 0,3472; DCT 0,4687; MH 0,5243; MCT 0,4877) pokazuju i da je novorazvijeni MCT algoritam najtočniji. Rezultat udaljenosti od 0,5000 se označava kao najtočniji u slučajevima kada su slike, a tako i percepcijski sažetci potpuno različiti i kada se percepcijski sažetci koriste u svrhu diskriminativnosti što su u svojim radovima opisali autori poput Zaunera (Zauner, 2010.), Wanga i suradnika (Wang et al., 2013.) te Tanga i suradnika (Tang et al., 2016.) kao i mnogi drugi spomenuti u ovoj disertaciji, a koji su se bavili područjem percepcijskih sažetaka.

8. ZAKLJUČAK

Autentikacija u biometriji označava usporedbu (1 : 1), odnosno pohranjeni predložak uspoređuje se s prikupljenim uzorkom na senzoru te se na temelju postavljenog praga odlučuje o autentičnosti korisnika. Budući da su i predložak i uzorak zapravo digitalne slike, kod većine biometrijskih karakteristika (pogotovo fizičkih) oni se prije usporedbe i odluke o autentičnosti moraju obraditi da bi se izdvojili atributi za analizu. Pritom se primjenjuju mnogobrojne metode i algoritmi koji imaju određena ograničenja te generiraju manji ili veći broj pogrešaka što je opisano i u disertaciji.

Ova disertacija bavi se percepcijskim sažetcima. Percepcijski sažetak definiran je kao „otisak" digitalne slike izveden iz različitih atributa njezina sadržaja, a upotrebljava se za provjeru autentičnosti ili identifikaciju digitalnih slika. Motivacija za pisanje ove disertacije proizašla je iz činjenice da se u analizi literature, a kasnije i u predistraživanju, utvrdila sličnost u provjeri autentičnosti percepcijskih sažetaka i autentičnosti osoba u biometrijskim sustavima.

Istraživanje je započelo analizom relevantne literature i uočeno je da postoji mnogo radova u kojima se opisuju algoritmi izradu percepcijskih sažetaka, ali ne postoje radovi koji se bave upotrebom percepcijskih sažetaka u području biometrije. Isto tako, zbog različitih metoda na kojima se ti algoritmi temelje vidljiva su ograničenja i nedostaci u robusnosti i točnosti.

U ovoj disertaciji predložen je novi pristup izrade percepcijskih sažetaka, a koji se temelji na izdvajanju atributa specifičnih interesnih regija na uzorcima biometrijskih karakteristika i njihovom analizom metodom modificirane cenzus transformacije. Metodom modificirane cenzus transformacije uspoređuje se intenzitet svakog pojedinog piksela odabrane regije slike s prosječnom vrijednošću intenziteta te regije. Na temelju usporedbe je li intenzitet pojedinog piksela veći od prosječnog intenziteta ili nije, generira se percepcijski sažetak odabrane regije.

Vrednovanje novorazvijenog algoritama za izradu percepcijskih sažetaka provedeno je radi ispitivanja mogućnosti njegove upotrebe u biometrijskoj autentikaciji. Istraživanje je pokazalo da percepcijski sažetci zbog svojih karakteristika imaju određene prednosti te da se mogu upotrebljavati u biometrijskim sustavima za autentikaciju. Neke od prednosti jesu mala veličina, standardiziranost, robusnost na manipulacije i modifikacije te sigurnost upotrebe. Mala veličina omogućuje brzu usporedbu predloška i uzorka; gotovo u stvarnom vremenu (engl. *real time*). Zbog istog razloga provjera autentičnosti s pomoću percepcijskih sažetaka u

novijim biometrijskim sustavima, koji su fizički udaljeni te je potrebno slanje podataka putem mreže, nije problem. Isto tako, upotrebom percepcijskih sažetaka mogao bi se riješiti velik problem standardizacije i kompatibilnosti u biometriji zbog pohrane percepcijskih sažetaka u binarnom obliku. Istraživanje je također pokazalo robusnost algoritama za izradu percepcijskih sažetaka na manipulacije i modifikacije slika što predstavlja problem u radu mnogih postojećih biometrijskih sustava. Sigurnost upotrebe postignuta je primjenom nasumičnih i tajnih ključeva u postupku izrade percepcijskih sažetaka što je opisano ranije u disertaciji te koji bi zbog toga trebali biti neupotrebljivi ako bi dospijeli u krive ruke.

Novorazvijeni algoritam je u vrednovanju opisanom u sedmom poglavlju uspoređen s pet drugih algoritama za izradu percepcijskih sažetaka, a koji su u literaturi isticani kao standardni te su ih drugi autori upotrebljavali za vrednovanje svojih novorazvijenih algoritama. Pri vrednovanju algoritama upotrijebljeni su po kategorijama podijeljeni negeometrijski, geometrijski i zlonamjerni kriteriji.

Od ukupno šest opisanih algoritama koji se temelje na različitim i u disertaciji opisanim metodama, četiri analiziraju globalne atribute slika, a samo dva (uključujući i novorazvijeni algoritam) analiziraju lokalne atribute slika. Ostali algoritmi koji upotrebljavaju globalne atribute slika, uključujući i VFPH algoritam, koji upotrebljava nasumične lokalne atribute slike, iako u testu robusnosti pri određenim kriterijima pokazuju zadovoljavajuće rezultate, u testu točnosti pokazuju velik broj pogrešaka. Pogreške u njihovu radu javljaju se najčešće jer analiziraju velik broj atributa koji su nepotrebni, odnosno višak za biometrijsku autentikaciju kao što je pozadina, a također ne mogu prepoznati male promjene na slikama (BMV i DWT) što je čest slučaj u biometrijskoj autentikaciji. Ono što je također značajno jest da je u ovoj disertaciji prikazan i nov način za uspoređivanje percepcijskih sažetaka koji nisu jednake duljine Damerau-Levenshteinovom metodom što u prethodnim istraživanjima koji su se bavili percepcijskim sažetcima nije bilo moguće.

