UNIVERZITET SINGIDUNUM
DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE

-STUDIJSKI PROGRAM-
SAVREMENE INFORMACIONE TEHNOLOGIJE

Primena digitalnih vodenih pečata za zaštitu biometrijskih podataka i privatnosti

- Master rad -

Mentor:
Doc.dr. Saša Adamović

Student:
Jelena Tašić
Br. indeksa:
410505/2014

Univerzitet Singidunum

Beograd, 2016.

Primena digitalnih vodenih pečata za zaštitu biometrijskih podataka i privatnosti

Sažetak: U ovom radu bavićemo se primenom digitalnog vodenog pečata za zaštitu biometrijskih podataka u servisima autentifikacije koji su zasnovani na biometriji. Osim zaštite biometrijskih uzoraka, ostvaren je doprinos u dodatnoj zaštiti privatnosti kod biometrijskih sistema koji obavljaju autentifikaciju bez čuvanja biometrije u bazi podataka. Polazeći od teorijskih osnova digitalnih vodenih pečata i biometrije, napravljen je detaljan pregled sa trenutnim stanjem u ovoj oblasti koja kombinuje ove dve tehnologije i tako stvara novo područje za istraživanje poznatije kao biometrijski vodeni pečati.

Ključne reči: Biometrijski identifikacioni sistemi, Napadi na biometrijske sisteme, Biometrijska kriptografija, Zaštita podataka, Steganografija, Digitalni vodeni pečati, Diskretna kosinusna transformacija, Diskretna talasna transformacija, Biometrijski vodeni pečati

Using digital watermark for protection of biometrical data and privacy

Abstract: This study focuses on digital watermark which are used for protection of biometrical data in authentication services based on biometry. Apart from protection of biometrical templates, there has been a breakthrough in additional privacy protection within biometrical systems which perform authentication without preserving biometry in their data basis. Using theoretical grounds of digital watermark and biometry as a starting point, a review of current state in this domain has been conducted. The domain combines the two technologies consequently creating a new sustainable ground for exploring, known as biometrical watermark.

Keywords: Biometric identification systems, Attacks on biometric systems, Biometric cryptography, Data protection, Steganography, Digital watermarking, Discrete cosine transform, Discrete wavelet transform, Biometric Watermarking

SADRŽAJ

Spisak slika **5**

Spisak tabela **5**

1. UVOD **6**
1.1. Cilj istraživanja **6**
1.2. Predmet istraživanja **6**
1.3. Struktura rada **7**

2. PREGLED U OBLASTI ISTRAŽIVANJA **8**
2.1. Digitalni vodeni pečati **8**
2.2. Digitalni vodeni pečati zasnovani na DWT transformaciji za kolor slike **9**
2.3. Biometrijski vodeni pečati **10**

3. TEORIJSKE OSNOVE **13**
3.1. Biometrijska identifikacija **13**
3.2. Primena biometrijskih identifikacionih sistema **14**
3.3. Princip rada biometrijskih sistema **16**
3.4. Performanse i greške u procesu verifikacije **17**
3.5. Nedostaci biometrijskih sistema **20**
3.6. Bezbednost biometrijskih sistema **21**
3.7. Zaštita biometrijskih sistema **23**
3.8. Čuvanje i poređenje biometrijskog šablona **24**
3.9. Zaštita biometrijskih šablona **25**
3.10. Biometrijska kriptografija **26**
3.11. Primena biometrijske kriptografije **27**
3.12. Primena infrastrukture javnih ključeva u biometriji **28**
3.13. Generisanje ključeva iz biometrije **28**
3.14. Generisanje ključeva na osnovu biometrije **29**
3.15. Primena zaštitnog koda i interlivera nad biometrijom **31**

4. DIGITALNI VODENI PEČATI **33**
4.1. Kompresija slike **33**
4.2. JPEG kompresija **33**
4.3. Transformacija slike **35**
4.3.1. Diskretna Furijeova transformacija 35
4.3.2. Diskretna kosinusna transformacija 36
4.3.3. Diskretna talasna transformacija 36
4.4. Klasifikacija digitalnih vodenih pečata **37**
4.5. Primena digitalnih vodenih pečata **38**
4.6. Algoritmi za označavanje i detekciju digitalnih vodenih pečata **40**
4.7. Savremena steganografija **40**
4.8. LSB supstitucija **40**
4.8.1. Skrivanje tajne slike unutar slike 42
4.8.2. Skrivanje tajnih poruka unutar slike 43
4.9. Tehnika kodovanja proširenim spektrom **44**

4.10. Ostali poznati algoritmi 44
4.11. Tehnike za korekciju slike 45
4.12. Geometrijske transformacije 46
4.13. Operacije za poboljšanje kvaliteta slike 47
4.14. Sigurnost digitalnih vodenih pečata i vrste napada 49
4.15. Otpornost digitalnih vodenih pečata na napade 50
4.16. Primena metode srednje vrednosti piksela protiv geometrijskog napada 52
5. BIOMETRIJSKI VODENI PEČATI 53
5.1. Primena vizuelne kriptografije i transformacija radi bezbedne biometrijske autentifikacije 54
5.2. Biometrijski vodeni pečat zasnovan na prioritetu bita 55
5.3. Primena algoritma robustnog vodenog pečata zasnovanog na DCT za obezbeđivanje sigurnosti slike irisa 56
5.4. Vodeni pečat biometrije irisa zasnovan na razlaganju jedinstvene vrednosti i DCT 58
5.5. Metoda vodenog pečata zasnovana na spajanju biometrija 58
5.6. Primena vodenog pečata i steganografije u zaštiti multimodalnih biometrijskih podataka 60
5.7. Primena dvostepene multimodale autentifikacije zasnovane na talasnoj kvantizaciji vodenog pečata za unapređenje bezbednosti biometrije 63
5.8. Vodeni pečati zasnovani na SDPQ metodi 64
5.9. Bezbednostni problemi biometrijskih vodenih pečata 65
6. ZAKLJUČAK 66
6.1. Predlog za budući rad 66
7. LITERATURA 67

Spisak slika

1. Primena biometrije 14
2. MorphoSmart FINGER VP OEM Series 15
3. Predloženo rešenje komapnije SAFRAN Morpho 15
4. Princip rada biometrijskih sistema [14] 16
5. Zavisnost FAR i FRR parametra od sigurnosnog praga 19
6. Vrste napada na biometrijski sistem 22
7. Blok šema funkcionisanja biometrijske kriptografije 27
8. Generička šema primene zaštitnog koda i interlivera nad biometrijom 31
9. Blok šema JPEG sistema za kompresiju slike: (a) koder, (b) dekoder [16] 33
10. Osnovni talasni oblici 8x8 DCT transformacije 34
11. Cik-cak očitavanje DCT koeficijenata 34
12. Piramidalno razlaganje talasa na jedan, dva i tri nivoa 36
13. Blok šema utiskivanja vodenog pečata primenom LSB supstitucije 41
14. Originalna slika 41
15. Primer vodenog pečata 41
16. Pročitani vodeni pečat 41
17. Razlika između originalnog i pročitanog vodenog pečata 41
18. Originalna slika 42
19. Tajna slika 42
20. Slika – kombinacija 42
21. Slika dobijena od tri bit ravni najmanje težine slike 4.8.1.3 42
22. Nosilac poruke 43
23. Steganografski medijum 43
24. Šema skrivanja tajne poruke unutar slike primenom LSB supstitucije 43
25. Frekventne oblasti u 8 x 8 DCT bloku 56
26. Percepcija slike vodenog pečata 57
27. Proces utiskivanja vodenog pečata 58
28. Predložena šema DCT vodenog pečata zasnovana na biometriji 59
29. Primena tehnike vodenog pečata i steganografije: (a) slika lica, (b) slika otiska prsta, (c) proizvoljna slika 60
30. Struktura sistema upisivanja i verifikacije podataka 61
31. (a) originalna slika, (b) slika sa utisnutim otiskom prsta kao vodenim pečatom 62
32. Razlike uzorka primenom različite jačine šifrovanja (a) originalna slika, (b) q=0.015, (c) q=0.030, (d) q=0.045 62
33. Blok šema utiskivanja vodenog pečata zasnovana na dvostepenoj biometrijskoj autentifikaciji 63
34. Prikaz SDQ i SDDM metode za utiskivanje vodenog pečata 65

Spisak tabela

1. Poređenje sa postojećim rezultatima u ovoj oblasti 23
2. Poređenje prostornog i frekventnog domena 37

1. UVOD

1.1. Cilj istraživanja

Cilj ovog istražiavanja je unapređenje zaštite biometrijskih podataka primenom steganografije, digitalnih vodenih pečata i kriptografije. Pregledom trenutnog stanja u oblasti biometrijskih vodenih pečata, kao i predloženih rešenja, stvorena je mogućnost detaljnijeg istraživanja ove oblasti radi dodatne zaštite biometrijskih podataka.

1.2. Predmet istraživanja

U današnje vreme, svaki čovek teži da obezbedi sigurnost i privatnost svojih podataka i zaštiti ih od zloupotrebe. Sastavni deo opšte bezbednosti svih informacionih sistema, jeste autentifikacija. Primena lozinki je trenutno jedna od najpopularnijih metoda za zaštitu podataka, međutim nije dovoljno sigurna. Iako su, u poslednje vreme, učinjene mnoge promene po pitanju autentifikacije (lozinke se više ne šalju preko mreže u otvorenoj formi, postavljen je zahtev za generisanje jačih lozinki i sl.), nista se nije učinilo po pitanju slabosti osnovnog pristupa, iako su dobro poznate.

Autentifikacija koja se zasniva na biometriji pruža najbolju i najsigurniju metodu zaštite podataka i obezbeđuje savremene informacione servise, a korisniku nudi bezbednu proveru identiteta. Za razliku od sistema koji se zasniva na lozinkama, biometrijske sisteme je mnogo teže prevariti.

Zbog sve značajnijeg porasta pristupu Internetu, kao i opasnosti od zloupotreba poslednjih godina, povećana je upotreba biometrije u autentifikaciji korisnika. S obzirom na osobine koje poseduju biometrijski podaci, biometrija sve više zamenjuje tradicionalne metode autentifikacije. Mnoge zemlje koriste biometrijske podatke radi zaštite pojedinca od krađe identiteta.

Ipak, biometija ne može da obezbedi autentičnost ili da garantuje zaštitu od odbijanja, zato što može biti kopirana ili falsifikovana. Biometrijski uzorci, iako smešteni u bazi podataka, nisu bezbedni zato što mogu biti kompromitovani. Ukoliko se biometrijski podatak ukrade ili modifikuje, on je izgubljen zauvek, te bezbednost i integritet biometrijskih podataka predstavlja izazov. Da bi se povećala bezbednost i poboljšale performanse sistema, treba kombinovati različite vrste autentifikacija.

Primena vodenih pečata je veoma značajna kod autentifikacije podataka, indentifikacije vlasnika i zaštite od nezakonitog kopiranja. Iako se, poslednjih nekoliko godina, radilo intenzivno na unapređenju i razvoju algoritama za utiskivanje digitalnih vodenih pečata, takođe razvijali su se i napadi na iste, kojih je sve više.

Za prenos kritičnih biometrijskih podataka od korisnika do servera može biti pogodna tehnika bazirana na steganografiji, te se na taj način može smanjiti mogućnost nelegalne izmene biometrijskih podataka. Nakon upisa, na biometrijske uzorke se primenjuje šifrovanje, koji se dešifruju za vreme autentifikacije uz pomoć tajnog ključa. Šifrovanje obezbeđuje sigurnost sve dok se podaci ne dešifruju.

Radi povećanja bezbednosti, poslednjih godina, dosta se radilo na biometrijskim vodenim pečatima. Za unapređenje sigurnosti autentifikacionih sistema, mogu nam pomoći biometrijski vodeni pečati, koji mogu obezbediti bezbednost nakon dešifrovanja. Pa tako, biometrijski podaci koji se utiskuju u dešifrovan host podatak, moći će ponovo da se dobiju samo uz pomoć tajnog ključa.

Biometrijski vodeni pečat je nevidljivi digitalni vodeni pečat, utisnut u osnovnu sliku, koji se lako može obnoviti pomoću kompjuterskog programa. Lokacija utiskivanja biometrijskih podataka u osnovnu sliku se određuje pomoću tajnog ključa i tako sprečava mogućnost zloupotrebe biometrijskih podataka. Nevidljivi vodeni pečat treba da bude robustan na različite tehnike obrade signala i da može ponovo da se dobije iz izmenjene slike. Tehniku nevidljivog vodenog pečata treba primenjivati u zakonskim okvirima zajedno sa bezbednošću lokacije i šifrovanjem.

1.3. Struktura rada

U sledećem, drugom poglavlju ovog rada bavićemo se dosadašnjim dostignućima u oblasti istraživanja digitalnih vodenih pečata, kao i biometrijskih vodenih pečata.

U trećem poglavlju govorićemo o teorijskim osnovama biometrijskih identifikacionih metoda, njihovoj primeni radi zaštite podataka, nedostacima i mogućim napadima na biometrijske sisteme. Osim što ćemo objasniti princip rada, bavićemo se i biometrijskom kriptografijom i generisanjem kriptoloških ključeva na osnovu biometrije.

U četvrtom poglavlju date su vrste digitalnih vodenih pečata i objašnjen njihov princip rada. Osim toga, dati su i algoritmi koji se koriste za skrivanje informacija unutar slike. Takođe, opisane su metode najčešćih napada na digitalne vodene pečate, ali i metode zaštite od istih.

U petom poglavlju predstavićemo biometrijske vodene pečate, noviju metodu koja kombinuje biometriju, digitalne vodene pečate, steganografiju i kriptografiju. Dati su primeri i opis nekoliko praktičnih rešenja radi unapređenja bezbednosti biometrijskih podataka.

Na kraju rada, u okviru zaključka, biće prikazana konačna analiza našeg rada. Takođe, navešćemo ostvarene doprinose u ovom radu, ali i predlog za budući rad.

2. PREGLED U OBLASTI ISTRAŽIVANJA

2.1. Digitalni vodeni pečati

Digitalno označavanje podataka nastalo je pri prelasku iz analognog u digitalni domen, zbog nemogućnosti razlikovanja originalnog dokumenta od kopije. Digitalni vodeni pečat (engl. *Digital watermarking*) se prvi put javlja 1954. godine, kada je patentiran od strane Emil Hembrooke (Muzac Corporation) kao metod za neprimetno ugrađivanje identifikacionog koda u muziku radi dokazivanja vlasništva. Tehnika digitalnog vodenog pečata vodi poreklo od imena vodenih pečata papira, u koji bi vlasnik zapečatio svoj logo u dokument, kao meru bezbednosti.

Skrivena informacija se ugrađuje u digitalni dokument i tako osigurava bezbednost. Primenjuje se na digitalni audio i video zapis, slike, mape, dokumenta, računarske programe, kao i za zaštitu autorskih prava. Skrivena informacija kod slika može biti takođe u vidu slike (npr. logo ili informacije o autorskim pravima), ili u vidu grupe bitova koji se, prema određenom algoritmu, šire oko slike.

Istraživanja u ovoj oblasti doprinela su značajnom napretku u zaštiti slike [1]. U periodu od 1990. do 2000. godine počinje da se javlja prilično veliko interesovanje za digitalne vodene pečate. Sve do tada istaživanje u ovoj oblasti bilo je zanemareno. Najviše se radilo na maksimalnom odnosu signal/šum (engl. *Peak Signal to Noise Ratio*, PSNR). U periodu od 2000. do 2010. godine, razvijale su se različite tehnike za utiskivanje vodenih pečata primenom Diskretne Furijeove transformacije (DFT), Diskretne kosinusne transformacije (DCT), Diskretne talasne transformacije (DWT), LSB supstitucije (engl. *Least Significant Bit*) i CDMA (engl. *Code division multiple access*) metode. Za vreme ovog perioda postignut je razvoj reverzibilnih vodenih pečata, ali i maksimalna sličnost između originalne i obnovljene slike, kod primene u medicini.

Tian et al. (2003) je predstavio reverzibilne vodene pečate, koristeći nejednaku ekspanziju i LSB metodu, da bi dobio veoma dobar kapacitet utiskivanja. Alattar (Narawade i Kanphade, 2011b) je upotrebio nejednaku ekspanziju transformisanu za „tri“, kako bi proširio Tian-ov algoritam i u svaka tri piksela utisnuo dva bita. Coltuc i Chassery (2007) predstavili su jednostavnu i efikasnu, reverzibilnu skrivenu šemu, zasnovanu na RCM algoritmu (engl. *Reversible Contrast Mapping*), koji ne zahteva mapu lokacija radi obnavljanja originalne slike. Ova šema utiskuje u vodeni pečat podatke velikog kapaciteta bez dodatne kompresije. RCM metoda je invertibilna, čak i kada se transformisani LSB pikseli izgube. U slučaju geometrijskog napada, promeniće se vrednosti piksela slike. GTC metoda prepoznaje i ispravlja geometrijsku distorziju (Yang et al., 2010).

Međutim, ova metoda ne može potpuno da kontroliše poziciju utisnute informacije, što daje loš kvalitet stego slike. Zato su Tzu-Chuen i Li-Ling Hsu (2008) uklonili ove nedostatke i predstavili novi RCM algoritam. Kanphade i Narawade (2012) razvili su dupli RCM algoritam koji smanjuje celu funkciju u predloženom algoritmu (Coltuc i Chassery, 2007).

Jedna od najboljih metoda u oblasti reverzibilnih vodenih pečata je metoda pomeranja histograma. Hong et al. (2010) je modifikovao ovu metodu i predstavio brži metod. Kod ove metode podaci se utiskuju pomeranjem histogramskih binova. Metod konstruiše sliku histograma iz originalne slike kao bi dobio par vrhova i nultu tačku.

Xiangli i Xuefang (2010) predstavili su metodu reverzibilnog nula-bit vodenog pečata zasnovan na haotičnom šifrovanju, koja obezbeđuje dodatnu sigurnost vodenom pečatu. Yang et al. (2010) predstavio je reverzibilni vodeni pečat, primenom metode podešavanja koeficijenata. Huang i Fang (2011) prikazali su histogram zasnovan na reverzibilnim skrivenim podacima za medicinske snimke. Narawade i Kanphade (2011a) razvili su tehniku pomeranja historama koja unapeđuje kvalitet i kapacitet utiskivanja reverzibilnih vodenih pečata. Awrangjeb et al. (2006) je predstavio metodu korekcije geometrijske distorzije, koja omogućava prepoznavanje geometrijskog napada.

Kanphade i Narawade (2013) su upotrebili robustni reverzibilni vodeni pečat protiv geometrijskog napada primenom GTC tehnike na metode prostornog domena. Kombinovanjem sa GTC metodom može se prepoznati geometrijski napad (Yang et al., 2010). Međutim, neutralizacija geometrijskog napada koriguje napadnutu sliku. Oporavljena slika i vodeni pečat mogu se dobiti obrnutim procesom. Razvojem ove tehnike postignut je bolji PSNR i veći kapacitet utiskivanja u poređenju sa postojećim tehnikama.

Napravljeno je poređenje metoda pomeranja histograma, reverzibilne metode kontrastnog mapiranja, metode nejednake ekspanzije, primenjenih na robustne vodene pečate protiv geometrijskog napada. Rezultati su pokazali da metoda pomeranja histograma ima bolji PSNR, dok metoda nejednake ekspanzije ima bolji kapacitet utiskivanja. Sve metode pogodne su za slike visokog kvaliteta, dok je jedino metoda pomeranja histograma pogodnija za medicinske snimke i dijagrame. Kombinacija svih ovih metoda sa GTC metodom stvara robustni reverzibilni vodeni pečat koji je otporan na geometrijski napad [2].

2.2. Digitalni vodeni pečati zasnovani na DWT transformaciji za kolor slike

Postoje mnoge tehnike za utiskivanje vodenog pečata u prostornom i frekventnom domenu (Bender et al., 1996; Banf et al., 2002; Ganic i Eskicioglu, 2004; Guangmin et al., 2007). Prostorne tehnike vrše prilagođavanje manje značajnih bitova piksela slike i taj način garantuju neprimetnost. Spektralne ili transformacione tehnike pripajaju vodeni pečat transformisanim koeficijentima slike. Algoritmi zasnovani na transformacijama omogućuju da se vodeni pečat lako smesti u perceptualno bitna područja slike, što stvara pečat koji je robusniji na napade i koji se teško može ukloniti bez izobličenja slike (Hartung i Kutter, 1999; Kong et al., 2003; Guangmin, 2007). Transformacije koje se primenjuju su DCT i DWT. Postoje različite tehnike za utiskivanje vodenog pečata u crno-bele slike (Guangmin, 2007; Vikas, 2007).

Kod kolor slike, od tri kanala (crveni, zeleni i plavi), crveni kanal je najrobustniji protiv JPEG napada, a plavi najmanje. Dakle, skrivene informacije vodenog pečata su mnogo sigurnije u crvenom nego u plavom kanalu. Guangmin (2007) predlaže tehniku vodenog pečata za kolor sliku, zasnovanu na DWT metodi, koja transformiše originalnu kolor sliku u YIQ model, i utiskuje vodeni pečat u Y i Q komponente (Hartung i Kutter, 1999). Mei et al. (2001) je predstavio tehniku za skrivanje vodenog pečata u koeficijente niskih frekvencija 8x8 DCT blokova crvenog, zelenog i plavog kanala (Kong et al., 2003). Banf et al. (2002) predlaže tehniku u kojoj se crveni, zeleni i plavi kanal transformišu celim ramom DCT i selektuju koeficijenti niskih frekvencija, kako bi se sakrio vodeni pečat (Kundur i Hatzinakos, 1999).

Iako je mnogo istraživanja urađeno sa DCT, danas sve veću popularnost imaju tehnike zasnovane na DWT. DWT ima dosta prednosti nad DCT (Lee i Lee, 2005). Talasno kodovana slika je multi-rezolucioni opis slike, tj. jedna slika može biti prikazana sa različitim nivoima rezolucije i može biti sekvencijalno obrađena od niske do visoke rezolucije. U poređenju sa DCT, DWT transformacija je mnogo bliža ljudskom vizuelnom sistemu (HVS). Takođe, vizuelni artefakt talasno kodovane slike je manje očigledan, jer DWT ne rastavlja sliku na blokove da bi je obradila.

U odnosima visoke kompresije, blokovni artefakti su uočljivi u DCT, međutim u talasno kodovanim slikama su mnogo jasniji. DFT i DCT su transformacije punog rama, te će bilo kakva promena u koeficijentima transformacije uticati na celu sliku, osim ako je DCT upotrebljena korišćenjem tehnike blokovnog pristupa.

Utiskivanje signala pomoću DWT, koja ima prostorno frekventnu poziciju, imaće lokalni uticaj na sliku (Mei et al., 2001; Meerwald i Uhl, 2001; Liu et al., 2005). Utiskivanje u HL i LH podopseg, u nekim slučajevima je otporno na izjednačavanje histograma i napad gama korekcijom (Polikar, 2001). Iz tog razloga su algoritmi vodenog pečata zasnovani na DWT postali važna oblast istraživanja (Stollnitz et al., 1995; Saraju, 1999; Reza et al., 2004; Raviraj i Sanavullah, 2007).

Postoje i druge DWT transformacije kao npr. Meyer, Mexican hat i Morlet talasi. Velika cena proračuna je nedostatak ovih transformacija, za razliku od Haar talasa. Haar talasna transformacija ima brojne prednosti, jednostavna je, brza, reverzibilna, bez efekta ivica, što je problem kod drugih talasnih transformacija (Vikas, 2007).

Tehnike vodenog pečata bazirane na DWT, postižu robustnost na račun kvaliteta skrivene slike. Algoritam baziran na CDMA uglavnom pokriva sliku, ali je obnavljanje slike izuzetno robustno. Shih-Chang et al. (2004) je predstavio algoritam baziran na filtriranju podopsega i učinio da vodeni pečat u slici postane neprimetan.

M. Gupta, D. Gupta i Saxena (2013), uporedili su rezultate klasičnog algoritma baziranog na CDMA (Vikas, 2007) i algoritma baziranog na filtriranju podopsega (Shih-Chang et al., 2004). Vikas (2007) je uspeo da obnovi vodeni pečat do JPEG kvaliteta faktora Q=10. Prednost ovog algoritma baziranog na CDMA tehnici, je kraće potrebno vreme za utiskivanje i obnavljanje vodenog pečata. U poređenju sa algoritmom baziranim na CDMA, predloženi algoritam ne utiče na kvalitet skrivene slike, dok u poređenju sa algoritmom baziranim na filtriranju podopsega (Shih-Chang et al., 2004), predloženi algoritam obnavlja podatke vodenog pečata do nivoa kompresije 4. [3]

2.3. Biometrijski vodeni pečati

Potreba za bezbednošću uticala je na razvoj personalnih biometrijskih identifikacionih sistema. Identifikacija pomoću biometrije pomaže u sprečavanju prevara i sugurnosnoj kontroli pristupa (Vacca, 2007).

Biometrijski sistem će raditi ispravno, ukoliko verifikacioni sistem zagarantuje da su biometrijski podaci došli od legitimne osobe u trenutku upisa (Yiwei et al., 2002). Kao rešenje za ovaj problem mogu se upotrebiti šifrovanje i vodeni pečat. Iako šifrovanje ne može da obezbedi sigurnost nakon što se podaci dešifruju, vodeni pečati to mogu.

Vodeni pečati skrivaju informacije u host podatak da bi zaštitili njegov integritet. Postoje brojne tehnike vodenog pečata za utiskivanje podataka u sliku. Mogu se uopšteno podeliti na tehnike prostornog domena (Mukherjee et al., 2004; Singh et al., 2012) i tehnike frekventnog domena (Yiwei et al., 2002; Wang et al., 2009; Sakib et al., 2011; Deb et al., 2012). Iako tehnike u prostornom domenu imaju najmanju složenost i veliki kapacitet nosivosti, one ne mogu da izdrže napade kao što su obrada slike i niskopropusno filtriranje (Dabas i Khanna, 2013).

Jain et al. (2002) pomoću tajnog ključa utiskuje niz bitova svojstvenih koeficijenata lica (engl. *Eigenface coefficients*) u nasumice izabrane piksele slike otiska prsta, primenom slepog vodenog pečata. Jain et al. (2003) primenom steganografije sakriva podatake minucije unutar nosioca podataka koji je nevezan za originalni otisak prsta. Informacija je sakrivena u tri vrste slika: u sliku otiska prsta, sliku lica i proizvoljnu sliku. Autori su sakrili svojstvene koeficijente lica unutar slike otiska prsta. Rezultati su pokazali da je izvučeno 100% tačaka minucije i time je dokazano da pečatirane slike otiska prsta ne degradiraju performanse.

Moon et al. (2005) je predložio nekoliko tehnika vodenog pečata za povećanje sigurnosti biometrijskih sistema primenom otiska prsta i lica. Vrhunske performanse, u pogledu tačnosti verifikacije, dobijene su pri utiskivanju karakteristika otiska prsta u sliku lica, što nije slučaj sa utiskivanjem karakteristika lica u sliku otiska prsta.

Vatsa et al. (2006) primenjuje kombinaciju DWT i LSB metode za pečatiranje biometrije. Tehnika vodenog pečata zasnovana na DWT je robustna na frekventne napade, a ranjiva na geometrijske napade, dok su LSB algoritmi vodenog pečata robustni na geometrijske napade, ali su više ranjivi na frekventne napade. Autori su pokazali da kombinovani algoritam bolje radi nego LSB ili DWT tehnike odvojeno i da zajedničko delovanje DWT i LSB algoritma dobro utiče na šifrovanje i dešifrovanje, u slučaju frekventnih i geometrijskih napada.

Komninos et al. (2007), predstavio je tehniku vodenog pečata i kriptografije za utiskivanje šablona otiska prsta u sliku lica, koja je zasnovana na razlaganju slike na blokove. Predložena metoda omogućava da se sačuva kvalitet slike. Park et al. (2007) predlaže upotrebu robustnog utiskivanja šablona irisa u sliku lica.

Bartlow et al. (2007) je utisnuo opisnu karakteristiku glasa u sliku irisa. Međutim, umesto da se nasumice izabrala bilo koja tačka u slici, opisna karakteristika glasa je sakrivena samo unutar segmentiranog irisa. Rezultati su pokazali da se sa uvođenjem opisne karakteristike glasa, kvalitet slike irisa ne ometa značajno, kao ni performanse poređenja irisa. Za unapređenje zaštite integriteta biometrijskih podataka, autori su predložili primenu infrastrikture sa javnim ključevima (PKI), što daje neporecivost porekla i integritet podataka kroz kriptografiju.

Low et al. (2007) primenjuje diskretnu radon transformaciju (engl. *Discrete Radon Transforms*, DRT) i analizu glavne komponente (engl. *Principal Component Analysis*, PCA), kako bi razložio potpis na binarni niz. Da bi se utvrdila robustnost i jačina protiv JPEG kompresije, upoređene su tri metode utiskivanja i izvlačenja: LSB, CDMA raspršeni spektar u prostornom domenu i CDMA raspršeni spektar u DWT domenu. Performanse ovih metoda testirane su od strane ljudske vizuelne percepcije, odnos signal/šum (PSNR) i stopa distorzije (normalizovana Hamingova udaljenost). Rezultati su pokazali da je LSB metoda veoma lomljiva na JPEG kompresiju, uprkos tome što ima najjednostavniji pristup biometrijskim vodenim pečatima. CDMA raspršeni spektar u DWT domenu ima komplikovaniji princip rada, ali je mnogo otporniji na JPEG kompresiju.

Rajibul et al. (2008) utiskuje šifrovani šablon otiska dlana u sliku otiska prsta, pomoću ključa koji je dobijen iz otiska dlana. Islam et al. (2008) je utisnuo vodeni pečat u sliku otiska prsta, pomoću lozinke koja je izvučena iz otiska dlana iste osobe. Međutim, robustnost algoritma na napade nije dokazana.

Kako bi utisnuo minucije otiska prsta u sliku lica, Ma et al. (2010) predlaže šemu blok piramide zasnovanu na prilagođenoj kvantizaciji vodenog pečata. U gornji nivo piramide se utiskuju numerički bitovi vodenog pečata sa većim prioritetom, sa većom snagom utiskivanja koristeći statistiku prvog reda tj. QIM (engl. *Quantization Index Modulation*) metodu.

Uhl et al. (2011) je predložio rešenje za bezbednosne pretnje u biometrijskim sistemima pomoću tehnologije vodenog pečata. Fouad et al. (2011) prestavio je šemu za zaštitu uzorka irisa, kombinacijom tehnika kriptografije i vodenog pečata. Slika irisa je zaštićena ključem i utisnuta, pomoću LSB i DWT tehnika, u skrivenu sliku. Lokacija utiskivanja definisana je pomoću drugog ključa. Takođe, oba ključa (ključ irisa i utisnuti ključ) su potrebna u procesu izvlačenja irisa.

Isa i Aljareh (2012) primenili su Cox-ov algoritam za utiskivanje vodenog pečata u sliku lica. Za identifikaciju, kao korisničko ime, je uzeta slika lica, dok je autentifikaciju, kao lozinka uzet vodeni pečat. Nedostatak ove šeme je taj što je potrebna originalna slika u procesu detektovanja vodenog pečata.

Majumder et al. (2013) je primenio biometrijski vodeni pečat pomoću DWT metode i razlaganja jedinstvene vrednosti host slike, kako bi dobio sopstveni vektor. Karakteristike irisa izvučene su pomoću DCT tehnike i utisnute u sopstveni vektor, koji je dobijen iz host slike. Međutim, nedostatak ovog pristupa je nemogućnost promene algoritma za izvlačenje karakteristika irisa.

Paunwala i Patnaik (2014) utisnuli su karakteristike otiska prsta i irisa u sliku, koja se zatim deli na blokove. Svaki blok se transformiše u dvodimenzionalni DCT i svrstava u blokove sa ili bez ivica. Biometrijske karakteristike su utisnute u koeficijente niskih frekvencija DCT 8 x 8 blokova, dok je blok sa ivicama uklonjen.

Prepoznavanje pomoću irisa se smatra jednom od najpouzdanijih biometrijskih tehnika, koja se široko primenjuje za personalnu identifikaciju. Međutim, da bi se zagarantovala pouzdanost biometrije irisa, potrebno je povećati bezbednost korišćenjem vodenog pečata.

3. TEORIJSKE OSNOVE

3.1. Biometrijska identifikacija

Postoje tri načina za proveru identiteta:

- **Nešto što znaš** – lozinka, PIN ili neka lična informacija;
- **Nešto što imaš** – kartica (npr. ID kartica, pasoš, platna kartica i sl.);
- **Nešto što jesi** – biometrija (npr. otisak prsta, crte lica, iris i sl.).

Ranije se provera identiteta u sigurnosnim sistemima zasnivala, pre svega, na vizualnom prepoznavanju određenih osoba od strane ovlašćenih lica. Vremenom su uvođene različite tehničke metode nadzora zaštićenog prostora kao što su magnetne kartice, ukucavanje PIN koda i sl., ali zbog određenih nedostataka, ova metoda nije imala uspeha. Nakon toga pojavljuju se biometrijske identifikacione metode, koje su se vremenom pokazale kao najpouzdanije. Danas, većina sigurnosnih sistema za kontrolu pristupa i utvrđivanja identiteta se zasniva na biometriji.

Svrha biometrijskih sistema je provera identiteta na osnovu biometrijskih karakteristika. Prednost ovih karakteristika se ogleda u tome što one ne mogu biti izgubljene ili zaboravljene.

Savremeni biometrijski sistemi zasnovani su na karakteristikama koje možemo podeliti u dve grupe [10]:

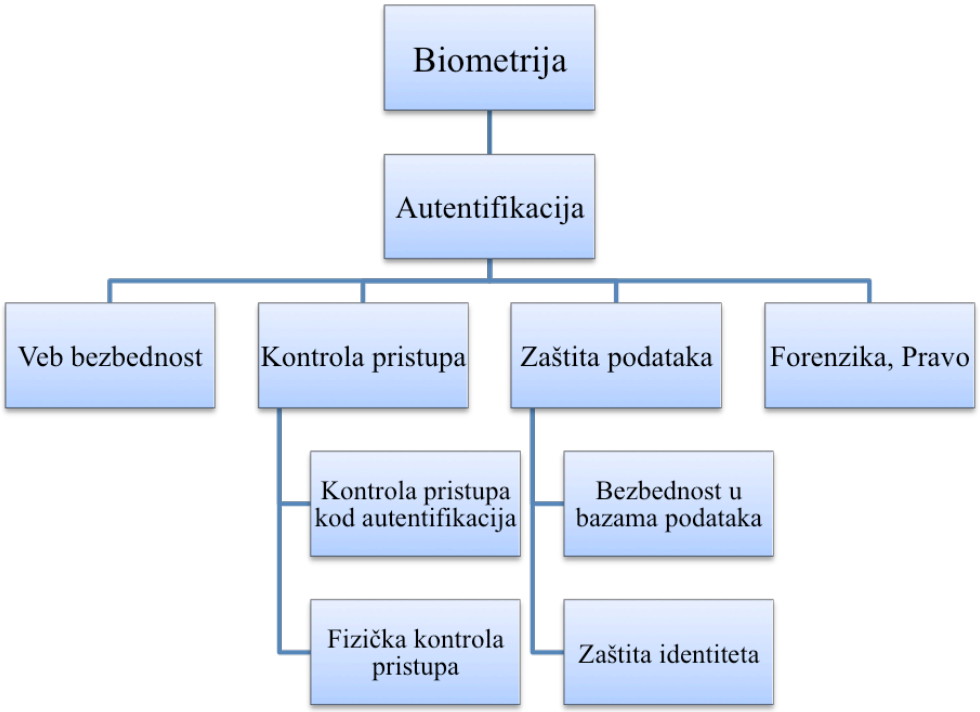
- **Fizičke karakteristike** – čine izgled i specifične fizičke osobine osobe, kao što su otisak prsta, dlana, lica, iris, retina, vene, termogram, telesni mirisi i DNK osobe. Ova metoda se bavi uzorkovanjem fizionomije ljudskog tela i njegovim jedinstvenim karakteristikama. Prepoznati uzorci mogu se koristiti u kombinaciji sa ostalim klasičnim zapisima kojima se jedinstveno opisuju osobe. Ovakva provera mora da bude jeftina, brza, pouzdana, ali ne sme da zalazi u fizički integritet osobe.
- **Bihevioralne karakteristike –** zasnivaju se na specifičnostima u ponašanju osobe, kao što su glas, potpis, dinamika kucanja i hod osobe. U ovu grupu mogu se svrstati i druge bivehioralne karakteristike kao što su svakodnevni rituali i navike koje karakterišu neku osobu. Međutim, ove karakteristike nisu dovoljno specifične da bi se koristile za identifikaciju, već samo mogu da nas upute na neku osobu.