Rezultati istraživanja pokazali veću točnost novorazvijenog algoritama koji upotrebljava lokalne atribute slika s precizno odabranih specifičnih regija na slici pri postavljenim kriterijima potrebnima za upotrebu u području biometrije. Što se tiče testa robusnosti novorazvijeni algoritam je robusniji od ostalih algoritama u dvije od tri kategorije napada (geometrijski i zlonamjerni). Iz dobivenih rezultata testa robusnosti može se zaključiti da bi novorazvijeni MCT algoritam u ovakvom obliku, bio najprikladniji u slučajevima provjere uzoraka biometrijskih karakteristika koji su označeni zbog nedovoljne kvalitete te koje bi postojeći biometrijski sustavi odbacivali kao neispravne zbog nedostatka dijelova

slike, loše prezentacije ili njihovog položaja (rotacija) odnosno gdje god dolazi do otežanog čitanja atributa na senzoru.

Iako je hipoteza disertacije ukupno potvrđena, iz rezultata robusnosti vidljivo je da rezultati pojedinačno ovise o upotrebljavanoj biometrijskoj karakteristici kao i o vrsti napada. Jedan od uočenih problema jest i manja robusnost algoritma na negeometrijske napade, iako u usporedbi s drugim testiranim algoritmima kod određenih kriterija i biometrijskih karakteristika pokazuje i bolje rezultate. Nedostatak novorazvijenog algoritma jest taj što se temelji na metodi koja analizira samo jednu komponentu izdvojenih atributa, a to je boja odnosno gradijent. To se posebno pokazalo kao problem kod modifikacija i manipulacija nad slikama koje utječu na boju kao što je napad Gaussovim ili binarnim šumom. U poglavlju Poboljšanje novorazvijenog algoritma nudi se djelomično rješenje tog problema što je vidljivo iz dobivenih rezultata.

Također, kao nedostatak algoritma može se istaknuti i to što je za izradu percepcijskih sažetaka potrebno imati već unaprijed označene i pohranjene lokacije biometrijskih točaka, ili ih je potrebno ručno označavati prilikom izrade, što komplicira i produljuje vrijeme izrade. Kao nedostatak algoritma pokazalo se i nepostojanje analize odnosa i udaljenosti biometrijskih točaka koja postoji u pojedinim standardnim metodama i algoritmima za biometrijsku autentikaciju, a koja bi pridonijela točnosti i robusnosti novorazvijenog algoritma te bi se mogla napraviti i njihova usporedba što će biti prikazano u nekim budućim radovima. Isto tako, na robusnost i točnost algoritma vjerojatno bi utjecala i promjena duljine percepcijskih sažetaka koja se može postići dodavanjem ili oduzimanjem točaka odnosno upotrijebljenih atributa, a također nije prikazana u ovoj disertaciji te je isto ostavljena za neke buduće radove. U planu je i ispitivanje novorazvijenog algoritma na ostalim biometrijskim karakteristikama.

Zaključno, na kraju se može ponoviti napisano i u uvodu. Implementacija opisanog rješenja ima znanstvenu važnost i mogućnost praktične primjene. Drugim riječima, predloženo istraživanje predstavlja novi pristup odabiru, razvoju i procjeni algoritama percepcijskih sažetaka radi upotrebe u biometrijskim sustavima autentikacije.

LITERATURA

1. Abaza, A., Ross, A., Herbert, C., Harrison, M. A. F., and Nixon, M. S. 2013. A survey on ear biometrics. ACM Comput. Surv. 45, 2, Article 22 (February 2013), 35 pages.
2. Agarwal, S., Dhawan, S., Singh, P., & Thakur, N.. (2015). Implementation of an efficient Fuzzy Logic based Information Retrieval System. *EAI Endorsed Trans. Scalable Information Systems, 2*, e5.
3. Alaswad A. O., Montaser A. H., Mohamad F. E. ,Vulnerabilities of Biometric Authentication "Threats and Countermeasures", International Journal of Information & Computation Technology. ISSN 0974-2239 Volume 4, Number 10 (2014), pp. 947-958
4. Andabak A., Gaura I., Utjecaj kompresije na kvalitetu slike, seminar iz kolegija Primjena digitalne fotografije u reprodukcijskim medijima, Grafički fakultet Sveučilišta u Zagrebu, 2010., dostupno na: http://repro.grf.unizg.hr/media/download_gallery/UTJECAJ%20KOMPRESIJE%20NA%20KVALITETU%20SLIKE.pdf, (pristupano 23.8.2016.)
5. Arambam Neelima, Kh. Manglem Singh, "A Short Survey on Perceptual Hash Function" ADBU J.Engg Tech, 1(2014) 0011405(8pp)
6. Baksi U., Singhal R., A Survey On Face Detection Methods And Feature Extraction Techniques Of Face Recognition, International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 3, Issue 3, May-June 2014
7. Baltzakis H., Papamarkos N.: A new signature verification technique based on a two-stage neural network classifier/ Engineering Applications of Artificial Intelligence 14 (2001), pp. 95–103
8. Bay H. et al, Speeded-Up Robus Features (SURF), Computer Vision and Image Understanding 110 (2008) 346–359, Elsevier, 2008.
9. Bertolami J., Perceptual hashing, http://www.bertolami.com/index.php?engine=blog&content=posts&detail=perceptual-hashing, 2014. (pristupano 2.3.2015.)
10. Bharadwaj S., Vatsa M., Singh R., Biometric quality: a review of fingerprint, iris, and face, EURASIP Journal on Image and Video Processing 2014, 2014:34, dostupno na: http://jivp.eurasipjournals.com/content/2014/1/34, (pristupano 12.9.2016.)