Način upotrebe biometrijskih podataka u autentifikacionim servisima, sa aspekta dimenzionalnosti, možemo da podelimo na monomodalne i multimodalne. Za razliku od monomodalne biometrije, gde se za autentifikaciju primenjuje samo jedna biometrijska karakteristika, multimodalna biometrija kombinuje dve ili više različitih vrsta biometrije. Multimodalna biometrija se primenjuje ukoliko podaci za proveru identiteta iz osnovnih dokumenata nisu dovoljni, ili ukoliko želimo da postignemo veću tačnost i otpornost sistema od zloupotrebe. Ukoliko se koristi samo jedna tehnika (npr. otisak prsta), postoji mogućnost da se treća osoba lažno predstavi. Međutim, ukoliko se koristi više tehnika (npr. otisak prsta i biometrija lica), tada je manja verovatnoća zloupotrebe identiteta, a sistem je sigurniji [11]. Primenjuje se pri kontroli na graničnim prelazima, za civilnu identifikaciju, kontrolu pristupa zaštićenom prostoru i za sigurnost mreža. Multimodalna biometrija može biti opoziva ili neopoziva.

3.2. Primena biometrijskih identifikacionih sistema

Biometrijski sistemi imaju široku primenu u aplikacijama gde se zahteva sigurna autentifikacija korisnika (Slika 3.2.1). Primena biometrijskih sistema identifikacije prvi put se javlja u kriminalistici radi bržeg pretraživanja i upoređivanja tragova sa bazom podataka. U prethodnoj deceniji, biometrijski sistemi počinju da se primenjuju u velikim ekonomskim transakcijama, radi potvrde identiteta učesnika. Biometrijski sistemi se danas osim u kriminalistici i forenzici koriste i u medicini, vladinim agencijama, finansijama, osiguranju i zaštiti podataka. Ovaj metod identifikacije koristi se u kompanijama za identifikovanje zaposlenih i u okruženjima sa strogim ovlašćenjima gde je nivo bezbednosti zahtevan i izuzetno visok (npr. vojne institucije, nuklearna postrojenja, vladine institucije).

Biometrijski sistemi se najčešće koriste za povećanje bezbednosti računarskih mreža, zaštitu prilikom finansijskih transakcija, obezbeđivanje međunarodnih granica, kontrolu pristupa zaštićenim radnim lokacijama i sprečavanje raznih vrsta prevara.

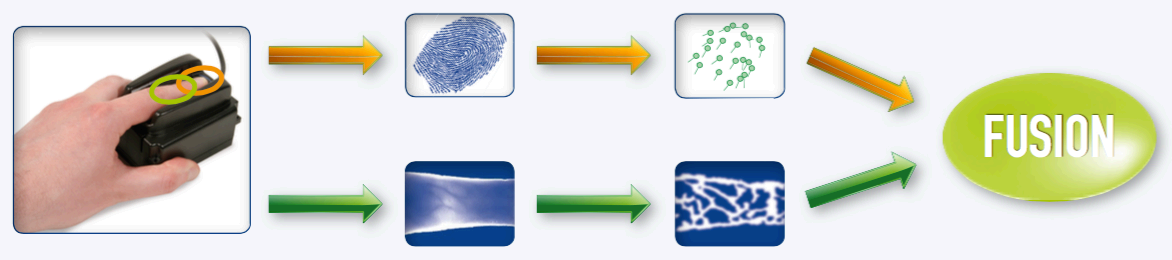


Slika 3.2.1: Primena biometrije

Biometrijski sistemi za identifikaciju se stalno usavršavaju i sve više primenjuju u različitim sistemima. Vremenom su postali sve precizniji, pouzdaniji, brži, ali i manjih dimenzija. Sve više nalaze primenu u slučajevima kada je neophodno nedvosmisleno utvrditi ili potvrditi identitet osobe.

Sistemi koji koriste biometrijsku metodu omogućavaju zaštitu privatnosti i ispravnu verifikaciju korisnika. Najpoznatije biometrijske metode koje se koriste u savremenim servisima za autentifikaciju su: lice, otisak prsta, otisak dlana, vene, retina, iris itd.

Najsavremeniji sistemi, osim 2D biometrije lica, mogu pružiti identifikaciju i pomoću 3D biometrije lica, koja uključuje i novu paletu algoritama za prepoznavanje. Sa razvojem novih tehnologija nastala je nova pouzdana i precizna metoda – prepoznavanje na osnovu rasporeda vena. Na slici 3.2.2 je prikazan multimodalni uređaj kompanije Morpho koji može istovremeno da snimi i obradi otisak prsta i vene.



Slika 3.2.2: MorphoSmart FINGER VP OEM Series

Jedna od najizazovnijih oblasti istraživanja jeste primena biometrije za skriveno nadgledanje, gde je određenu osobu moguće automatski identifikovati pri ulazku u zaštićenu prostoriju. Međutim, biometrija irisa se pokazala kao najpouzdanija i najpreciznija biometrijska metoda za autentifikaciju i generisanje kriptoloških ključeva, zbog veoma bogatog informacionog sadržaja.

Trenutno, jedna od najzastupljenijih biometrijskih tehnika u oblasti zaštite je biometrija otiska prsta. Prvo rešenje za pristup primenom biometrije, koje jednim zamahom ruke snima i upoređuje četiri otiska prsta, dala je kompanija SAFRAN Morpho. „*MorphoWave*^{TM}“ omogućava autentifikaciju korisnika u pokretu, bez zaustavljanja, što ga čini pogodnim za okruženja sa velikim prometom ljudi (granična kontrola, kontrola pritupa u javnim i privatnim preduzećima itd.). Tehnologija „bez kontakta“ koja, ne samo što pribavlja vrlo tačne podatke o otisku prsta, već i prevazilazi nedostatke kao što su suvi i vlažni prsti i skriveni otisci koji ostaju na konvencionalnim sistemima za skeniranje [15]. Na slici 3.2.3 prikazan je uređaj *MorphoWave*^{TM} *Desktop* integrisan u rešenje za kontrolu pristupa *MorphoWave*^{TM} *Tower*.



Slika 3.2.3: Predloženo rešenje komapnije SAFRAN Morpho

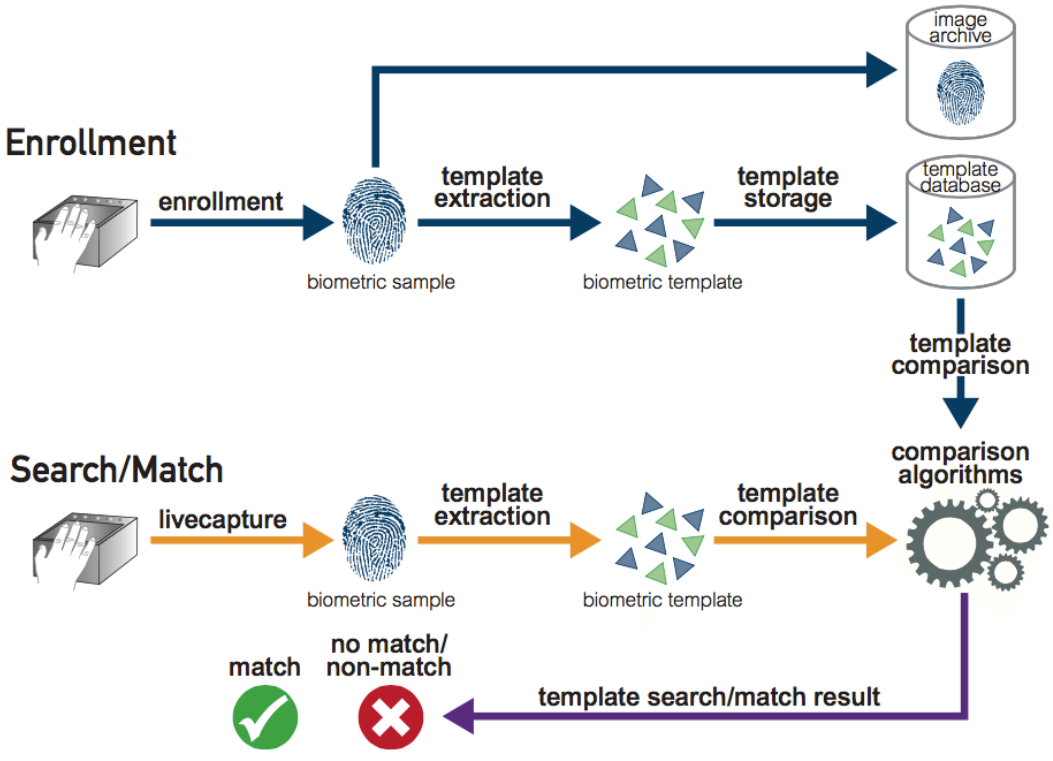
3.3. Princip rada biometrijskih sistema

Svaki biometrijski sistem se sastoji od pet modula:

- Senzorskog modula,
- Modula za izdvajanje podataka,
- Modula za skladištenje podataka (baze podataka),
- Modula za poređenje podataka,
- Modula za odlučivanje.

Svi biometrijski sistemi imaju dve faze, fazu upisivanja i produkcionu fazu. Faza upisivanja podataka neke osobe se sastoji od digitalizacije i memorisanja biometrijskih uzoraka. Pomoću senzora, od osobe se uzima biometrijski uzorak i konvertuje u digitalni oblik. Zatim se u modulu za izdvajanje jedinstvenih podataka, pomoću algoritama za obradu signala, obrađuje digitalizovani uzorak, smešta u šablon i čuva u bazi podataka za kasnije korišćenje.

U produkcionoj fazi, odnosno tokom provere identifikacije ili autentifikacije, skenira se biometrijski uzorak osobe, izdvajaju se podaci, a zatim ih biometrijski sistem, pomoću algoritma za poređenje, poredi sa podacima iz šablona, sačuvanih u bazi podataka. Kao izlazni rezultat dobija se stepen podudarnosti snimljenog ulaznog podatka sa šablonom iz baze podataka. Što je stepen podudaranja veći, to je sistem sigurniji da uzorci dolaze od iste osobe. U zavisnosti od stepena podudarnosti, sistem će prihvatiti ili odbiti osobu. Na slici 3.3.1. prikazan je princip rada biometrijskog sistema.



Slika 3.3.1: Princip rada biometrijskih sistema [14]

Bitno je napomenuti da nijedan biometrijski identifikacioni sistem nije potpuno precizan i da nikada nemamo apsolutno poklapanje. Skenirani biometrijski uzorak skoro sigurno se razlikuje od šablona sačuvanog u bazi podataka. Razlog za to su vreme i uslovi njihovog uzimanja, različite vrste senzora, pritisak na senzor, mikroklima, povrede i sl.

Biometrijski sistemi se mogu primeniti na dva načina [7]:

1. **Autentifikacija** tj. potvrda identiteta („Da li si ti onaj za koga se izdaješ?“) – sistem potvrđuje ili odbija identitet upoređivanjem biometrijskih karakteristika sa šablonom iz baze podataka. Ovakva vrsta poređenja naziva se jedan prema jedan (engl. *One-to-one comparison*). Ako neko želi da se identifikuje ili bude identifikovan, prilaže svoj biometrijski šablon koji se nalazi na kartici (npr. smart kartica). Sistem tada upoređuje podatke sa kartice osobe koja je priložila karticu sa ranije snimljenim podacima. Jedino ukoliko se oba podatka podudaraju, osoba će biti prihvaćena. Ovo je tzv. pozitivno prepoznavanje. Cilj je sprečiti da više ljudi koristi isti identitet.
2. **Identifikacija** tj. prepoznavanje identiteta („Da li ja znam ko si ti?“) – sistem upoređuje biometrijske karakteristike osobe sa šablonom sačuvanim u bazi podataka i traži najveće poklapanje. Ovakva vrsta poređenja naziva se jedan prema mnogo (engl. *One-to-many comparison*). U ovom slučaju osoba ne prilaže svoje podatke, već je sistem skenira i proverava da li su njeni podaci u sistemu. Nakon toga sistem proverava da li je toj osobi dozvoljen pristup. Ovo je tzv. negativno prepoznavanje. Cilj je sprečiti da jedna osoba koristi više identiteta.

Uobičajene metode autentifikacije (lozinka, PIN i token) rade samo u pozitivnom režimu prepoznavanja, dok u negativnivnom režimu se koristi biometrija. Aplikacije sa pozitivnim režimom prepoznavanja mogu da vrše verifikaciju i identifikaciju, a aplikacije sa negativnim režimom prepoznavanja samo identifikaciju.

Biometrijski sistemi mogu da rade u *online* i *offline* režimu rada. *Online* sistemi zahtevaju brzo prepoznavanje i trenutni odgovor (npr. logovanje na računaru). Ovi sistemi su potpuno automatizovani. *Offline* sistemi ne zahtevaju brzo prepoznavanje, te je odziv sistema duži. Ovi sistemi su polu-automatizovani, pa zahtevaju nadzor pri upisu biometrijskih podataka i manuelnu kontrolu kvaliteta. Algoritam poređenja daje listu mogućih kandidata, dok konačnu odluku donosi ekspert. Ovi sistemi se uglavnom primenjuju u forenzičkim i kriminološkim aplikacijama.

3.4. Performanse i greške u procesu verifikacije

Preciznost biometrijskog sistema može da se proceni na osnovu tri parametra:

1. koliko se biometrijski podatak jedne osobe povezuje sa biometrijskim podatkom druge osobe,
2. koliko se sadašnji biometrijski podatak neke osobe, ne poklapa sa ranije uzetim podacima,
3. nemogućnost preciznog određivanja.

Sva tri parametra su važna u slučaju identifikacije tipa 1:*N*, dok su drugi i treći parametar važni kod poređenja tipa 1:1.

Biometrijski uzorci i šabloni nikada nisu isti, pa sistem mora da izvrši procenu sličnosti i donese odluku o prihvatanju ili neprihvatanju. Sistem donosi odluku na osnovu vrednosti sigurnosnog praga. Ukoliko su vrednosti iznad sigurnosnog praga, prepoznavanje je uspešno, a ukoliko su vrednosti ispod sigurnosnog praga, prepoznavanje je neuspesno.

Moguće su dve vrste ispravnih odluka [12]:

- Ispravno prihvatanje (engl. *Genuine Acceptance*, ***GA***) – sistem prihvata legitimnog korisnika,
- Ispravno odbijanje (engl. *Genuine Rejection*, ***GR***) – sistem odbija osobu koja nije legitimni korisnik sistema.

Međutim, prilikom korišćenja biometrijskih sistema mogu se pojaviti sledeće greške:

- Greška lažnog prihvatanja (engl. *False Acceptance*, ***FA***) – sistem greškom prihvata osobu koju je trebao da odbije. Sistem prihvata lažnog korisnika kao legitimnu osobu, jer je u bazi pronašao podatak sličan ulaznom. Ova greška može se javiti ukoliko je veliki stepen sličnosti biometrijskih karakteristika različitih osoba,
- Greška lažnog odbijanja (engl. *False Rejection*, ***FR***) – sistem odbija osobu koju je trebao da propustiti. Ova greška nastaje ukoliko sličnost ulaznih podataka sa podacima u bazi nije dovoljna za prepoznavanje legitimnog korisnika.

Procenat lažnog prihvatanja (engl. *False Acceptance Rate*, ***FAR***) i procent lažnog odbijanja (engl. *False Rejection Rate*, ***FRR***) možemo izračunati na sledeći način:

$$FAR = \frac{FA}{GR + FA} \tag{3.4.1}$$

$$FRR = \frac{FR}{GA + FR} \tag{3.4.2}$$

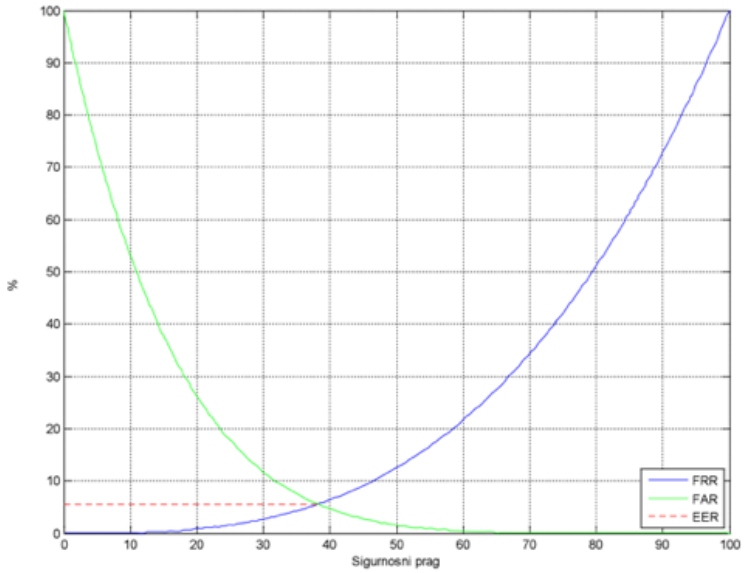
Tačan iznos *FAR* i *FRR* parametra, obično zavisi od korišćenog sigurnosnog praga sistema za identifikaciju ili verifikaciju. Menjanjem sigurnosnog praga smanjuje se *FRR* parametar na račun *FAR* ili obrnuto. Međutim, kod sistema sa višim nivoom sigurnosti, sistem će preciznije upoređivati trenutno unesene biometrijske podatake sa podacima u bazi.

Često se, za neki konkretni prag, tačnost biometrijskog sistema ne prikazuje *FAR* i *FRR* parametrima, već *ROC* (engl. *Reciever Operating Characteristic*) krivom. Korisnik sistema može izabrati tačku na *ROC* krivoj u kojoj će sistem da radi. Ova kriva na *x* osi ima *FAR* parametar, a na *y* osi procenat ispravnog prihvatanja (engl. *Genuine Acceptance Rate*, ***GAR***), gde je

$$GAR = 1 - FRR \tag{3.4.3}$$

Kao mera za procenu performansi sistema obično se koristi procenat jednakih grešaka (engl. *Equal Error Rate*, ***EER***), koji se dobija kao procenat grešaka u tački gde se parametri *FAR* i *FRR* seku, tj. imaju istu vrednost. Što su niže vrednosti ovih parametara, to je viši nivo osetljivosti sistema, tj. sistem će biti kvalitetniji i bolje će funkcionisati. Osim procenta jednakih grešaka, koristi se i minimalni ukupni procenat grešaka (engl. *minimum Total Error Rate*, ***mTER***), koji predstavlja minimalnu dobijenu vrednost za sumu *FAR* i *FRR* parametra.

Na slici 3.4.1. date su vrednosti *FAR* i *FRR* parametra, tipične za biometrijski sistem. Sa slike možemo da zaključimo da biometrijski sistem sa *EER* parametrom od 5% je tačniji od sistema sa *EER* parametrom od 50%. Međutim, *ERR* parametar se ne koristi u praksi. U zavisnosti od potrebe sistema, moguće je kreirati tzv. kritičnu vrednost sistema. Visoka kritična vrednost čini sistem identifikacije veoma sigurnim, pa je mogućnost neovlašćenog pristupa minimalna.



Slika 3.4.1: Zavisnost FAR i FRR parametra od sigurnosnog praga

Procenat grešaka je važan, ali ne učestvuje u proceni performansi sistema. Cena greška lažnog prihvatanja i lažnog odbijanja nije ista, već zavisi od domena upotrebe aplikacije. Na primer, kod sigurnosnih aplikacija za kontrolu pristupa zahteva se što manji *FAR* parametar. Kod forenzičkih aplikacija je slučaj obrnut i zahteva se manji *FRR* parametar. Forenzičke aplikacije uglavnom zahtevaju upotrebu sistema koji proizvodi *FAR*, zbog provere načina pristupa i hvatanja kriminalca.

Greške *FAR* i *FRR* su karakteristične kod pozitivnog režima rada, dok se kod negativnog režima javljaju greške koje se opisuju *FMR* i *FNMR* parametrima. Procenat lažnog poklapanja (engl. *False Match Rate*, ***FMR***) pokazuje kvalitet sistema, dok procenat lažnog ne poklapanja (engl. *False Non-Match Rate*, ***FNMR***) pokazuje robustnost sistema. Za sumarizovanje tačnosti verifikacionih sistema i pokazivanje nivoa greške za sigurnosni prag najčešće se koristi *EER* parameter, gde je *FMR* = *FNMR*.

FMR i *FNMR* su funkcije koje zavise od sistemskog sigurnosnog praga. Ako se sigurnosni prag smanji, da bi se sistem učinio tolerantnijim, tada će se sigurnosni prag *FMR* funkcije povećati. Ako se sigurnosni prag poveća, da bi se sistem učinio sigurnijim, tada će se sigurnosni prag *FNMR* funkcije povećati [13].

Performanse biometrijskih sistema zavise od vrste aplikacije koja se primenjuje. Osnovni zahtev za sistemsku tačnost je mali *FNMR* parametar, što je karakteristično kod forenzičkih aplikacija, dok se kod sigurnosnih aplikacija zahteva mali *FMR* parametar. Međutim, postoji niz aplikacija gde se oba parametra moraju uzeti u obzir.

Za određivanje performansi identifikacionih sistema, mogu se koristiti parametri verifikacionih sistema. Ako je *FMR* parametar veoma mali, tada verovatnoća greške raste linearno sa veličinom baze podataka. Ovo veoma utiče na razvoj velikih identifikacionih sistema, više nego brzina računara. U slučaju da su šabloni klasifikovani, tada se pretražuje samo deo baze podataka. Ukoliko postoji verovatnoća da je povučen pogrešan šablon (engl. *Retrieval Error Rate,* ***RER***), generiše se *FMR*, a ako je šablon korektno povučen, tada je *FNMR = FNMR*.

Tokom procesa upisa, mogu se pojaviti problemi pri prikupljanju podataka za hendikepirane osobe, osobe sa urođenim manama, izvršenim operacijama ili povredama. Tada korisnik nije u mogućnosti da u pojedinim sistemima identifikacije pruži tražene biometrijske podatke. Ove teškoće mogu se definisati parametrima: greška kod uzimanja podataka (engl. *Failure to Acquire,* ***FTA***) i greška kod upisa (engl. *Failure to Enroll,* ***FTE***).

FTA parametar predstavlja procenat korisnika koji pri upisu ne mogu da prezentuju sistemu korisne biometrijske karakteristike. *FTE* parametar predstavlja procenat korisnika gde, zbog tehnološkog ograničenja, sistem ne može da generiše kvalitetan šablon za upis. Kvalitet prihvatanja biometrijskog šablona zavisi od *FTA* i *FTE* parametra. Pri procesu upisa koristi se i ***TTE*** (eng. *Time to Enroll*) parametar, koji pokazuje trajanje procesa upisa od trenutka očitavanja uzorka do kreiranja šablona.

3.5. Nedostaci biometrijskih sistema

Sa razvojem i primenom biometrijskih sistema, javljuju se nedostaci, koje možemo da podelimo u dve kategorije. Prvu kategoriju čine nedostaci koji su vezani za lošu zaštitu privatnosti biometrijskih podataka. U slučaju kompromitovanja kriptoloških ključeva, biometrijski podaci se zauvek gube, uprkos šifrovanom biometrijskom obrazcu. Drugu kategoriju čine nedostaci koji su vezani za bezbednost sistema. Biometrijski obrazci se ne nalaze uvek u šifrovanoj formi, pa se prilikom autentifikacije tj. provere stepena poklapanja dva biometrijska obrasca, koriste dešifrovani biometrijski podaci.

Jedan od najvećih problema, kod biometrijskih podataka, predstavlja varijabilnost. Bez obzira na tip biometrijskog izvora, varijabilnost između biometrijskih podataka nastaje skoro u svim fazama obrade podataka (od trenutka očitavanja, pa sve do generisanja biometrijskog obrazca), a kao posledica varijabilnosti, sveže generisani biometrijski obrazac će se potpuno razlikovati od uskladištenih referentnih biometrijskih obrazaca. Svaki novi biometrijski podatak, generisan na istom biometrijskom izvoru, uvek se razlikuje od prethodnih za 10% – 20%, dok se biometrijski podaci generisani na različitim biometrijskim izvorima razlikuju za 40% – 60%.

S obzirom da biometrijski podaci sadrže šum koji znatno povećava varijabilnost podataka i utiče na informacioni kvalitet biometrijskog uzorka, nikada nećemo imati potpuno poklapanje dva biometrijska podatka, jer je nemoguće očitati identičan biometrijski podatak sa istog biometrijskog izvora više puta. Ovakav problem može da se reši primenom odgovarajućih tehnika za obradu signala i kodova za ispravljanje grešaka.

Na primer, tehnika za identifikaciju na osnovu biometrije lica ima visok stepen varijabilnosti zbog raznih spoljašnjih uticaja (osvetljenje i ugao pomeranja korisnika). Sličan slučaj je i kod biometrije otiska prsta, gde brojni faktori utiču na neefikasno izdvajanje postojanih informacija iz otiska prsta. Na osnovu analize osobina utvrđeno je da iris oka, osim visokog stepena pouzdanosti i postojanosti, sadrži najmanju varijabilnost i najveću količinu informacija.

Ukoliko biometrijski sistem, u fazi prepoznavanja, ne može da potvrdi visok stepen sličnosti, on je prinuđen da odbaci legitimnog korisnika (*FRR*). Ukoliko bi se dizajnirali biometrijski sistemi sa niskim *FRR* parametrom, omogućilo bi se pravilno funkcionisanje sistema. Standardne metode za poboljšanje rada su kontrolisanje uslova u kojima se očitavaju izvori biometrijskih podataka i optimizacija matematičkih algoritama. Sa smanjenjem *FRR* parametra, direktno se utiče na *FAR* parametar, a to bi značilo da je sistem napravio grešku kod identifikacije i prihvatio pogrešnu osobu na osnovu tuđeg referentnog biometrijskog obrasca. Takođe, neophodno je napraviti kompromis između ova dva parametra, tako da sistem bude prilagođen okruženju (neka okruženja dozvoljavaju visok *FRR*, dok druga visok *FAR*), imajući u vidu da sa smanjenjem jednog parametra utičemo na drugi.

Vrednosti *FAR* i *FRR* parametara su često nepouzdane, jer ih navodi prodavac sistema. S obzirom da ne postoji standard u proizvodnji biometrijskih uređaja za identifikaciju, postoji mogućnost da se ne poklope biometrijski podaci sa dva različita uređaja, što dovodi do povećanog broja neuspešnih pokušaja. Zbog toga neophodno konsultovati nezavisne izvore informacija tj. javna takmičenja na polju biometrijskih istraživanja u organizaciji Nacionalnog instituta za standarde i tehnologiju (engl. *National Institute of Standards and Technology,* ***NIST***).

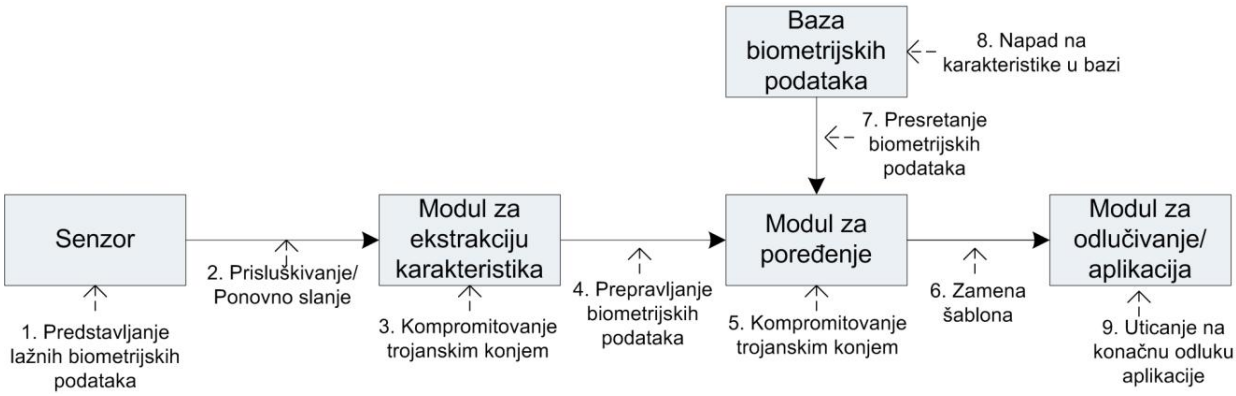
Kod većine biometrijskih sistema, vrednost *FRR* parametra kreće se od 0.1% do 20%, što znači da će legitimni korisnik biti odbijen najmanje jednom od 1000 puta. Kod *FAR* parametra je jedan prihvaćen od 100 (aplikacije sa niskim stepenom sigurnosti) i jedan prihvaćen od 10.000.000 (aplikacije sa visokim stepenom sigurnosti) [4].

3.6. Bezbednost biometrijskih sistema

Sa uvođenjem biometrije pojavljuju se izazovi i pretnje u domenu privatnosti za poslovna okruženja. Ukoliko nisu primenjene odgovarajuće metode zaštite, mogući su napadi na privatnost, krađa poslovnih tajni, ali i napadi u cilju zloupotrebe.

Napad na privatnost podrazumeva neovlašćeni pristup tuđim, privatnim informacijama. Na osnovu poređenja biometrijskih podataka u sistemu za kontrolu pristupa sa odgovarajućim podacima u nekom zdravstvenom sistemu, kompanija može saznati detaljne informacije o zdravlju svojih zaposlenih. Kod krađe poslovnih tajni, pojedinac kompromituje kompaniju, a kao posledica svega, kompanija može da bude izložena ogromnim finansijskim gubicima. Kod napada u cilju zloupotrebe, neovlašćeno lice manipuliše sa tuđim podacima tj. lažno se predstavlja i preusmerava transakciju na druge račune.

Pri prenosu biometrijskih podataka, od senzora do modula za odlučivanje, postoji rizik od različitih vrsta napada kao što su: predstavljanje lažnih biometrijskih podataka senzoru (engl. *Spoofing*) i maskiranje (engl. *Masquerade attack*), prisluškivanje kanala (engl. *Eavesdropping*) i ponovno slanje (engl. *Replay attack*), ubacivanje prethodno snimljenog podatka, prepravljanje i falsifikovanje biometrijskih karakteristika (engl. *Tampering*), kompromitovanje podataka ubacivanjem trojanskog konja, presretanje podataka, zamena sačuvanih biometrijskih karakteristika u bazi (engl. *Substitution attack*), uticanje na odluku modula za odlučivanje (engl. *Overriding Yes/No response*). Izazivanje preopterećenja (engl. *Overloading*) je takođe veoma čest napad, u kom se ulazni uređaj oštećuje ili primorava na generisanje grešaka (npr. kratak spoj, kvašenje poluprovodničkih senzora, izlaganje senzora bljesku svetlosti). Na slici 3.6.1. prikazana je generička šema biometrijskog sistema sa potencijalnim napadima na biometrijski sistem [8].



Slika 3.6.1: Vrste napada na biometrijski sistem

Kako napadač ne bi uspeo da dođe do poverljivih podataka, potrebno je, komunikacioni kanal, obezbediti fizički ili kriptografski. Primenom neke od kriptografskih tehnika možemo rešiti bezbednosni rizik kojem je biometrijski sistem izložen. Jedno od rešenja je upotreba smart kartice, što ceo sistem (od senzora do modula za odlučivanje) integriše u celinu. Međutim, ovo rešenje nije primenljivo kod svih biometrijskih sistema.

Neki sistemi zahtevaju centralizovanu bazu podataka, gde primenom kriptografije možemo zaštititi komunikacioni kanal. Ukoliko imamo manji sistem, podatke možemo zaštititi kriptovanjem, primenom nekog od simetričnih algoritama enkripcije (npr. AES algoritam), uz prethodnu razmenu ključeva. Kako bi spečili ponovno slanje podataka, uz podatak možemo slati informaciju o vremenu slanja (engl. *Timestamp*). Primenom nekih od kriptografskih heš funkcija, takođe, možemo obezbediti integritet poruke. Ukoliko imamo neku složeniju arhitekturu, predlaže se primena PKI infrastrukture ili protokola koji koristi i asimetrične kriptografske algoritme (npr. SSL/TLS).

Mere protiv obmane (engl. *Anti-spoofing*) i enkriptovanje podataka pri prenosu predstavljaju kritične tačke biometrijske sigurnosti. Veoma je važno da slanje biometrijskih podataka, lokalnom ili udaljenom računaru, bude sigurno. Većina biometrijskih sistema šifruje podatke pri prenosu, ali se to ne odnosi uvek na same aplikacije i uređaje. Kao sigurnosno rešenje, može se primeniti tzv. više-faktorna autentifikacija i randomizacija.

Više-faktorna autentifikacija se može predstaviti kao kombinacija od više biometrijskih metoda ili kao kombinacija biometrije i pametne kartice ili PIN-a. Takođe, verifikacioni podaci mogu biti randomizovani, što povećava nivo sigurnosti, pa se za autentifikaciju jedan dan mogu tražiti tri prsta, dok sledeći dan kombinancija od dva prsta itd. Kopiranje više ljudskih karakteristika je vremenski zahtevnije, pa ove metode smanjuju mogućnost neželjene autentifikacije.

3.7. Zaštita biometrijskih sistema

Da bi biometrijski sistemi bili bezbedni potrebno je primeniti servise zaštite koji će obezbediti:

- **Zaštitu tajnosti informacija** – sprečavanje otkrivanja sadržaja informacija, primenom odgovarajućeg algoritma za šifrovanje;
- **Autentifikaciju** – proveru identiteta pošiljaoca;
- **Integritet informacija** – sprečavanje neovlašćene izmene informacija;
- **Neporecivost** – dokaz da je korisnik poslao određenu poruku u određeno vreme;
- **Nadzor i upravljanje** – praćenje i beleženje bezbednosnih elemenata primenom specijalnih aplikacija koje prepoznaju i onemogućavaju upad u sistem.

Mehanizmi zaštite koji omogućuju realizaciju predhodno navedenih servisa su:

- **Šifrovanje** – obezbeđuje tajnost;
- **Digitalni potpis** – obezbeđuje autentifikaciju;
- **Kontrolni niz** – štiti integritet poruke i onemogućuje njenu izmenu;
- **Digitalni pečat** – obezbeđuje neporecivost;
- **Kontrolna lista pristupa**.

Zbog kontinualnog tehnološkog razvoja, kriptografski mehanizmi koji su namenjeni za zaštitu poverljivosti i integriteta podataka, zahtevaju kriptološke ključeve većih dužina koje je potrebno čuvati na sigurnim mestima. Međutim, te informacije nije moguće zapamtiti, pa je neophodna primena različitih hardverskih uređaja za skladištenje kriptoloških ključeva.

Biometrija se, osim za generisanje ključeva, može primeniti i za skladištenje, čuvanje i distribuciju kriptoloških ključeva. Na osnovu izvršenih analiza različitih kriptoloških ključeva, pokazalo se da iris ima dovoljnu količinu informacija za generisanje ključa dovoljne dužine sa visokim stepenom sigurnosti. U tabeli 3.7.1. dato je poređenje vrednosti dužine ključa sa *FAR* i *FRR* parametara, za različite vrste biometrije.

Tabela 3.7.1: Poređenje sa postojećim rezultatima u ovoj oblasti

Biometrija	Dužina ključa (bit)	Procenat lažnog odbijanja (*FRR*)	Procenat lažnog prihvatanja (*FAR*)
Glas	46	20%	–
Svojeručni potpis	40	28%	1.2%
Otisak prsta	–	–	–
	69	30%	–
	49 i 85	5.4% – 9.9%	3.2% – 2.5%
Lice	80	0.93%	–
	58	3.5%	0%
Iris	140	0.47%	0%
	186	0.76%	0.096%
	400	4.75%	0%
EKG i Glas	240	1.27%	10.62%

3.8. Čuvanje i poređenje biometrijskog šablona

Svaka aplikacija za autentifikaciju sa biometrijskim sistemom povezana je skupom funkcija koja treba da omogući prijavu korisnika, authentifikaciju i pretragu identiteta.