11. Bhatacherjee S., Vandergheynst P., End-stopped wavelets for detection low-level features, Proc. SPIE, Wavelet Applications in Signal and Image Processing VII, pp. 732-741, 1999.
12. Bilan O., Nastavni materijali iz kolegija, Digitalna obrada zvučnih signala SPIE09, Sveučilišni studijski centar za stručne studije, 2010., http://www.audiologs.com/ozrenbilan/06_DSP.pdf , (pristupano 27.7.2016.)
13. Biometrics Ideal Test (BIT) databases, Tinieu T., Center for Biometrics and Security Research (CBSR), China, http://biometrics.idealtest.org/, (pristupano: 21.4.2014.)
14. Biometrics Institute, Biometrics institute industry survey 2015, Tech. rep., Biometrics Institute, 2015.
15. Bjeropera A.: Poželjna svojstva diskretne wavelet transformacije za primjenu u kompresiji slike, Sveučilište u Dubrovniku Odjel za elektrotehniku i računarstvo, 2012., https://www.fer.unizg.hr/_download/repository/Anamaria_Bjelopera,_rad_za_KDI.pdf , (pristupano 12.7.2016.)
16. Bloom B. S.: Taxonomy of Educational Objectives, Longman, New York, 1956.
17. Chen J., Kellokumpu V., Zhao G., Pietikäinen M. , RLBP: Robus Local Binary Pattern; The British Machine Vision Conference (BMVC), 2013., dostupno na: http://www.bmva.org/bmvc/2013/Papers/paper0122/paper0122.pdf, (pristupano: 29.8.2016.)
18. Cormen T.H. et al., Introduction to Algorithms . McGraw-Hill, 2nd edition, 2001.
19. Coskun, B. and Memon, N.: Confusion/diffusion capabilities of some robus hash functions. In Proceedings of the Conference on Information Sciences and Systems (CISS), pp. 1188-1193. IEEE, Mar. 2006.
20. Creswell JW. Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (2nd Edition). Sage Publications, Thousand Oaks, California; 2002.
21. Crowley L. J., FGnet - IST-2000-26434, Face and Gesture Recognition Working group, dostupno na: http://www-prima.inrialpes.fr/FGnet/html/home.html, (pristupano 12.2.2016.)
22. Davarzani R., Mozaffari S., Yaghmaie Kh., Image authentication using LBP-based perceptual image hashing, Journal of AI and Data Mining Vol 3, No 1, 2015, pp. 21-30.

23. De Roover, C.; De Vleeschouwer, C.; Lefebvre, F.; Macq, B., "Robus image hashing based on radial variance of pixels," Image Processing, 2005. ICIP 2005. IEEE International Conference on , vol.3, no., pp.III,77-80, 11-14 Sept. 2005
24. Dolecek L.: Using Reed–Muller RM Codes Over Channels With Synchronization and Substitution Errors, IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 53, NO. 4, APRIL 2007
25. Dujella A., Maretić M.: Kriptografija, Udžbenik Sveučilišta u Zagrebu, Element, Zagreb, 2007., ISBN: 978-953-197-565-0
26. F. Breitinger, H. Liu, C. Winter, H. Baier, A. Rybalchenko, and M. Steinebach. "Towards a process model for hash functions in digital forensics," 5th International Conference on Digital Forensics & Cyber Crime, September 2013.
27. Fang L., Cheng L-M., Wave Atom-Based Perceptual Image Hashing Against Content-Preserving and Content-Altering Attacks
28. Fridrich, J. & Goljan, M. (2000). Robus hash functions for digital watermarking, Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'00), IEEE Computer Society,Washington, DC, USA, pp. 178–183.
29. Froba, B., Ernst, A.: Face detection with the modified census transform. In: Proc. 6th IEEE International Conference on Automatic Face and Gesture Recognition, IEEE Computer Society Press (2004) 91-96
30. Govindaraj P., Sandeep R., Ring Partition and DWT based Perceptual Image Hashing with Application to Indexing and Retrieval of Near- Identical Images, IJRECE VOL. 3 ISSUE 2, APR-JUNE 2015
31. Grgić S., Kerš K., Grgić M., Image Compression Using Wavelets", Proceedings of the IEEE International Symposium on Industrial Electronics, vol.1, ISIE'99, Bled, Slovenija, 1999. pp. 99-104
32. Grother P., Tabassi E., Performance of biometric quality measures. EE Trans. Pattern Anal. Mach. Intell. 29(4), 531–524 (2007)
33. Hadmi A., Puech W., Es Said Ait B. Ouahman Ait A. (2012): Perceptual Image Hashing, Watermarking - Volume 2, Dr. Mithun Das Gupta (Ed.), ISBN:978-953-51-0619-7, InTech, available from: http://www.intechopen.com/books/watermarking-volume-2/perceptual-image-hashing

34. Han, S. H. & Chu, C. H. (2010). Content-based image authentication: current status, issues, and challenges, International Journal of Information Security 9: 19–32.

35. Hamon, K.; Schmucker, M.; Xuebing Zhou, "Histogram-Based Perceptual Hashing for Minimally Changing Video Sequences," Second International Conference on Automated Production of Cross Media Content for Multi-Channel Distribution, 2006. AXMEDIS '06. , pp.236,241, 13-15 Dec. 2006

36. Heeringa W., Measuring Dialect Pronunciation Differences using Levenshtein Distance, 2004, University of Groningen, Faculty of Arts, the Humanities Computing department

37. Heineman G. T., Pollice G., Selkow S.: Algorithms in a Nutshell, O'Reilly Media, Inc., 2009.

38. Howell R., Dept. of Computing and Information Sciences, Kansas State University Manhattan, Lecture, 2008., http://people.cis.ksu.edu/~rhowell/asymptotic.pdf (pristupano: 25.4.2015.)

39. Hrvatska enciklopedija – mrežno izdanje, Percepcija, Leksikografski zavod Miroslav Krleža, 2017., dostupno na: http://www.enciklopedija.hr/natuknica.aspx?ID=47529, (pristupano 12.12.2017.)

40. ICFHR 4NsigComp, Biometrics Signature Database, dostupno na: http://www.iaprtc11.org/mediawiki/index.php/ICFHR_2012_Signature_Verification_Competition_(4NSigComp2012), (pristupano 23.8.2016.)

41. Jain A. K., Ross A., Prabhakar S., An Introduction to Biometric Recognition, IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, Vol. 14, No. 1, January 2004.