Sa aspekta sigurnosti, dva osnovna elementa biometrijskog sistema su čuvanje i poređenje. U zavisnosti od aplikacije, šablon se može čuvati na više lokacija [13]:

- **Centralna baza podataka** – Omogućava autentifikaciju sa više različitih lokacija, zbog povezanosti sa puno senzora. Upravljanje podacima koji se nalaze na jedinstvenoj lokaciji je jednostavno. Međutim, ukoliko podaci nisu dovoljno zaštićeni, mogu biti kompromitovani;
- **Lokalna baza podataka** – Smeštena je u računaru na koji je priključen biometrijski senzor. Zbog nemogućnosti udaljene autentifikacije smanjuje se mogućnost napada;
- **Pametna kartica** – Podaci se ne prenose putem mreže, već se smeštaju na pametnu karticu, što smanjuje opasnost od napada. Nedostatak ove metode je što administrator nema uvid da li postoji duplikat kartice (jedan otisak prsta za dva različita identiteta), kao i visoka cena (svaki senzor zahteva čitač kartice);
- **Senzor** – Primenjuje se ukoliko korisnik za pristup uvek koristi isti senzor. Sistem daje brz odgovor, pošto se šablon smešta na senzor. Nedostatak ovog sistema je što senzor može biti ukraden ukoliko nije obezbeđen, kao i nemogućnost autentifikacije sa više lokacija.

Takođe, veoma bitan faktor koji utiče na performanse sistema je lokacija za poređenje šablona. Postoje četiri lokacije za poređenje šablona:

- **Centralni server** – Primenjuje se ukoliko su šabloni smešteni u centralnu bazu podataka. Nedostatak ove metode je što postoji mogućnost upada u komunikacionu vezu između senzora i servera;
- **Lokalni računar** – Može funkcionisati sa centralnim i lokalnim bazama. Bolje performanse se dobijaju u drugom slučaju;
- **Senzor** – Obezbeđuje brz rad i visok nivo sigurnosti, jer je izolovan od spoljne sredine;
- **Pametna kartica** – Sistem je izolovan, pa ovaj mehanizam obezbeđuje kompletnu sigurnost. Nedostatak je komunikacija između čitača i kartice.

U daljem tekstu ćemo razmatrati kombinacije mesta čuvanja i poređenja podataka.

1. **Poređenje na centralnom serveru / Čuvanje u centralnoj bazi –** Poređenje na centralnom serveru je poređenje u zaštićenom okruženju. Administrator može da detektuje pokušaj napada, jer ima potpunu kontrolu nad bazom podataka. Čuvanjem na serveru u centralnoj bazi, šablon je zaštićen od spoljašnje zloupotrebe. Međutim, sigurnosni problem predstavlja prenos šablona, od senzora do servera, putem otvorene mreže. Ovaj problem se može rešiti sigurnijom Internet sesijom ili primenom nekih od kriptografskih rešenja.
2. **Poređenje na centralnom serveru / Čuvanje na pametnoj kartici –** Šablon ostaje kod korisnika na pametnoj kartici, pa korisnik ima potpunu kontrolu nad šablonom. Sigurnosni problem se javlja prilikom prenosa šablona putem otvorene mreže i njegovog smeštanja na server.
3. **Poređenje u lokalnom računaru / Čuvanje u lokalnoj bazi –** Šablon se čuva na hard disku lokalnog računara na kojem se vrši poređenje. Iako je ova kombinacija česta, lokalni računar nije bezbedno okruženje za osetljive podatke, jer postoji opasnost da šablon ili

lozinka budu kompromitovani. Takođe, problem predstavlja mobilnost tj. korisnik se može prijaviti samo na računaru na kojem se nalazi šablon.

4. **Poređenje u lokalnoj bazi / Čuvanje na pametnoj kartici –** Sa unosom tačnog PIN-a dozvoljava se pristup kartici. Zatim se PIN i šablon prenose do lokalnog računara, gde se u lokalnoj bazi proverava šablon. Ukoliko uneta slika odgovara šablonu, PIN se vraća nazad do kartice i omogućava se pristup. Do šablona je nemoguće doći sve dok se nalazi na kartici, Međutim, u fazi slanja na lokalni računar tj. tokom verifikacije, PIN i šablon mogu biti izloženi napadima.
5. **Poređenje u senzoru / Čuvanje u senzoru –** U ovom slučaju, sve informacije se nalaze u senzoru. S obzirom da se šablon nalazi u senzoru, prenosivost je ograničena i ne može mu se pristupiti putem nekog drugog uređaja. Korisnik ima kontrolu nad šablonom koji nikad nije izložen spoljnim uticajima, što drastično otežava zloupotrebu.
6. **Poređenje u senzoru / Čuvanje na pametnoj kartici –** Poređenje se vrši na samom senzoru. Korisnik ima kontrolu nad svojim šablonom, kojem se može pristupiti sa svakog uređaja. Pomoću PIN-a ili lozinke pristupa se pametnoj kartici. Nakon potvrde autentičnosti biometijskog podatka, PIN se vraća pametnoj kartici kako bi omogućio pristup. Sigurnosni problem se javlja kada PIN za otključavanje kartice (i koji se nalazi na njoj) se šalje do senzora, pre dozvole pristupa kartici. Tada je šablon izložen spoljnim napadima.
7. **Poređenje na pametnoj kartici / Čuvanje na pametnoj kartici –** Pametnoj kartici se ne može pristupiti bez odgovarajuće biometrijske autentifikacije. Korisnik kontroliše svoj šablon koji je uvek na kartici. Nakon uspešnog poređenja unete slike i šablona, omogućava se upotreba sertifikata, bez ikakve potrebe za PIN-om ili lozinkom. Za razliku od prethodnih slučajeva, šablon nije izložen nesigurnom okruženju i ne postoji informacija koja može biti ukradena. Ovaj metod je zasnovan na PKI infrastrukturi i predstavlja najsigurniji način zaštite računara i digitalnih podataka.

3.9. Zaštita biometrijskih šablona

Skladištenje biometrijskih podataka je izuzetno osetljivo po pitanju bezbednosti. Ukoliko podaci, koji se čuvaju, nisu kriptovani, može doći do značajnog narušavanja bezbednosti. Rizik je mnogo veći ukoliko sistem koristi centralnu bazu podataka.

Za zaštitu ovih podataka možemo primeniti dva pristupa:

1. **Primenom nekih od kriptografskih algoritama** – Algoritmi za kriptovanje i dekriptovanje (npr. AES, RSA) zahtevaju upotrebu tačno određenog ključa. Međutim, uvek postoji razlika između šablona biometrijskih karakteristika kod iste osobe. Uprkos tome što su te razlike minimalne, standardni algoritmi za enkripciju projektovani su tako da se kriptovani izlazi potpuno razlikuju, čak i ako su ulazi veoma slični. Ukoliko želimo da primenimo neki od ovih algoritama, potrebno je izvršiti dekripciju u okviru modula za poređenje, što može dovesti do kompromitovanja sistema.
2. **Primenom alternativnih kriptografskih metoda** – Algoritmi za zaštitu šablona mogu se podeliti na:
    - Biometrijski kriptosistem – Služi za zaštitu kriptografskog ključa, a može se primeniti i za zaštitu šablona. Na osnovu podataka, koji se čuvaju u bazi, nije moguće rekonstruisati originalne biometrijske karakteristike, niti doći do korisnih

informacija o njima. Često korišćena tehnika za skladištenje je (engl. *Fuzzy vault*). Uvođenjem ove šeme, napadač neće imati informacije o biometrijskim karakteristikama, dok će se, prilikom poređenja sa šablonom, ponašati kao originalni šablon sa biometrijskom karakteristikom.

- Algoritmi za transformaciju karakteristika – Ovi algoritmi vrše enkripciju karakteristika. Poređenje se vrši nad transformisanim biometrijskim karakteristikama. Predložena su tri algoritma za transformaciju karakteristika otiska prsta, čiji je osnovni cilj omogućavanje povlačenja biometrijskih karakteristika.

Prilikom zaštite biometrijskog šablona mora se obezbediti raznovrsnost tj. mogućnost uzajamne pretrage kroz više različitih baza podataka pomoću zaštićenog šablona, ali i obnovljivost tj. dobijanje novog šablona iz iste biometrijske karakteristike. U slučaju kompromitovanja treba omogućiti da se šablon poništi, kako napadač ne bi došao do izvorne biometrijske karakteristike. Takođe, treba obratiti pažnju da primenjene zaštitne mere ne naruše performanse sistema.

Metoda koja je bliska biometrijskoj kriptografiji, je metoda nazvana (engl. *Cancelable Biometrics*), koja omogućava opoziv biometrijskog šablona i izdavanje novog. Ovaj IBM-ov koncept predviđa upotrebu distorzije, koja će uneti deformisanost na sačuvani šablon. Ukoliko dođe do kompromitovanja, šablon se otkazuje i uklanja sa liste dozvoljenih pristupa. Kada se legalni korisnik bude ponovo prijavljivao, kreiraće se njegov novi šablon, sa dodatnim deformitetom, primenom distorzije.

Ova metoda, isto kao i biometrijska kriptografija, primenjuje tehniku biometrijskog hešovanja (engl. *bioHashing*). Takođe, bitno je reći da se originalna slika nikada ne čuva, jer je pomoću originalne slike i novog generisanog izobličenog šablona, moguće izvršiti ponovnu prijavu. Sve dok je algoritam dobro zaštićen, ovaj koncept predstavlja dobro rešenje za smanjenje nastanka štete.

3.10. Biometrijska kriptografija

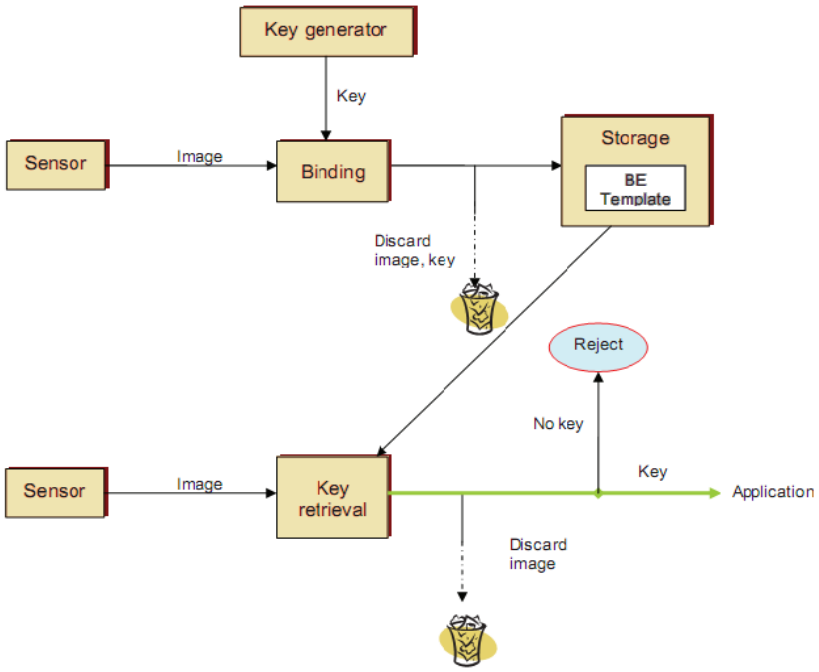
Biometrijska kriptografija (engl. *Biometric Encryption*) je tehnologija koja primenjuje PIN, lozinku ili kriptološki ključ u kombinaciji sa biometrijskim podatkom.

Originalni koncept biometrijske kriptografije primenjuje se 1994. godine nad otiscima prstiju. Od tada, zbog izuzetnih mogućnosti biometrijskih i kriptoloških sistema, mnoge naučno-istraživačke grupe radile su na povezivanju i razvoju ovih oblasti, ali i drugih srodnih tehnologija.

Osim naziva biometrijska kriptografija, u literaturi se koriste i drugi nazivi: biometrijski kripto sistemi (engl. *Biometric cryptosystem*), privatni obrasci (engl. *Private template*), biometrijsko zaključavanje (engl. *Biometric locking*), sigurna skica (engl. *Secure sketch*), biometrijsko vezivanje ključeva (engl. *Fuzzy commitment scheme, Fuzzy vault*), biometrijsko generisanje ključeva (engl. *Biometric key generation*), virtuelni PIN (engl. *Virtual PIN*), biometrijski potpis (engl. *Biometric signature*) i biometrijsko hešovanje (engl. *BioHashing*).

Kriptografski ključevi predstavljaju suštinski deo svakog kriptografskog sistema. Ključ predstavlja binarnu sekvencu definisane dužine (128, 192, 256 bitova ili više). Mogu biti simetrični, javni ili privatni. Dužina ključa ne sme da prelazi ukupnu količinu informacija koju ima biometrijski izvor, što je dato preko entropije na kojoj su zasnovani kriptograski principi.

Originalni biometrijski podaci i ključ ne mogu se otkriti na osnovu referentnog podatka za skladištenje. Originalni ključ moguće je regenerisati u početnoj fazi generisanja sa novim biometrijskim podatkom, bez sladištenja prvog generisanog biomerijskog podatka. Da bi ključ bilo moguće regenerisati, oba biometrijska podatka ne moraju biti identična, ali moraju da potiču iz istog biometrijskog izvora. Na ovaj način je napravljen kompromis između kriptografske preciznosti i biometrijske promenljivosti. Na slici 3.10.1. prikazana je blok šema sistema za biometrijsku kriptografiju.



Slika 3.10.1: Blok šema funkcionisanja biometrijske kriptografije

3.11. Primena biometrijske kriptografije

Sa primenom biometrijske kriptografije ostvaren je veliki napredak u poboljšanju informacione bezbednosti.

Radovi objavljivani od 2002. godine, koji su osnova tehnologije biometrijske kriptografije, pokazali su da je moguće napraviti sistem otporan na napade, čak i kod potpune pretrage (engl. *Brute force*). Kod ovog napada, ukoliko napadač poseduje podatak koji ne odgovara ni jednom referentnom podatku u bazi, probaće sve kombinacije. Takođe, napadač može da izvede sofisticirani napad koji koristi nasledne slabosti (zavisnost između dva biometrijska podatka ili dva referentna biometrijska podatka koji u sebi sadrže zaključan ključ i originalni biometrijski podatak). Ako ovakav napad uspe, sigurnost sistema smanjiće se sa 140 bitova na 70 ili 50 bitova.

Soutar i Tomko izučavali su praktičan sistem privatnog šifrovanja (sličan DES-u) koji se zasniva na Furijeovoj transformaciji slike otiska prsta. Primena nevidljivih vodenih pečata obezbeđuje da sve slike u biometrijskoj bazi budu autentične i da ih niko neovlašćeno ne menja. Primenjuje se u slučaju kada je neophodna vizuelna kontrola, a da se pritom kodirana informacija ne enkriptuje. Ovakve slike se ne primenjuju prilikom izdvajanja ili upoređivanja biometrijskih karakteristika [9].

Upotreba digitalnih vodenih pečata je dobro rešenje ukoliko se biometrijske karakteristike prenose nesigurnim mrežom. Biometrijske karakteristike se sakrivaju u slici u kojoj su pikseli izmenjeni po tajnom ključu. Tajni ključ, koji je sakriven u slici, može biti lice korisnika.

Kod metode primene dva ključa, jedan ključ se primenjuje za šifrovanje biometrijskog šablona, a drugi za utiskivanje vodenog pečata. Prvi ključ čini metod sigurnijim, a drugi robusnijim. Ova metoda obezbeđuje visoku tačnost izdvajanja sadržaja, čak i kada postoje šumovi i izobličenja.

Biometrija i kriptografija su dve komplementarne tehnologije, pa se njihovom kombinacijom, uz veliki stepen sigurnosti, može napraviti jaka veza između digitalnog potpisa i njegovog vlasnika. Najviše se primenjuje u mobilnim aplikacijama, kod identifikacionih dokumenata, u kontroli pristupa digitalnim podacima i očuvanju autorskih prava.

3.12. Primena infrastrukture javnih ključeva u biometriji

Infrastruktura javnih ključeva (engl. *Public Key Infrastructure*, **PKI**) je sistem za podršku digitalnog potpisa i tajnosti dokumenata u komunikaciji. PKI sadrži bazu javnih ključeva preko kojih obezbeđuje autentifikaciju u mrežama.

Za razvoj biometrijske PKI infrastrukture, potreban je novi sistem sa javnim ključevima koji će biti direktno zasnovan na biometrijskim podacima, a da pritom odgovara postojećoj PKI infrastrukturi. Ovaj sistem zahteva ključeve velike dužine (1024 ili 2048 bitova), koji su često zaštićeni lozinkama ili PIN-om.

Prilikom primene biometrije u PKI infrastrukturi, mogu da nastupe sledeći slučajevi [9]:

- **Upotreba biometrije za oslobađanje ključa** – Ključ se čuva zajedno sa biometrijskim šablonom. Nakon uspešne verifikacije, ključ se oslobađa, a šablon se čuva;
- **Upotreba biometrije za dodeljivanje ključa** – Ključ se dodeljuje biometrijskom šablonu. Nakon uspešne verifikacije, ključ se oslobađa, a šablon se ne čuva;
- **Upotreba biometrije za generisanje ključa** – Ključ se dobija iz biometrijskog podatka. Međutim, šablon sa velikom entropijom veoma je teško generisati.

Sa razvojem biometrijskog PKI sistema, omogućilo bi se jednostavnije generisanje i distribucija kriptoloških ključeva. Takođe, svaki korisnik *online* transakcije bio bi maksimalno bezbedan. Međutim, nedostatak ovog sistema je što zahteva poverenje u treću stranu od poverenja, koja je zadužena za izdavanje i potpisivanje privatnih ključeva.

3.13. Generisanje ključeva iz biometrije

Tehnika za generisanje ključeva iz biometrije obezbeđuje zaštitu privatnosti, mogućnost ponovnog generisanja javnih ključeva za primenu kod sistema za autentifikaciju, kriptografsku zaštitu podataka, digitalno potpisivanje i sl.

Nakon što korisnik pristupi svom nalogu i unese lozinku L, servis, koji već poseduje informaciju $y = f(L)$, će izračunati $f(L) = y'$. Ukoliko su vrednosti y i y' jednake, izvršena je uspešna autentifikacija korisnika.

Lozinka može biti generisana na osnovu jednog ili kombinacijom više biometrijskih podataka. Biometrijski podaci sadrže mnogo veću količinu informacija od tradicionalnih lozinki. Međutim, biometrijski podaci u ulozi lozinke nisu sa uniformnom distribucijom i nisu precizno ponovljivi. Zbog razlike u očitavanju biometrijskih podataka iz istog biometrijskog izvora, određeni broj grešaka treba tolerisati kako bi sigurnost ostala na visokom nivou.

Sigurnost sistema zasniva se na neinvertibilnosti funkcije $f(L)$. Jednosmerna funkcija (engl. *one-way functions*) poseduje osobinu neinvertibilnosti, koja obezbeđuje mogućnost opoziva biometrijskih podataka i ponovno generisanje biometrijskih podataka u svrhu autentifikacije. Na ovaj način su zamenjeni tradicionalni biometrijski sistemi.

Neke jednosmerne funkcije zadržavaju u podacima osnovne karakteristike biometrijskih podataka koje pozitivno utiču na Hamingovo rastojanje (metod koji se koristi za prepoznavanje ili poređenje biometrijskih podataka).

Ulogu kriptološkog ključa kod ovih aplikacija imaju slučajni uniformni nizovi bez šuma. Međutim, u stvarnosti, takve nizove teško je generisati i čuvati. Konvertovanje neuniformih biometrijskih podataka sa šumom u uniformne nizove sa velikom entropijom je važan problem. Kao rešenje predložena je funkcija „*Fuzzy extractors*“ koja ima zadatak da neuniformni slučajni podatak sa malom entropijom pretvori u podatak sa uniformnom distribucijom i velikom entropijom.

3.14. Generisanje ključeva na osnovu biometrije

Vremenom je nastala ideja o generisanju kriptoloških ključeva na osnovu biometrije. Softverska i hardverska rešenja za skladištenje, obradu i prenos podataka, moraju da koriste kriptografske mehanizme radi obezbeđivanja informacione sigurnosti. Jačina kriptografskog mehanizma zavisi od kriptološkog ključa.

Postoje dva načina za generisanje kriptoloških ključeva. Kod prvog (engl. *Data binding*), nezavisno generisani ključ čvrsto se vezuje sa biometrijskim podatkom, a kod drugog (engl. *Fuzzy extractor*), ključ se ekstraktuje iz biometrijskog podatka.

Kod oba načina korste se pomoćni podaci. Pomoćni podatak je ključ izveden iz biometrijske karakteristike, ali može, zajedno sa originalnim biometrijskim podatkom, omogućiti generisanje ključa. Može se čuvati u bazi, računaru, smart kartici, tokenu ili mobilnom telefonu.

Nakon uzimanja uzorka, kriptografski ključ se generiše. Ključ je nezavisno generisan, a podaci o njemu su nepoznti i mogu se menjati. Primenom logičke operacije sabiranja XOR, ključ se šifruje sa biometrijskim podatkom, a rezultat je biometrijski kodovani ključ (javna informacija ili pomoćni podatak). Po završetku celokupne procedure ključ i biometrijski podatak se uništavaju.

Na osnovu pomoćnog podatka i odgovarajućeg biometrijskog obrazca, uz ponovljenu XOR operaciju, kriptološki ključ se može regenerisati ili ponoviti. Ukoliko napadač pokuša da regeneriše ključ, koristeći biometrijski podatak koji se razlikuje od originalna, algoritam neće prezentovati originalni ključ.

Kriptološki ključevi mogu se generisati iz biometrijskih podataka. U biometrijske podatke moguće je smestiti jedinstvene binarne nizove, koji imaju ulogu kriptološkog ključa. Ovaj ključ je moguće kasnije regenerisati.

Metoda „*Fuzzy commitment scheme*“ prikriva i vezuje podatke. Za otključavanje ovakve vrste podatka potreban je identifikator. Predložena šema tolerantna je na nastale greške, a primenljiva je u sistemima za biometrijsku autentifikaciju, gde može da zaštiti biometrijske podatke.

Sistem baziran na otisku prsta, primenjuje faznu informaciju koja se ekstraktuje sa slike otiska prsta, primenom Furijeove transformacije i kodova za ispravljanje grešaka. Uvodi se metod biometrijskog zaključavanja, gde se slučajni ključ zaključava sa faznom informacijom. Ovako dobijen podatak može se otključati samo sa originalnom biometrijom.

Kod biometrije otiska prsta primenjuje se fazni Gaborov filtar za ekstrakciju informacionih sadržaja i *BCH* kodovi za ispravljanje grešaka (izdvajanje pouzdanih bitova informacija iz biometrije). Za ključ dužine 49 i 85 bitova, vrednost *FRR* parametra je 5.4% – 9.9%, a *FAR* parametra 3.2% – 2.5%.

Kod sistema baziranih na biometriji lica, slika lica se ne uzima iz baze, već se dobija preko kontinualnog video signala. Primenjen je metod biometrijskog zaključavanja, gde je ključ generisan sa entropijom od 80 bitova i *FRR* parametrom od 0.93%. Varijacije koje se javljaju u video signalu su manje nego u slikama iz baze, što je usporilo razvoj ove metode. Metoda „virtuelni PIN“ primenjuje Gabor filtar za ekstrakciju informacionih sadržaja i zaštitni kod za ispravljanje grešaka (engl. *Low Density Parity Check*).

Sistem baziran na biometriji lica, zasniva se na vezi biometrije i nezavisno generisanog ključa. Da bi se povećala tačnost algoritma, ekstraktuju se pouzdani i konzistentni bitovi informacija iz biometrijskih uzoraka i primenjuju *BCH* kodovi za ispravljanje grešaka. Biometrija lica sa *FRR* parametarom od 3.5% i *FAR* parametrom od 0% omogućila je generisanje kriptografskog ključa dužine 58 bitova i izbacivanje lozinki iz upotrebe. Ovaj algoritam je primenjen u Philips „ $privID^{TM}$ “ sistemu [6].

Pomoću jednosmerne funkcije, ekstraktuje se informacioni sadržaj iz biometrije glasa i elektrokardiograma i na taj način generiše kriptološki ključ po bimodalnom biometrijskom sistemu. Vrednost *FAR* parametra je 1.27%, a *FRR* parametra 10.62%.

Predložene tehnike generišu ključeve manjih dužina i imaju veliki *FRR* parametar. Dobre performance pokazlala je šema za generisanje ključeva na osnovu biometrije irisa, sa dužinom ključa od 140 bitova, *FRR* parametrom od 0.47% i *FAR* parametrom od 0%. Analizom grešaka u iris podatku, dobijeni su rezultati na osnovu kojih su izabrani zaštitni kodovi i izvršena je njihova optimizacija za maksimalno ispravljanje grešaka.

Ukoliko se primeni šema sa dva faktora (biometrija i token), ključ će zavisiti od njihove kombinacije. Napadač neće moći da regeneriše ključ ukoliko jedan od faktora bude kompromitovan. Takođe, postoji mogućnost da se lozinka doda kao treći faktor. Ova šema povezuje biometrijske podatake sa konvencionalnom kriptografijom.

Prvo se generiše biometrijski ključ kao slučajna binarna sekvenca, tačno određene dužine, a zatim se koduje se konkatentnim kodovima za ispravljenje grešaka. Ključ kodovan konkatentnim kodovima naziva se „pseudo kod“. U završnoj fazi kodovanja, dužina ključa biće 2048 bitova. Pomoću logičke operacije XOR, pseudo kod se vezuje za biometrijski podatak, a rezultat je pomoćni podatak, koji se smešta na token zajedno sa heš vrednošću ključa. Nakon upisa i generisanja biometrijskog ključa, ključ se uništava na siguran način. Korisnik daje originalnu biometriju i sa logičkom operacijom XOR otključava pseudo kod iz pomoćnog podatka. Faza

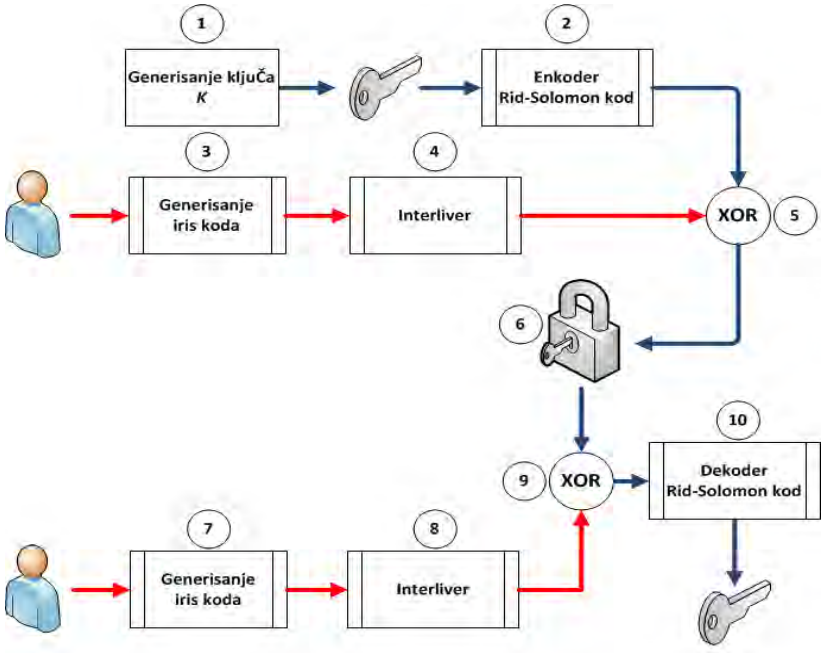
dekodovanja obavlja se sa istim konkatentnim kodovima za ispravljanje grešaka. Za rezultat uzima se heš vrednost, pomoću koje se utvrđuje sličnost sa heš vrednošću na tokenu.

Da bi se povećao kapacitet kodova za ispravljanje grešaka, uvode se redundantni bitovi (nule), sa uniformnom raspodelom, što povećava dužinu pseudo koda za 40%. Povećana je entropija biometrijskog obrasca, a dužina ključa dostigla je 186 bitova sa *FRR* parametrom od 0.76% i *FAR* parametrom od 0.096%. Ukoliko kriptološki ključ, smart kartica i lozinka budu kompromitovani, pseudo kod neće otkriti biometrijsku informaciju.

3.15. Primena zaštitnog koda i interlivera nad biometrijom

Biometrijski podaci su osnova za sintezu veoma kvalitetnog sistema za ekstrakciju kriptoloških ključeva. Segmente u biometriji irisa, najpogodnije za proces generisanja kriptoloških ključeva, moguće je pronaći uvođenjem informacionih mera, entropije, lokalne entropije i uzajamne informacije. Osnove sistema za ekstrakciju slučajnih nizova iz biometrije irisa date su optimizacijom parametara odgovarajuće jednosmerne funkcije. Zbog postojanja šuma u biometrijskim podacima, biometrija iz istog izvora nije uvek identična, pa treba osmisliti šemu tolerancije. Široko je primenjena tehnika za obradu signala, jer se biometrijski izvor i podaci mogu posmatrati kao komunikacioni kanal sa šumom.

Sistem, koji se sastoji od podsistema za kodovanje biometrijskog izvora (zasnovan na algoritmu tradicionalnih biometrijskih sistema) i podsistema za prenos poruka preko biometrijskog kanala sa šumom, predstavljen je na slici 3.15.1.



Slika 3.15.1: Generička šema primene zaštitnog koda i interlivera nad biometrijom

U početnoj fazi generiše se slučajni kriptološki ključ, zadate veličine. Zatim se vrši proces zaštitnog kodovanja za korekciju grešaka primenom Rid-Solomon koda, tj. kriptološki ključ se koduje primenom Rid-Solomon kodera. Nakon toga se generiše iris kod, koji pripada podsistemu za kodovanje biometrijskog izvora. Ovaj proces u sebi sadrži dva podprocesa.

Prvi podproces odnosi se na standardnu proceduru za generisanje biometrijskog obrasca. Drugi podproces uvodi informacione mere, na osnovu rezultata dobijenih pomoću analiza i koduje informacioni izvor sa ciljem izdvajanja najkonzistentnijih informacija. Performanse sistema zavisiće od kvaliteta procesa kodovanja iris informacionog izvora.

Zatim se primenjuje interliver, koji se koristi za raspršivanje paketskih grešaka i smanjenje uzajamnih informacija između različitih irisa. U ovom slučaju, primenjuje se tehnika slučajnog interlivinga (engl. *Random interliver*). Pomoću logičke operacije XOR, u kojoj se bodovan kriptološki ključ, čvrsto vezuje za originalni iris kod nad kojim je primenjena tehnika za interliving. Rezultat XOR operacije u sebi čuva zaključanu originalnu biometriju i slučajno generisani ključ. Na osnovu ovog podatka nije moguće otkriti originalnu biometriju ili ključ.

Korisnik sada želi da, na osnovu originalne biometrije, regeneriše ključ. Ovaj proces identičan je procesu generisanja iris koda i interlivinga sa početka. Nad kodovanim iris kodom i podatkom koji u sebi čuva ključ primenjuje se logička operacija XOR, i na taj način se regeneriše zaključani ključ. Zatim se, pomoću Rid-Solomon dekodera, koriguju sve greške koje su nastale. Ukoliko je, dobijeni rezultat, jednak generisanom ključu iz početne faze, onda je procedura realizovana uspešno.

Kod ovog sistema moguće su dve vrste grešaka. Prva vrsta su slučajne greške, nastale od *CCD* senzora kamere ili distorzije irisa, uzrokovane promenom osvetljenja. Druga vrsta grešaka nastaje zbog refleksije i loše detekcije kapaka i trepavica. Za ispravljanje prve vrste grešaka koriste se Hadamardovi kodovi, a za drugu Rid-Solomon kodovi. Kao spoljašnji sloj, koriste se Hadamardovi kodovi za ispravljanje slučajnih grešaka u binarnom podatku irisa, a za unutrašnji sloj Rid-Solomon kodovi za ispravljanje paketskih grešaka na blokovskom nivou [5].

Drugi predloženi sistem zasniva se na biometrijskom uzorku, lozinki ili PIN-u i smart kartici. Korisnik sistema prilaže smart karticu, koja sadrži pseudokod i heš vrednost od zaključanog ključa u pseudokodu. Nakon unosa ispravne korisničke lozinke, podaci sa smart kartice se prosleđuju sistemu za regenerisanje ključa. Pomoću senzora očitava se korisnikova originalna biometrija. Nakon toga se primenjuje sistem za generisanje biometrijskog obrasca, koji se zatim prosleđuje sistemu za regenerisanje ključa. Ukoliko je dobijena heš vrednost identična kao sa smart kartice, kao rezultat ćemo dobiti biometrijski ključ.

Ovaj sistem omogućava proveru identiteta i generisanje ključeva u *offline* režimu rada. Na ovaj način se izbegava centralizovana baza podataka. Dobijeni ključevi mogu se koristiti u kriptografske svrhe i kod sistema za bezbednu autentifikaciju korisnika na bazi heš vrednosti ključa.

Problem varijabilnosti u biometriji, možemo rešiti primenom zaštitnih kodova za ispravljanje grešaka (engl. *Error correcting code*) i interlivera. Interliver tehnika se koristi kod klasičnih komunikacionih kanala za podizanje performansi zaštitnih kodova ili kodova za ispravljanje grešaka. Primenom ovih tehnika, biometrija postaje ekvivalentna sa klasičnim komunikacionim kanalima. Kanal, koji ima zajedničke osobine i koji je ekvivalentan sa biometrijskim komunikacionim kanalom, doprinosi poboljšanju performansi celokupnog sistema. Cilj je projektovati biometrijski komunikacioni kanal preko koga bi se preneo ključ, a da pritom dva irisa utiču na njega. Biometrijski kanal indukovan sa dva iris koda, sa istog biometrijskog izvora, može da prenese ključ bez greške. U zavisnosti od toga da li dva irisa pripadaju istoj osobi ili ne, vrednost grešaka će varirati. Dekoder za ispravljanje grešaka mora da razlikuje originalnog korisnika od lažnog.

4. DIGITALNI VODENI PEČATI

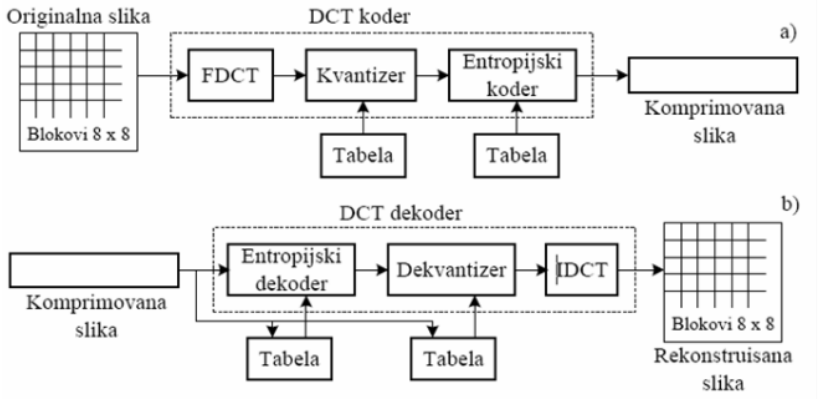
4.1. Kompresija slike

Postoje dve vrste kompresije:

1. **Kompresija bez gubitaka** (engl. *Lossless compression*) smanjuje originalnu veličinu slike primenom različitih algoritama, nakon čega je moguće takvu sliku dekompresovati i vratiti u originalno stanje. Međutim, ova kompresija ne smanjenje značajno broj bitova, te se kvalitet slike neće bitno smanjiti. Zasniva se na statistici podataka i ima veliku primenu u medicini za kompresiju različitih snimaka, kao i za kompresiju multimedijalnih podataka. Kompresija bez gubitaka ima ograničene mogućnosti, pa se češće koristi kompresija sa gubicima. Stepen kompresije je ograničen i iznosi od 1:2 do 1:8.
2. **Kompresija sa gubicima** (engl. *Lossy compression*) smanjuje originalnu veličinu slike na račun kvaliteta, čime se postiže ušteda u prostoru. Ona odbacuje vizuelno manje važne informacije i mnogo intenzivnije komprimuje podatke. Stepen kompresije iznosi od 2 do 100. Rekonstruisana slika ima oštećenja u odnosu na original, ali ona nisu primetna pod normalnim uslovima gledanja. Takvu sliku je nemoguće vratiti u originalno stanje jer su neki njeni delovi trajno uklonjeni. Koristi se kod audio i video zapisa, skeniranih slika i računarske grafike. Metode kompresije sa gubicima mogu se podeliti u sledeće grupe: Chroma subsampling, Transform coding, redukovanje prostora boja i kompresija fraktalima. Često se, u praksi, neke od ovih metoda kombinuju. Predstavnik kompresije sa gubicima je JPEG kompresija, koja obuhvata dve metode: Chroma subsampling i Transform coding.