42. Jain A.K., Patrick Flynn, Arun A. Ross: Handbook of Biometrics, Springer, 2008.

43. Jain, A.K., Pankanti, S., Prabhakar, S., Hong, L., Ross, A., Wayman, J.L. : Biometric Tutorial, Michigan State University, dostupno na: http://biometrics.cse.edu/icprareviewtalk.pdf, 2005. , (pristupano 23.8.2016.)

44. Jančić M., NORME ZA KOMPRESIJU MIRNIH SLIKA, Fakultet elektrotehnike i računarstva, http://www.vcl.fer.hr/dtv/jpeg/dct.htm, 2002.

45. Just A., Rodriguez Y., Marcel S., Hand Posture Classification and Recognition using the Modified Census Transform, *7th International Conference on Automatic Face and Gesture Recognition (FGR06)*, Southampton, 2006, pp. 351-356.

46. Kafai M., Eshghi K., Bhanu B.: Discrete Cosine Transform Locality-Sensitive Hashes for Face Retrieval, IEEE Transactions on multimedia, Vol. 16, Vo. 4, June 2014, pp. 1090-1103

47. Kailasanathan, C.; Naini, R.S.; Ogunbona, P., "Compression tolerant DCT based image hash," Distributed Computing Systems Workshops, 2003. Proceedings. 23rd International Conference on , vol., no., pp.562,567, 19-22 May 2003

48. Khelifi, F. & Jiang, J. (2010). Perceptual image hashing based on virtual watermark detection, IEEE Transactions on Image Processing 19: 981–994.

49. Kozat, S. S., Venkatesan, R. & Mihçak, M. K. (2004). Robus perceptual image hashing via matrix invariants, Proceedings of the IEEE International Conference on Image Processing (ICIP'04), pp. 3443–3446.

50. Krawetz N., Look like it, http://www.hackerfactor.com/blog/index.php?/archives/432-Looks-Like-It.html, 2011., (pristupano 24.3.2015.)

51. Kumar, A. and Zhang, D.: Biometric Recognition Using Feature Selection and Combination. In Proceedings of Fifth International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA), pages 813-822, Rye Brook, 2005.

52. Kumbharana D., Meva C.K., Comparative Study of Different Fusion Techniques in Multimodal Biometric Authentication, *International Journal of Computer Applications, Volume 66 , No.19, March 2013, str. 16-19*

53. Kunhu, A.; Al-Ahmad, H., "A new multi watermarking algorithm based on DWT and hash functions for color satellite images," Electronics, Circuits, and Systems (ICECS), 2013 IEEE 20th International Conference on , vol., no., pp.429,432, 8-11 Dec. 2013

54. Lazarević, D. et. al., 2014. Postojeće tehnike za segmentaciju slike recent image segmentation techniques. *ZBORNIK abstrakata / Festival kvaliteta 2014*, pp.26-1-11.

55. Lees K., Image Compression Using Wavelets, 2002., dostupno na: http://web.cecs.pdx.edu/~mperkows/CAPSTONES/HAAR/u9kvl.pdf, (pristupano 12.7.2016.)

56. Lef`ebvre, F., Macq, B., and Legat, J.D.: RASh: RAdon Soft Hash algorithm. In Proceedings of the European Signal Processing Conference (EUSIPCO), vol. I, pp. 299–302. European Association for Signal Pro- cessing, Sept. 2002.

57. Lei, Y., Wang, Y. & Huang, J.,Robus image hash in radon transform domain for authentication, Signal Processing: Image Communication 26, pp. 280–288., 2011.

58. Leutenegger, S., M. Chli and R. Siegwart. "BRISK: Binary Robus Invariant Scalable Keypoints", Proceedings of the IEEE International Conference, ICCV, 2011.

59. Levitin A.: Introduction to The Design & Analysis of Algorithms, Addison Wesley, 2nd edition, 2007.

60. Lew M., et al., ACM Transactions on Multimedia Computing, Communications, and Applications, pp. 1–19, 2006., http://www.liacs.nl/home/mlew/mir.survey16b.pdf (pristupano 22.7.2015.)

61. Li W., Preneel B., Attacking Some Perceptual Image Hash Algorithms, 2007, IEEE International Conference on Multimedia and Expo, 2007., Bejing, p. 879 – 882, ISBN: 1-4244-1016-9

62. Li Z. S., Jain K. A.: Encyclopedia of Biometrics, Springer, 2009.

63. Lin, C. Y. & Chang, S. F. (2001). A robus image authentication method distinguishing jpeg compression from malicious manipulation, IEEE Transactions on Circuits and Systems for Video Technology 11(2): 153–168.

64. Liverovski P.: How to fight against reposts or couple of words about perceptual hashes, 2014., dostupno na: https://habrahabr.ru/post/237307, (pristupano 27.7.2016.)

65. Lončarić S.: Ekstrakcija značajki slike, FER, Predavanja sa kolegija Digitalna obrada slike, 2008., dostupno na: https://www.fer.unizg.hr/_download/repository/08-OI-EkstrakcijaZnacajkiSlike.pdf, (pristupano 26.7.2016.)

66. Lu, C. S. & Liao, H. Y. M. (2003). Structural digital signature for image authentication: an incidental distortion resistant scheme, IEEE Transactions on Multimedia 5(2): 161–173.

67. Lv X., Robus Digital Image Hashing Algorithms for Image Identication, thesis, The University of British Columbia, Vancouver, 2013.