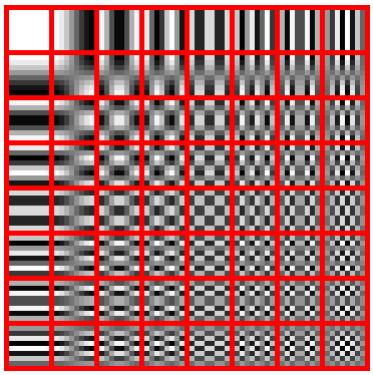
4.2. JPEG kompresija

JPEG (engl. *Joint Photographic Experts Group*) je najraširenij format zapisa slika, ali i vrsta napada na digitalne vodene pečate. Ovaj format najbolje komprimuje fotografije u punoj boji, gde može da prikaže svih 16,7 miliona boja. Zbog toga je JPEG format najpopularniji za prikazivanje realističkih slika, a slabije se pokazao kod slika u nijansama sive i kod jednostavnih crteža sa oštrim ivicama. Ukoliko podatke, pre ubacivanja u sliku, kompresujemo i smanjimo njihovu veličinu, povećaćemo prostor za skladištenje unutar slike. Na slici 4.2.1 je data blok šema JPEG sistema za kompresiju slike.



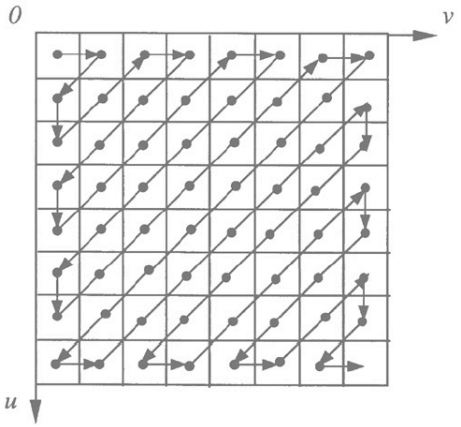
Slika 4.2.1: Blok šema JPEG sistema za kompresiju slike: (a) koder, (b) dekoder [16]

Svaka komponenta slike (Y, Cb, Cr) deli se u blokove od po 8×8 piksela. Zatim se svaki blok konvertuje u prostor frekvencije koristeći dvodimenzionu DCT transformaciju (Slika 4.2.2). Cilj je pronaći blok gde bi promena vrednosti piksela bila najmanja. Ako je vrednost prevelika, blok se deli na 8x8 podblokova, sve dok vrednost ne bude dovoljno niska. Ako dimenzije slike nisu multipli broja 8, onda se nekompletni blokovi (u desnom, donjem delu slike) prethodno dopunjavaju „lažnim" podacima (crnim pikselima ili ponavljanjam piksela sa ivice slike). Svaki 8x8 blok, ili podblok, je transformisan u 64 DCT koeficijenta koji su približni osvetljenju (svetlosti, tami i kontrastu) i signalu boje tog dela slike.



Slika 4.2.2: Osnovni talasni oblici 8x8 DCT transformacije

Kvantizovane komponente slike uređuju se u cik-cak redosled (Slika 4.2.3), čime se dodatno grupišu slične frekvencije i povećavaju dužine sekvenci nula, a zatim se koristi Hafmenovo kodiranje tako uređenog niza. JPEG standard dozvoljava i korišćenje aritmetičkog kodiranja umesto Hafmenovog. Aritmetičko kodiranje je matematički superiornije od Hafmenovog, ali se retko koristi zato što je pokriveno patentima, kodiranje i dekodiranje su dosta sporiji, a fajlovi su nešto manji (za oko 5%) [17].



Slika 4.2.3: Cik-cak očitavanje DCT koeficijenata

Kompresija 10:1 obično rezultuje u slici koju ljudsko oko ne može da razlikuje od originala, dok će kompresija od 100:1, imati uočljive blokovske artifakte. Zbog toga se JPEG smatra lošim formatom za komprimovanje. Obnovljena slika iz kompresije nije identična originalnoj slici, oštećenja su trajna, a gubici se akumuliraju prilikom višestrukog uređivanja slike.

Standard JPEG 2000 bazira se na primeni Diskretne talasne transformacije (DWT), gde se slika razlaže u tri slike u nijansama sive, koje se zatim zasebno komprimuju. Svaka slika se deli u pločice iste veličine, koje se zatim transformišu primenom DWT do proizvoljne dubine i kodiraju zasebno. Moguće je celu sliku tretirati kao jedinstvenu pločicu. JPEG 2000 primenjuje dve različite transformacije talasima: CDF 9/7 transformacija, koja uvodi kvantizacioni šum, i CDF 5/3 transformacija, koja koristi samo celobrojne koeficijente (korak kvantizacije je 1) [18].

JPEG 2000 omogućuje bolji kvalitet slike i veću fleksibilnost pri vrlo niskim brzinama prenosa, pa se primenjuje u oblastima u kojima JPEG nije dao zadovoljavajuće rezultate [19].

4.3. Transformacija slike

Najvažniji deo kompresije sa gubicima je transformacija, kod koje se podaci slike preslikavaju iz prostornog u frekventni domen, a da se pritom energija slike sačuva.

Raspodela energije je veoma važna kod kompresije slike. Poželjno je koristiti transformaciju koja raspodeljuje maksimalnu količinu energije u što manji broj koeficijenata. Kod ortogonalnih transformacija veliki deo srednje energije se raspodeljuje u svega nekoliko koeficijenata, dok ostali koeficijenti sadrže mali deo energije. Kod frekventnog domena energija je skoncentrisana na sasvim malom broju koeficijenata.

Postoje sledeće transformacije:

- Diskretna unitarna transformacija,
- Diskretna Furijeova transformacija (**DFT**),
- Diskretna kosinusna transformacija (**DCT**),
- Diskretna sinusna transformacija (**DST**),
- Diskretna talasna transformacija (**DWT**),
- Diskretna Hartlijeva transformacija (**DHT**),
- Diskretna Volš-Adamarova transformacija (**WHT**),
- Diskretna Harova transformacija,
- Diskretna slant transformacija i
- KL (optimalna) transformacija (**KLT**).

Najpoznatija transformacija je DFT. DCT, DFT i WHT, koriste matricu transformacije koja zavisi od dimenzija slike, ali ne i od same slike. Ipak, najbolje rezultate u kompresiji daje KLT, ali je ujedno i najkomplikovanija za korišćenje, jer zahteva da se matrica transformacije računa za svaku sliku posebno. Od svih navedenih transformacija, DCT je najsličnija KLT.

4.3.1. Diskretna Furijeova transformacija

Diskretna Furijeova transformacija je često korišćena u algoritmima za digitalnu obradu signala. Njene modifikacije su primenjene kod JPEG kompresije slike, kao i u drugim oblastima vezanim za analizu diskretnih signala.

Ova transformacija je robustna protiv geometrijskih napada, kao što su rotacija, skaliranje, odrezivanje, translacija itd. Takođe, se može koristiti za oporavak od geometrijske distorzije. Nedostaci ove transformacije su kompleksna implementacija i visoka cena.

4.3.2. Diskretna kosinusna transformacija

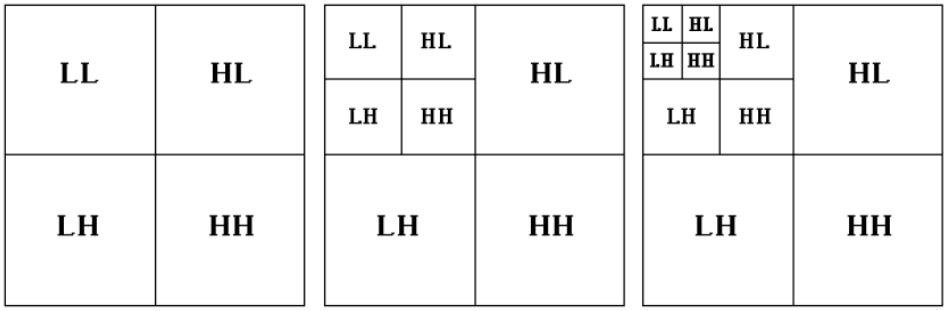
Diskretna kosinusna transformacija je nastala iz Furijeove treansformacije. DCT ne vrši kompresiju, već pretvara vrednosti elemenata slike u koeficijente koji se dalje mogu lakše podvrgnuti postupku kompresije. Ova transformacija razlaže diskretni siganl na sinusoidalne komponete različitih učetanosti.

Ovi algoritmi su otporni na jednostavne obrade slike, kao što je niskofrekventno filtriranje, podešavanje osvetljenosti, kontrasta i zamućenosti. Istovremeno, slabi su na geometrijske napade kao što su rotacija, skaliranje i odrezivanje. Utiskivanje vodenog pečata u koeficijente srednje frekvencije neće uticati na vidljivost slike i ne može biti uklonjen bilo kakvim napadom, dok će neke više komponente frekvencija biti potisnute u koraku kvantizacije.

4.3.3. Diskretna talasna transformacija

DWT transformacija zasniva se na malim talasima (talasićima) promenljive frekvencije i ograničenog trajanja. Ova transformacija razlaže sliku na tri prostorna pravca: horizontalni, vertikalni i dijagonalni.

Primenom DWT transformacije na sliku, ista će se podeliti na 4 jednaka kvadrata. LL opseg sadrži aproksimacije, dok horizontalna (HL), vertikalna (LH) i dijagonalna komponenta (HH) sadrže detalje. Ukoliko se, na svaki red podataka, primeni niskopropustni i visokopropustni filtar, dobiće se podaci gde će prva polovina reda sadržati niske, a druga polovina visoke frekvencije [3]. Nakon toga se primenjuje filtriranje za svaku kolonu međupodataka. Magnituda DWT koeficijenata veća je na nižim opsezima (LL), na svakom nivou razlaganja, a manja na drugim opsezima (HH, LH i HL). Proces možemo ponoviti tako da se talasna dekompozicija računa u više nivoa (Slika 4.3.3.1).



Slika 4.3.3.1 Piramidalno razlaganje talasa na jedan, dva i tri nivoa

DWT je pogodna za analizu kratkotrajnih promeljivih signala, pa zbog svojih naglih promena zahteva širok spektar frekvencija, kao i DCT. Često se primenjuje u aplikacijama za obradu signala kao što je digitalna obrada slike, audio i video kompresija, uklanjanje šuma kod zvuka, simulacija bezičnog prenosa, ali i u vodenom pečatiranju.

Noviji grafički formati (PDF i DjVu), u kompresiji, uglavnom koriste DWT. Razlog za to je što DWT ima viši odnos kompresije u odnosu na JPEG, što odgovara ljudskoj percepciji. Takođe, ova transformacija omogućuje istovremeno lociranje u prostoru, i frekventno raspršen vodeni pečat u originalnoj slici, što je čini veoma pogodnom. Nedostatak ove tehnike je duže vreme kompresije, šum, zamućenost na ivicama slika ili video ramova i visoka cena.

4.4. Klasifikacija digitalnih vodenih pečata

Klasifikacija digitalnih vodenih pečata može se izvršiti po domenu, tipu, moći opažanja, robustnosti, upotrebi ključeva, procesu detekcije i prema nameni [20].

Podela prema domenu:

- **Prostorni domen** (engl. *Spatial domain*) je usresređen na modifikovanje piksela, jednog ili dva slučajno izabrana podskupa slika, tako što neobrađeni podatak direktno smešta u piksele slike. U ovom domenu utiskivanje vodenog pečata može se realizovati samo u jednoj boji iz palate boja. Na ovaj način pečat postaje teško vidljiv običnim gledanjem. Neki od ovih algoritama su LSB, algoritam zasnovan na tehnici SSM modulacije, aditivni vodeni pečat, tehnika kodovanja teksturne mape, Pačvork algoritam i tehnika na bazi korelacije.
- **Frekventni domen** (engl. *Frequency domain*) ili transformacioni domen ima širu primenu. Karakteristike ljudskog vizuelog sistema bolje zapažaju spektralne koeficijente, što je i razlog utiskivanja vodenog pečata u spektralne koeficijente slike u ovom domenu. Najčešće primenjivane transformacije su Diskretna Furijeova transformacija (DFT), Diskretna kosinusna transformacija (DCT) i Diskretna talasna transformacija (DWT).

Tabela 4.4.1: Poređenje prostornog i frekventnog domena

Faktori	**Prostorni domen**	**Frekventni domen**
Cena troškova	Niska	Visoka
Robustnost	Lomljiv	Više robustan
Kvalitet percepcije	Visoka kontrola	Niska kontrola
Kompleksnost	Mala	Velika
Vreme obračuna	Kraće	Duže
Kapacitet	Veliki	Mali
Primer primene	Autentifikacija	Zaštita autorskih parava

Izvor: Prabhishek Singh, R. S. Chadha (2013), International Journal of Engineering and Innovative Technology (IJEIT), Volume 2, Issue 9, str. 166

Vodeni pečati se mogu, prema tipu, podeliti zavisno od vrste šuma (pseudo šum, Gausove slučajne i haotične sekvence) i zavisno od vrste slike (binarne slike, žigove, logo i etikete).

Podela prema moći opažanja:

- **Vidljivi vodeni pečati** (engl. *Visible watermarking*) – jasno i primetno identifikuju vlasnika, a pritom ne utiču na sadržaj same slike. Primenjuje se za naprednu zaštitu od kopiranja i zaštitu autorskih prava.
- **Nevidljivi vodeni pečati** (engl. *Invisible watermarking*) – pri normalnim uslovima gledanja posmatraču su nevidljivi. Međutim, na ovaj način se ne moze zaštititi slika od krađe, ali se može dokazati da je slika ukradena, što je dobro.
- **Dvostruki vodeni pečati** (engl. *Dual watermarking*) – predstavljaju kombinaciju vidljivog i nevidljivog vodenog pečata.

Podela prema robustnosti:

- **Robusni nevidljivi vodeni pečati** (engl. *Robustness watermarking*) – vizuelno su nevidljivi i otporni na različite vrste napada. Primenjuju se za detekciju nelegalnih dokumenata i za evidentiranje autorskog prava.
- **Lomljivi nevidljivi vodeni pečati** (engl. *Fragile watermarking*) – vizuelno su nevidljivi. Na osnovu stanja pečata možemo zaključiti da li je došlo do neovlašćenog pristupa podacima. Uglavnom se primenjuju za zaštitu integriteta, pouzdane (sigurne) kamere, kao i za detekciju promene slike u digitalnoj biblioteci.
- **Polu lomljivi vodeni pečati** (engl. *Semi fragile watermarking*) – mogu da tolerišu promene na slici sa vodenim pečatom do izvesnog stepena (npr. kvantizacioni šum koji se pojavljuje kod kompresije sa gubicima).

Podela prema upotrebi ključeva:

- **Asimetrični vodeni pečati** (engl. *Asymmetric watermarking*) – za utiskivanje i detekciju koriste različite ključeve.
- **Simetrični vodeni pečati** (engl. *Symmetric watermarking*) – za utiskivanje i detekciju koriste iste ključeve.

Podela prema procesu detekcije:

- **Vizuelni vodeni pečati** (engl. *Visual watermarking*) – imaju veliku robusnost i zahtevaju originalni podatak pri testiranju. Primena im je ograničena.
- **Polu slepi vodeni pečati** (engl. *Semi blind watermarking*) – ne zahtevaju originalni podatak za detekciju.
- **Slepi vodeni pečati** (engl. *Blind watermarking*) – zasnovani su na savremenoj tehnologiji i ne zahtevaju originalni podatak. Imaju široko aplikaciono polje.

Podela prema nameni:

- **Vodeni pečati za zaštitu autorskih prava** (engl. *Copyright protection watermarking*) **–** vlasnik pridodaje vodeni pečat u sliku, tako da pečat bude vidljiv.
- **Vodeni pečat koji obaveštava o promeni** (engl. *Tampering tip watermarking*) **–** štiti integritet sadržaja slike, označava promenjeni sadržaj i pruža otpornost kompresiji sa gubitkom.
- **Vodeni pečat protiv falsifikovanja** (engl. *Anti-counterfeiting watermarking*) **–** dodaje se prilikom procesa izgradnje beleški, može se detektovati nakon štampanja, skeniranja ili nekih drugih procesa.
- **Anonimna oznaka vodenog pečata** (engl. *Anonymous mark watermarking*) **–** sakriva važne pribeleške poverljivih podataka i ograničava nelegalne korisnike da dođu do istih.

4.5. Primena digitalnih vodenih pečata

Digitalni vodeni pečat se primenjuje za identifikaciju i zaštitu autorskog prava (engl. *Copyright protection*), pa tako, digitalni sadržaj koji je utisnut sa vodenim pečatom, identifikuje vlasnika autorskog prava.

Kod zaštite od kopiranja (engl. *Copy protection*), digitalni sadržaj sa vodenim pečatom treba da ukaže da ne može biti ilegalno kopiran. Ukoliko dođe do neautorizovanog kopiranja sadržaja, sredstva za kopiranje će detektovati vodeni pečat i sprečiti kopiranje.

Digitalni vodeni pečati koji su po prirodi lomljivi, mogu se koristiti za proveru neovlašćenog pristupa (engl. *Tamper proofing*) i potvrdu autentičnosti sadržaja. Digitalni sadržaj može biti utisnut sa lomljivim vodenim pečatom koji će biti uništen uvek kada se napravi bilo kakva vrsta modifikacije sadržaja.

Kod autentifikacije izgleda i sadržaja (engl. *Image and content authentication*) detektuju se promene na podacima. Karakteristike slike utisnute su u važeću sliku, pa se poređenjem lako može otkriti razlika. Rešenje ovog problema možemo pronaći u kriptografiji, gde se digitalni potpis primenjuje za autentifikaciju slike kod verodostojne digitalne kamere.

Upravljanje digitalnim pravima (engl. *Digital right management*, DRM) predstavlja opis, identifikaciju, trgovinu, zaštitu, monitoring i praćenje svih formi korišćenja materijalne i nematerijalne svojine.

U nekim sistemima, poželjno je da korisnici imaju kopiju i pristup kontrolnom mehanizmu za zaštitu od ilegalnog kopiranja sadržaja ili ograničenje broja kopiranja (engl. *Access control*). Robustni vodeni pečati se mogu primeniti u ove svrhe.

U aplikaciji za zaštitu autorskih prava, otisak prsta (engl. *Fingerprinting*) se koristi kao vodeni pečat da prati autorizovane korisnike koji krše licencne ugovore i nezakonito distribuiraju kopirani materijal. Korisnikov identifikacioni broj biće utisnut u sadržaj.

Forenzička aplikacija (engl. *Media forensics*) vodenog pečata omogućava vlasniku sadržaja da detektuje i reaguje na zloupotrebu. Forenzički vodeni pečat se koristi da bi se sakupili dokazi za krivični postupak, kao i kod ugovora između vlasnika sadržaja i kompanija ili ljudi koji dele taj sadržaj.