68. Lv X.; Wang, Z.J., Perceptual Image Hashing Based on Shape Contexts and Local Feature Points, Information Forensics and Security, IEEE Transactions on, vol.7, no.3, pp.1081,1093, June 2012

69. Mallat S., A Wavelet Tour of Signal Processing , Academic Press, San Diego, second ed., 1999.

70. Mamillapalli V., Handling the Problems in Biometrics, 2014, Foundations of Information Assurance, dostupno na: https://dl.packetstormsecurity.net/papers/general/Handling_Problems_in_Biometrics.pdf, (pristupano: 21.9.2016.)
71. MathWork, Understanding What Happens in Geometric Transformation, dostupno na: https://www.mathworks.com/help/images/understanding-what-happens-in-geometric-transformation.html, (pristupano 27.8.2016.)
72. Meixner, A. and Uhl, A.: Robusness and security of a wavelet-based CBIR hashing algorithm. In Proceedings of the Workshop on Multimedia and Security (MM&SEC), pp. 140-145. Association for Computing Machinery, Sept. 2006.
73. Menezes, A. J., Vanstone, S. A., Oorschot, P. C. V. (1996), Handbook of Applied Cryptography, 1st Edn, CRC Press, Inc., Boca Raton, FL, USA.
74. Mesarević S., Multimodalni biometrijski sistemi, Univerzitet Signidunum, Fakultet za poslovnu informatiku, magistarsjka teza, Beograd, 2007.
75. Mohamed, M.A., Mertsching, B.: TV-L1 optical flow estimation with image details recovering based on modifed census transform. In Bebis, G., Boyle, R., Parvin, B.,Koracin, D., Charless, F., Wang, S., Choi, M.H., Mantler, S., Schulze, J., Acevedo, eds: Advances in Visual Computing. Volume 7431 of LNCS. Springer, Berlin (2012) 482-491
76. Monga V., Banerjee A., Evans B. L., "A clustering based approach to perceptual image hashing," IEEE Trans. Inf. Forensics Security, vol. 1, no. 1, pp. 68–79, Mar. 2006.
77. Monga V., Evans B.L.: Perceptual Image Hashing Via Feature Points: Performance Evaluation and Tradeoffs, Image Processing, IEEE Transactions on (Volume:15, Issue: 11), 2006. p. 3452 – 3465, ISSN: 1057-7149, INSPEC Accession Number: 9141133
78. Monga V., Vats D, Evans L. B., Image Hashing Toobox in Matlab, 2006., dostupno na: http://users.ece.utexas.edu/~bevans/projects/hashing/toolbox/, (pristupano: 21.3.2015.)
79. Monga, V. (2005). Perceptually based methods for robus image hashing (Ph.D. thesis), in Electrical Engineering, Electrical and Computer Engineering, The University of Texas at Austin.
80. Muller, T., Rannacher, J., Rabe, C., Franke, U.: Feature- and depth-supported modifed

total variation optical flow for 3D motion field estimation in real scenes, In: Proc. 24th IEEE Conference on Computer Vision and Pattern Recognition, Colorado Springs, IEEE Computer Society Press (2011) 1193-1200

81. Nagarajan S. K., Saravanan S.: Content-based Medical Image Annotation and Retrieval using Perceptual Hashing Algorithm, VIT University, India, IOSR Journal of Engineering Apr. 2012, Vol. 2(4) pp: 814-818
82. Nan L., Jiafen L., Qing L., Xubin L., Jiang D., Online Signature Verification Based on Biometric Features, 2016, 2016 49th Hawaii International Conference on System Sciences
83. Nandakumar K.: Integration of multiple cues in biometric systems, Technical Report, Master's Thesis, Michigan State University, 2005.
84. Nappi M., Ricciardi S., Tistarelli M., Real Time 3D Face-Ear Recognition on Mobile Devices: New Scenarios for 3D Biometrics “in-the-Wild”, Using Computer Vision, Pattern Recognition and Machine Learning Methods for Biometrics, 2017.
85. Navajit S., Prabin K. B., Perceptual hash function for scalable video, International Journal of Information Security, Volume 13, Issue 1, February 2014, ISSN: 1615-5262, Springer Berlin Heidelberg, 2014.
86. Nimac L. Pregled biometrijskih metoda identifikacije, dostupno na: http://sigurnost.zemris.fer.hr/protokoli/2007_nimac/Seminar[2007]Nimac_Luka.html, 2007., (pristupano 12.8.2016.)
87. Obdrzalek D., S. Basovnik, L. Mach, and A. Mikulik. "Detecting Scene Elements Using Maximally Stable Colour Regions," Communications in Computer and Information Science, La Ferte-Bernard, France; 2009, vol. 82 CCIS (2010 12 01), pp 107–115.
88. Ojala T., Pietikäinen M., and Harwood D. (1994), "Performance evaluation of texture measures with classification based on Kullback discrimination of distributions", Proceedings of the 12th IAPR International Conference on Pattern Recognition (ICPR 1994), vol. 1, pp. 582 - 585.
89. Ojala T., Pietikäinen M., Mäenpää T., Multiresolution Gray-scale and Rotation Invariant Texture Classification with Local Binary Patterns, IEEE TPAMI, 2002.

90. Oravec M. et al., Mobile ear recognition application, IEEE, 2016 International Conference on Systems, Signals and Image Processing (IWSSIP), Bratislava, Slovakia.

91. Ouyang J., Coatrieux G., Shu H.: Robus hashing for image authentication using quaternion discrete Fourier transform and log-polar transform, Digital Signal Processing, Vol. 38, Elsevier, March 2015.

92. Petrou M., Petrou C., Image Processing: The Fundamentals, Second Edition, John Wiley & Sons, Ltd. ISBN: 978-0-470-74586-1, 2010.

93. Pietikäinen M., Hadid A., Zhao G., Ahonen T., Computer Vision Using Local Binary Patterns, Springer, Volume 40, 2011, pp. 13-47

94. Prungsinchai S., Robus And Secure Perceptual Image Hashing In The Transform Domain, PhD thesis, University of Northumbria at Newcastle, 2014.

95. Pug A., Busch C., Ear Biometrics: A Survey of Detection, Feature Extraction and Recognition Methods, IET Biometrics, 2012

96. Radmilović Ž.: Biometrijska identifikacija, Policijska sigurnost, Zagreb, 2008., str. 159-180

97. Ramakrishnan M., Sujatha R., Sony Thangam S.B.: Chaotic neural network based hashing algorithm for image authentication, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 3, Issue 1, January 2014, ISSN (Print) : 2320 – 3765

98. Ramirez-Gutierrez K., Nakano-Miyatake M., Perez-Meana H., Image authentication using perceptual hashing, Academic Journals, Vol. 8(11), pp. 447-455, 18 March, 2013

99. Ranftl, R., Gehrig, S., Pock, T., Bischof, H.: Pushing the limits of stereo usingvariational stereo estimation. In: IEEE Intelligent Vehicles Symposium, Alcala de Henares, IEEE Computer Society Press (2012) 401-407

100. Rojković D., Raspoznavanje prometnih znakova križnom korelacijom, završni rad, Fakultet elektrotehnike i računarstva, Sveučilište u Zagrebu, 2009.

101. Rosten, E., and T. Drummond. "Fusing Points and Lines for High Performance Tracking," Proceedings of the IEEE International Conference on Computer Vision, Vol. 2 (October 2005): pp. 1508–1511.

102. Schneider M. and Chang S-F, “A robus content based digital signature for image

authentication", In Proceedings of the IEEE International Conference on Image Processing, vol.3, pp.227−230, Laussane, Switzerland, Sept. 16−19, 1996. at the 3rd International Conferences on Image Processing (ICIP) in 1996.

103. Schneider, M., Chang, S. F. (1996). A robus content based digital signature for image authentication, Proceedings of the IEEE International Conference on Image Processing (ICIP'96), Vol. 3, pp. 227–230.

104. Schowengerdt R. A., "Image Noise", dostupno na: http://www.dig.cs.gc.cuny.edu/seminars/IPCV/pres12.pdf, (pristupano 23.8.2016.)

105. Sekhar M., Sarika R., Kumar Ch. S., Rao K.V., Rao N. S.: An Attack on Image Authentication: Unaltered Histogram, International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 11 (2016), pp 7217-7222

106. Setyawan, I.; Timotius, I.K., "Digital image hashing using local histogram of Oriented Gradients," Information Technology and Electrical Engineering (ICITEE), 2014 6th International Conference on , vol., no., pp.1,4, 7-8 Oct. 2014

107. Shi, J., and C. Tomasi, "Good Features to Track," Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, June 1994, pp. 593–600.

108. Shradha K., Gupta P., Veer C., Loke A., Visual Based Image Search using Perceptual Hash Codes for Online Shopping, International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 3, March 2016.

109. Sović, I., Trogrlić D., Meštrović T., Draganović M., Lokalizacija pozicije registarskih pločica u slici, Sveučilište u Zagrebu, Fakultet elektrotehnike i računarstva Zavod za elektroničke sustave i obradu informacija, 2009., dostupno na: https://www.fer.unizg.hr/_download/.../Lokalizacija_registarskih_plocica_v11.0.pdf, (pristupano 23.7.2016.)

110. Standaert, F.X., Lef`ebvre, F., Rouvroy, G., Macq, B.M., Quisquater, J.J., and Legat, J.D.: Practical evaluation of a radial soft hash algorithm. In Proceedings of the International Symposium on Information Technology: Coding and Computing (ITCC), vol. 2, pp. 89–94. IEEE, Apr. 2005.

111. Stein, F.: Efficient computation of optical flow using the census transform. In Rasmussen, C.E., Bulthoff, H.H., Giese, M.A., Scholkopf, B., eds.: Pattern Recognition. Volume 3175 of LNCS. Springer, Berlin (2004) 79-86

112. Sulzberger C., The Levenshtein-Algorithm, dostupno na: http://www.levenshtein.net, (pristupano 12.8.2016.)
113. Swaminathan A., Yinian M., Wu M.: Robus and secure image hashing, Information Forensics and Security, IEEE Transactions on , vol.1, no.2, pp.215,230, June 2006
114. Swaminathan A., Yinian M., Wu M.: Security of feature extraction in image hashing, ICASSP (2) 2005, p. 1041-1044
115. Tang Z. et al.: Robus image hashing with dominant DCT coefficients, Optik - International Journal for Light and Electron Optics, Volume 125, Issue 18, Elsevier ,September 2014, pp. 5102–5107
116. Tang Z., Huang L., Dai Y., Yang F., Robus Image Hashing Based on Multiple Histograms, International Journal of Digital Content Technology and its Applications 6(23), pp. 39-47, December 2012
117. Tang Z., Zhang X., Li X., Zhang S., Robus Image Hashing With Ring Partition and Invariant Vector Distance, IEEE Transactions On Information Forensics And Security, Vol. 11, No. 1, January 2016
118. Toshiaki K.: Gradient orientation pattern matching with the Hamming distance, Pattern Recognition, Elsevier Ltd., Volume 47, Issue 10, October 2014, p. 3387–3404
119. Tuytelaars T., Mikolajczyk K. Local invariant feature detectors: a survey. Foundations and Trends in Computer Graphics and Vision, 3(3):177–280, July 2008.
120. University of British Columbia, 2013., dostupno na: https://www.cs.ubc.ca/~woodham/cpsc505/examples/edge.html, (pristupano 27.7.2016.)
121. Venkatesan R., Koon S.M., Jakubowski M. H. i Moulin P.: Robus image hashing, Proc. IEEE Conf. on Image Processing, September 2000.
122. Voloshynovskiy S. et al.: Conception and limits of robus perceptual hashing: towards side information assisted hash functions, Proc. SPIE 7254, Media Forensics and Security, 72540D, February 04, 2009; doi:10.1117/12.805919
123. Vukelić B., Bača M., Comparison of RADIAL variance based and Maar-Hildreth operator perceptual image hash functions on biometric templates, Central European Conference on Information and Intelligent Systems, CECIIS 2014, ISSN 1847-2001, p. 286-296, FOI Varaždin

124. Wang H., Yin B., Perceptual Hashing-Based Robus Image Authentication Scheme for Wireless Multimedia Sensor Networks, Hindawi Publishing Corporation International Journal of Distributed Sensor Networks, Volume 2013
125. Wang S., Zang X.: Recent development of perceptual image hashing, Journal of Shanghai University (English edition), August 2007, Vol 11, pp. 323-331, Springer, ISSN: 1007-6417 (Print) 1863-236X (Online)
126. Wang, Z., Bovik, A. C., Sheikh, H. R. & Simoncelli, E. P. (2004). Image quality assessment: From error visibility to structural similarity, IEEE Tansactions on Image Processing 13(4): 600–612.
127. Wang, Z., Bovik, A., Sheikh, H., and Simoncelli, E. Image quality assessment: From error visibility to structural similarity. IEEE Transactions on Image Processing 13, 4 (April 2004), 600–612.
128. Wayman J., Anil Jain, Davide Maltoni, Dario Maio (Eds): Biometric Systems: Technology, Design and Performance Evaluation, Springer, 2005.
129. Weng L. et al., Robus Image Content Authentication Using Perceptual Hashing and Watermarking Advances in Multimedia Information Processing – PCM 2012 Lecture Notes in Computer Science Volume 7674, 2012, pp 315-326
130. Weng, L., 2012. *Perceptual Multimedia Hashing*, PhD thesis, Katholieke Universiteit Leuven – Faculty of Engineering, dostupno na: http://www.cosic.esat.kuleuven.be/publications/thesis-217.pdf. (pristupano 3.3.2015.)
131. Wilson C., R., Hancock R. E., Levenshtein Distance for Graph Spectral Features, Pattern Recognition, 2004. ICPR 2004. Proceedings of the 17th International Conference on, Volume: 2
132. Wojtowicz W., Ogiela R. M., Security issues on digital watermarking algorithms, AGH University of Science and Technology, Annales UMCS Informatica AI XII, 4 (2012) 123–139, Poland
133. Woodfill J., Herzen Von B.: Real-Time Stereo Vision on the PARTS Reconfigurable Computer IEEE Symposium on FPGAs for Custom Computing Machines, April 1997, dostupno na: http://www.woodfill.com/Papers/FCCM1997.pdf (pristupano 15.9.2015.)
134. Woodham R., Image Understanding I: Image Analysis, Department of Computer Science
135. WPUTE-DB Biometrics Ear Database, dostupno na: http://ksm.wi.zut.edu.pl/wputedb/,

(pristupano 25.3.2016.)

136. Yang, B., Gu, F., and Niu, X.: Block mean value based image perceptual hashing. In Proceedings of the International Conference on Intelligent Information Hiding and Multimedia Multimedia Signal Processing (IIH-MSP), pp. 167{172. IEEE, 2006, ISBN 0-7695-2745-0.
137. Z J Tang, X Q Zhang, Y M Dai, and W W Lan. "Perceptual image hashing using local entropies and DWT." The Imaging Science Journal 2013; 61(2), 241-251.
138. Zabih R., Woodfill J., A non-parametric approach to visual correspondence. IEEE Transactions on Pattern Analysis and Machine Intelligence, 1996.
139. Zabih, R. and Woodfill, J., 1994. Non-parametric local trans- forms for computing visual correspondence. In: ECCV '94: Pro- ceedings of the Third European Conference-Volume II on Com- puter Vision, Springer-Verlag, London, UK, pp. 151–158.
140. Zauner, C.: Implementation and Benchmarking of Perceptual Image Hash Functions. Master's thesis, Upper Austria University of Applied Sciences, Hagenberg Campus, 2010.
141. Zeng J., A Novel Block-DCT and PCA Based Image Perceptual Hashing Algorithm, International Journal of Computer Science Issues (IJCSI). Volume 10, Issue 1, pp. 399-403, 2013.
142. Zhenjun T., Xianquan Z.; Shichao Z., Robus Perceptual Image Hashing Based on Ring Partition and NMF, Knowledge and Data Engineering, IEEE Transactions on, vol.26, no.3, p. 711-724, 2014.
143. Živić N.: Robus Image Authentication in the Presence of Noise, Springer 2015., pp. 55
144. Žugaj M.; Dumičić, K.; Dušak, V.: Temelji znanstvenoistraživackog rada, Fakultet organizacije i informatike Varaždin, Varaždin, 2006.

ŽIVOTOPIS

Bernard Vukelić rođen je 25. ožujka 1978. godine u Rijeci. Osnovnu i srednju školu završio je u Delnicama. Diplomirao je na Ekonomskom fakultetu u Rijeci – smjer Menadžment. Magistrirao je na Fakultetu organizacije i informatike u Varaždinu na temu biometrije. Radi na Veleučilištu u Rijeci na Poslovnom odjelu – studij Informatike, kao nastavnik na kolegijima Sigurnost informacijskih sustava, Sigurnost web alikacija i Operacijski sustavi. Autor je nekoliko znanstvenih i stručnih radova iz područja sigurnosti informacijskih sustava.

POPIS RADOVA:

Znanstveni radovi:

1. ANALYSIS OF AN INDOOR POSITIONING SYSTEMS
   By: Kaluza, Marin; Beg, Kristina; **Vukelic**, Bernard
   ZBORNIK VELEUCILISTA U RIJECI-JOURNAL OF THE POLYTECHNICS OF RIJEKA Volume: 5 Issue: 1 Pages: 13-32 Published: MAY 2017
2. CONTENT MANAGEMENT SYSTEM SECURITY
   By: Kaluza, Marin; **Vukelic**, Bernard; Rojko, Tamara
   ZBORNIK VELEUCILISTA U RIJECI-JOURNAL OF THE POLYTECHNICS OF RIJEKA Volume: 4 Issue: 1 Pages: 29-44 Published: MAY 2016
3. **Vukelić**, Bernard; Pogarčić, Ivan.
   Employer's evaluation of online education // *Annals of DAAAM for 2011 & Proceedings the 22st international DAAAM symposium "Intelligent manufacturing&automation: Power of Knowledge and Creativiity"* / Branko Katalinić (ur.). Vienna : DAAAM International Vienna, 2011., p. 1471-1472, ISSN: 1726-9679, ISBN: 978-3-901509-83-4, (predavanje, međunarodna recenzija, objavljeni rad, znanstveni).
4. **Vukelić** B., K. Škaron (Veleučilište u Rijeci, Rijeka, Croatia) Cyber Crime and Violation of Copyright, MIPRO 2013 - 36. međunarodni skup; ISS - Sigurnost informacijskih sustava; Opatija, 2013., p. 1127 - 1130, ISBN: 978-953-233-076-2, INSPEC Accession Number: 13768246, (predavanje, međunarodna recenzija, objavljeni rad, znanstveni).
5. **Vukelić** B., Bača M.: Comparision of RADIAL variance based and Maar- Hildreth operator perceptual image hash functions on biometric templates, Central European Conference on Information and Intelligent Systems (CECIIS2014), Varaždin, p.286 - 292, ISSN 1847-2001, (predavanje, međunarodna recenzija, objavljeni rad, znanstveni)
6. **Vukelić** B., Matić Vukelić U., Pavletić Božić Z.: Using Multicriteria Decision Making Methods for Information Security Risk Management Standards Selection, IIAS 2013, 25th International Conference on System Research, Informatics &

Cybernetics, Symposium on Global Education, Managerial Cybernetics, Risk Analysis & Risk Management, Baden-Baden, Germany, 2013

Stručni radovi:

1. **Kaluža, Marin; Troskot, Krešimir; Vukelić, Bernard: Comparison of front-end frameworks for web applications development;** ZBORNIK VELEUCILISTA U RIJECI-JOURNAL OF THE POLYTECHNICS OF RIJEKA Volume: 6 Issue: 1 Pages: 261-282 Published: MAY 2018
2. **Vukelić, Bernard**.Sigurnost informacijskih sustava - skripta .Rijeka : Veleučilište u Rijeci, 2016., ISBN: 978-953-6911-84-4
3. **Vukelić B.**, Brumić J.: Korištenje informacijsko-komunikacijskih tehnologija u tvrtkama Primorsko-goranske županije, Neki se bude neki još spavaju, InfoTrend, br 186, 12/2011., pp. 18-21
4. Pogarčić, Ivan; Babić, Snježana; **Vukelić, Bernard**.
   E ili M: U čemu je razlika? // CASE 19 - Metode i alati za razvoj poslovnih i informacijskih sustava / Polonijo, Mislav (ur.).
   Rijeka : CASE d.o.o., 2007. (predavanje,objavljeni rad,stručni).
5. **Vukelić, Bernard**; Gligora Marković, Maja; Tomljanović, Jasminka.
   eObrazovanje – izbor ili nužnost? // CASE 18 - Metode i alati za razvoj poslovnih i informacijskih sustava / Polonijo, Mislav (ur.). - Rijeka : CASE d.o.o. , . . / Polonijo, Mislav (ur.).
   Rijeka : CASE d.o.o. Rijeka, 2006. 205-207 (predavanje,objavljeni rad,stručni).
6. Pogarčić, Ivan; Kaluža, Marin; Tomljanović, Jasminka; Gligora Marković, Maja; **Vukelić, Bernard**.
   Primjena alata u stručnoj visokoškolskoj izobrazbi // Zbornik CASE17 - metode i alati za razvoj poslovnih i informacijskih sustava / Polonijo, Mislav (ur.).
   Rijeka : CASE d.o.o., 2005. (predavanje,objavljeni rad,stručni).
7. **Vukelić, Bernard**; Pogarčić, Ivan; Kukuljan, Elvis.
   Hoće li tablet računala izmijeniti tiskarstvo? // Tiskarstvo 2011 / Vilko Žiljak (ur.).
   Zagreb : FS d.o.o., 2011. (predavanje,domaća recenzija,sažetak,stručni). prilozen text rada
8. Gligora Marković, Maja; **Vukelić, Bernard**; Pogarčić, Ivan.
   Donošenje odluke o izboru LMS alata pomoću sustava za potporu u odlučivanju // Konkurentnost kroz inovacije i upravljanje poslovnim procesima.
   Sarajevo : Infodom d.o.o. Sarajevo, 2009. 39-39 (predavanje,međunarodna recenzija,sažetak,stručni).
9. **Vukelić, Bernard**; Pogarčić, Ivan; Gligora Marković, Maja.
   Tiskani ili digitalni nastavni materijal? // Tiskarstvo 08 / Vilko Žiljak (ur.).
   Zagreb : FS d.o.o, 2008. (predavanje,domaća recenzija,sažetak,stručni).
10. **Vukelić B**, Kaurić S, Kukuljan D.: Metode phishing napada na primjeru lažiranja facebook web stranice, Privatnost 2011. - Konferencija o zaštiti osobnih podataka, Polonijo, Mislav, editor(s). Zagreb: CASE d.o.o., 2011., (predavanje, ppt prezentacija, stručni)
11. **Vukelić B**.: Najveća prijetnja privatnosti – lozinka - Bernard Vukelić, Veleučilište u Rijeci, Privatnost 2012., Zagreb: CASE d.o.o., 2012., (predavanje, ppt prezentacija, stručni)
12. **Vukelić B**., Moguš M.: Opasnosti korištenja javnih bežičnih mreža: primjer krađe lozinke, Privatnost 2013 - Konferencija o zaštiti privatnosti podataka., Polonijo,

Mislav, editor(s), Zagreb: CASE d.o.o., 2013., (predavanje, ppt prezentacija, stručni) -

13. **Vukelić B**., Tabak M., Vrca M., VPŠ Minerva Dugopolje: Ugrožava li Internet marketing privatnost korisnika? , Privatnost 2013. - Konferencija o zaštiti osobnih podataka, Polonijo, Mislav, editor(s), Zagreb: CASE d.o.o., 2013. , (predavanje, ppt prezentacija, stručni)
14. **Vukelić B.:** Privatnost kod Internet of things (IoT) povezenih uređaja, , Privatnost 2014. - Konferencija o zaštiti osobnih podataka, Polonijo, Mislav, editor(s), Zagreb: CASE d.o.o., 2014. , (predavanje, ppt prezentacija, stručni)
15. **Vukelić B**.: Privatnost kod MS Windows 10 operacijskog sustava, Privatnost 2015. - Konferencija o zaštiti osobnih podataka, Polonijo, Mislav, editor(s), Zagreb: CASE d.o.o., 2015. , (predavanje, ppt prezentacija, stručni)