Primenom vidljivog vodenog pečata u medicini (engl. *Medical application*), imena pacijenata se štampaju na rendgenskim snimcima i snimcima magnetne rezonance. Takođe, vodeni pečat se može koristiti za pribeleške na slici, pa se tako, evidencija pacijenta i detalji vazani za snimak mogu umetnuti u sliku, što će smanjiti prostor za smeštanje i omogućiti povezanost slike i pribeleške. Pod uslovom da se osetljive informacije ne čuvaju kao jasan tekst u čitljivoj formi, a vodeni pečat se dodatno osigura šifrovanjem, privatnost pacijenta biće sačuvana (engl. *Annotation and privacy control*).

S obzirom da se poslednjih nekoliko godina broj televizijskih i radio kanala znatno povećao, a sa tim i količina protoka sadržaja, nadgledanje ovog tržišta veoma je važno za vlasnike svojine, imaoce vlasničkih prava, distributere i emitere (engl. *Broadcast monitoring*).

Digitalni formati namenjeni za prodaju ili iznamljivanje audio i video sadržaja potrošačima (DVD, Blu-Ray Disc i iTunes), objedinjuju tehnologije za zaštitu sadržaja, kontrolišu pristup, upotrebu sadržaja, ograničavaju neautorizovano kopiranje i ponovnu distribuciju (engl. *Content protection for audio and video content*).

4.6. Algoritmi za označavanje i detekciju digitalnih vodenih pečata

Digitalni vodeni pečat se može dodati u bilo koji digitalni dokument pomoću algoritma za kodiranje, dok se primenom algoritma za dekodiranje pečat vadi iz označenog dokumenta i jednoznačno se određuje vlasnik i integritet dokumenta [21]. Otkrivanje prisutnosti vodenog pečata u slici vrši se upoređivanjem originalne (neoznačene) i označene slike.

Algoritmi koji služe za označavanje digitalnog dokumenta, mogu se podeliti prema [22]:

- Domenu u kojem se obavlja utiskivanje i detekcija pečata,
- Dostupnosti referentnih podataka za detekciju pečata,
- Metodi modifikacije slike,
- Strategiji perceptualnog modeliranja,
- Nameni.

4.7. Savremena steganografija

Steganografija je tehnika koja skriva tajne poruke unutar računarskih fajlova, teksta, slika i filmova, na takav način da niko osim predajne i prijemne strane to ne primeti. Savremena steganografija podrazumeva skup sredstava i metoda za formiranje skrivenog kanala prenosa informacija [23].

Pošiljalac tajne poruke nasumično bira nosioca, koji ima za zadatak da prenese skrivenu poruku. Da bi se tajna poruka učinila nevidljivom, nosilac poruke mora da sadrži dovoljno redundantnih bitova koji će biti zamenjeni tajnom porukom. U izabrani nosilac poruke ugrađuje se tajna poruka pomoću steganografskog ključa (steganografski sistem može imati jedan ili više steganografskih ključeva). Nosilac i skrivena poruka čine steganografski medijum, koji se zatim šalje komunikacionim (steganografskim) kanalom do primaoca poruke. Primalac poruke prima steganografski medijum i obrnutim postupkom dolazi do sadržaja tajne poruke.

Velika količina informacija u digitalnim audio i video signalima, uticala je na razvoj kompjuterske steganografije, koja se bavi realizacijom steganografskog sistema primenom kompjuterske tehnike u cilju zaštite informacija.

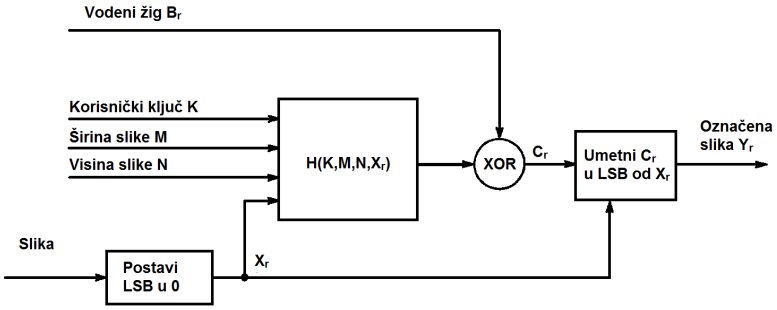
Postoji puno programa za skrivanje informacija, koji primenjuju različite steganografske tehnike. Savremene metode kompjuterske steganografije koriste posebne kompjuterske formate za prenošenje tajnih poruka. Međutim, specijalna svojstva ovih formata sve manje se koriste kao metod za realizaciju kompjuterske steganografije, a sve više kao metod napada. Postoji više programa za stegoanalizu čiji je zadatak prepoznavanje steganografije u komunikaciji i uništavanje poruke [4].

4.8. LSB supstitucija

Jedna od najčešće korišćenih steganografskih tehnika je LSB supstitucija (engl. *Least Significant Bit*), koja iz izabrane datoteke uzima bitove sa najmanjim značenjem i zamenjuje ih sa bitovima tajne poruke. Zamena bitova sa najmanjim značenjem sa tajnom porukom, neće značajno uticati na kvalitet reprodukovane slike, jer ovi bitovi sadrže malo korisnih informacija.

Ima veoma dobre performanse kada se primenjuje na slikama, jer malo kvari kvalitet slike i ima veliku transparentnost. Lako se primenjuje na slike velike rezolucije sa mnogo detalja. Moguće je sakriti veliku količinu informacija uz minimalni uticaj na datoteku nosioca skrivene informacije. Zbog svoje jednostavnosti, ova metoda je pogodna i za dešifrovanje tajne poruke.

Ova tehnika se može primeniti na sledeći način: prema tabeli za konverziju svakom znaku se dodeljuje određena kombinacija bitova ili se po poznatim pravilima selektuju pikseli u koje se skrivaju znakovi, koji takođe mogu zavisiti od korisničkog ključa [24]. Na slici 4.8.1 je prikazana blok šema utiskivanja digitalnog vodenog pečata primenom LSB supstitucije.

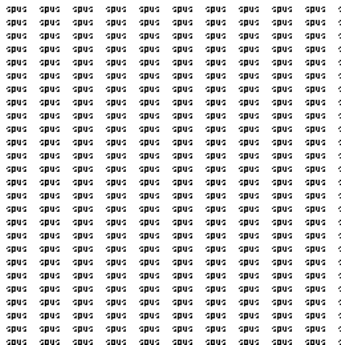


Slika 4.8.1: Blok šema utiskivanja vodenog pečata primenom LSB supstitucije

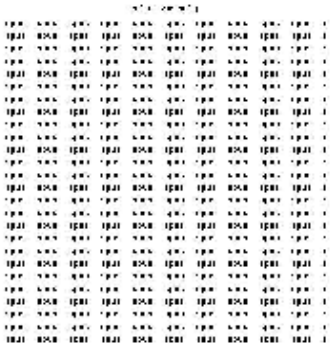
Ako vodeni pečat sakrijemo unutar slike, dobićemo novu sliku koja u sebi sadrži vodeni pečat (Slika 4.8.2 i 4.8.3). Rezutat je slika u kojoj nema vidljivih promena (Slika 4.8.5) i iz koje se pečat može lako izvući (Slika 4.8.4).



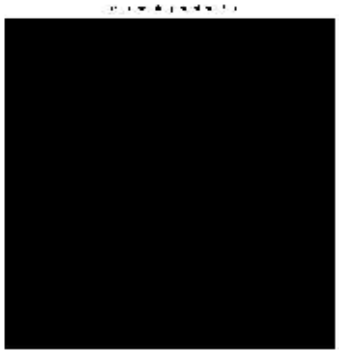
Slika 4.8.2: Originalna slika



Slika 4.8.3: Primer vodenog pečata



Slika 4.8.4: Pročitani vodeni pečat



Slika 4.8.5: Razlika između originalnog i pročitanog vodenog pečata

Najbolji i najkvalitetniji format za skrivanje informacija je 24-bitna BMP slika, kao najveći tip fajla. Danas, najveći broj aplikacija za digitalne slike podržava 24-bitne slike, gde je svaki piksel kodiran u 24 bita (3 Bajta). Međutim, slanje slika velikih dimenzija preko Interneta može izazvati sumnju, pa se zato mnogi opredeljuju za 8-bitni GIF ili BMP format slike. Tipična 8-bitna slika dimenzija 640x480 sa 256 nijansi boja omogućava da se skrije poruka od 300 KB, dok se u 24-bitnu sliku dimenzije 1024x768 može smestiti do 2.3 MB skrivene poruke. BMP i GIF se uzimaju jer obezbeđuju idealnu kompresiju tj. nakon kodiranja i kompresije obnovljena slika biće identična originalnoj slici.

Iako se odlikuje velikim kapacitetom za skrivanje poruka i ugrađivanje vodenog pečata, ova metoda ipak ne pruža veliku sigurnost. Vodeni pečat koji je nastao LSB supstitucijom, nije otporan na većinu napada (podložan je šumu, odrezivanju i skaliranju), što ga svrstava u kategoriju lomljivih pečata. Postavljanje svih LSB bitova na jedinicu predstavlja najbolji napad na vodeni pečat, dok slika ostaje nepromenjena.

4.8.1. Skrivanje tajne slike unutar slike

Slika u slici je vrsta LSB supstitucije. Za slanje grube aproksimacije tajne slike, dovoljna su tri bita. Pri slanju tajne slike (Slika 4.8.1.2), tri bita najmanje težine originalne slike (Slika 4.8.1.1) zameniće se sa tri bita najveće težine tajne slike. Kao rezutat dobijamo sliku u kojoj degradacija nije vizuelno uočljiva (Slika 4.8.1.3). Primalac izvlači tri bita najmanje težine iz primljene slike, te tako dobija pristup do tri najznačajnija bita tajne slike (Slika 4.8.1.4) [17].



Slika 4.8.1.1: Originalna slika



Slika 4.8.1.2: Tajna slika



Slika 4.8.1.3: Slika – kombinacija



Slika 4.8.1.4: Slika dobijena od tri bit ravni najmanje težine slike 4.8.1.3

4.8.2. Skrivanje tajnih poruka unutar slike

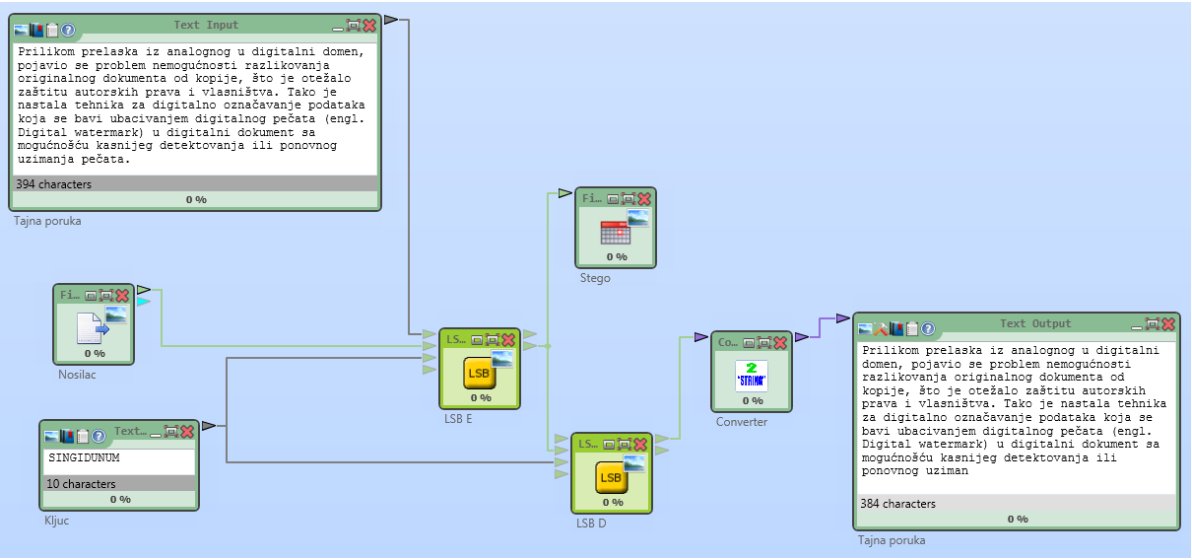
Primenom LSB supstitucije možemo sakriti tekst unutar slike. Pomoću ključa, pošiljalac utiskuje tajnu poruku u nosilac poruke tj. u sliku 4.8.2.1. Ključ je tajni i poznat je samo pošiljaocu i primaocu tajne poruke. Rezultat je steganografski medijum koji sadrži u sebi tajnu poruku (Slika 4.8.2.2). Nakon dekodovanja steganografskog medijuma, primalac uspešno izdvaja tajnu poruku (Slika 4.8.2.3) [25].



Slika 4.8.2.1: Nosilac poruke



Slika 4.8.2.2: Steganografski medijum



Slika 4.8.2.3: Šema skrivanja tajne poruke unutar slike primenom LSB supstitucije

Na steganografskom medijumu nema vidljivih promena, te napadač ne može da posumnja da postoji tajna poruka unutar slike. Međutim, sa modifikacijom steganografskog medijuma, menjaju se i njegova statistička svojstva, pa napadač može da otkrije postojanje tajne poruke unutar slike, ali ne može da je pročita. Iako može da poznaje steganografski medijum, model šifarskog sitema ili algoritam po kojem je vršeno šifrovanje, napadač nije u stanju da otkrije tajnu poruku koja se prenosi ukoliko nema ključ.

4.9. Tehnika kodovanja proširenim spektrom

Tehnika kodovanja proširenim spektrom (engl. *Spread Spectrum Modulation Based Technique*) je metoda u kojoj se energija generisana u jednu ili više diskretnih frekvencija namerno proširi ili rasporedi u vremenu. Vodeni pečati, bazirani na SSM algoritmu, utiskuju informaciju linearnim kombinovanjem originalne slike sa malim signalom pseudo šuma koji je modulisan sa utisnutim vodenim pečatom.

Kako bi obrada bila što kvalitetnija, na sam spektar se primenjuje neka od transformacija: DCT, FFT, DWT ili WHT. Zatim se bira jedan skup spektralnih koeficijenata dobijen takvom transformacijom. Povećanje koeficijenta za neku vrednost, znači da u njega sakrivamo vrednost 1, dok smanjenje znači vrednost 0. Spektralni koeficijenti biraju se tako da pečat bude „raspršen" po celom frekventnom spektru slike, a energija pečata neprimetna u svakoj odabranoj frekvenciji, bez vidljivih promena na slici. Pri obradi slike, filtriranje visokih frekvencija može ukloniti pečat zajedno sa ostalim sadržajem u tom području, ali ne i u području niskih frekvencija.

Sliku možemo zamisliti kao komunikacioni kanal kojim prenosimo signal (u našem slučaju pečat). Eventualno sužavanje frekventnog opsega ne sme uništiti signal, a koeficijenti, pod uticajem šuma, ne smeju izmeniti značenje.

S obzirom da su frekventna područja za dodavanje signala pečata dobro poznata, da bi detekcija bila što teža, moguće je povećati odnos signal/šum dodavanjem skupa slabijih signala. Pečat se pri dodavanju na sliku postavlja tamo gde će njegovo uklanjanje značajno degradirati kvalitet slike.

4.10. Ostali poznati algoritmi

Aditivni vodeni pečat (engl. *Additive watermarking*) – Ova najdirektnija metoda za utiskivanje vodenog pečata u prostornom domenu sastoji se u dodavanju uzorka slučajnog pseudo šuma intenzitetu piksela slike. Signal šuma je obično intedžer (-1,0,1) ili decimalni broj. Da bi obezbedili detekciju vodenog pečata, šum treba da se generiše po ključu, tako da korelacija između brojeva različitog ključa bude veoma mala [20].

Tehnika kodovanja teksturne mape (engl. *Texture Mapping Coding Technique*) – Krije vodeni pečat u kontinualnoj slučajnoj teksturnoj šari slike. Ovaj algoritam je pogodan samo za oblasti sa velikim brojem slučajnih teksturnih slika i ne može biti urađen automatski.

Pačvork algoritam (engl. *Patchwork Algorithm*) **–** Ova tehnika skrivanja podataka bazira se na slučajnom pseudo statističkom modelu. Neprimetno ubacuje vodeni pečat koristeći posebnu statistiku Gausove raspodele. Pseudo slučajna selekcija se izvršava na dva parčeta, gde je prvo A i drugo B. Podatak u delu slike A je posvetljen, a u delu slike B je potamnjen. Prednost ove tehnike je visok nivo robustnosti protiv većine napada, a nedostatak što može da sakrije malu količinu informacija.

Cox-ov algoritam – Najpoznatiji algoritam koji primenjuje DCT transformaciju. Kao digitalni vodeni pečat uzima se Gausov niz od 1000 pseudo-slučajnih brojeva koji se zatim sabiraju sa 1000 najvećih koeficijenata DCT-a. Ukoliko se uporede vodeni pečat izvučen iz označene slike i utisnuti pečat, dobija se faktor sličnosti između originalne slike i slike sa digitalnim pečatom

(Hamingovo rastojanje) od 0.999999. Ovaj algoritam je efikasan za teksturne slike sa što manje jednako svetlih površina [21].

Algoritam Corvi – Digitalni vodeni pečat je Gausov niz pseudo-slučajnih realnih brojeva dužine 32x32 (ukupno 1024 realna broja). Algoritam Corvi originalnu sliku prebacuje u DWT, i samo se niskofrekventni koeficijenti sabiraju sa pečatom. Ukoliko se uporede vodeni pečat izvučen iz označene slike i utisnuti pečat, dobija se Hamingovo rastojanje od 0.950000. Za razliku od Cox-ovog algoritama, Corvi algoritam je efikasan za slike sa što manje tekstura.

Algoritam Xia – Primenjuje DWT transformaciju. Kao digitalni vodeni pečat koristi se Gausov niz pseudo-slučajnih realnih brojeva. Preporučuje se prelaz u DWT, razlaganjem na dva nivoa uz upotrebu Harovog filtra. Digitalni vodeni pečat se utiskuje u velike koeficijente visokih i srednjih frekventnih pojaseva (detaljnih podpojaseva). Ovim algoritmom se najviše energije vodenog pečata smešta u područja ivica i tekstura, jer veliki koeficijenti u detaljnim podpojasevima najčešće predstavljaju ivice. Tako je postignuta dobra nevidljivost utisnutog pečata, jer ljudsko oko manje primećuje promene kod ivica i tekstura. Ukoliko se uporede vodeni pečat izvučen iz označene slike i utisnuti pečat, dobija se Hamingovo rastojanje od 0.997599.

Tehnika na bazi korelacije (engl. *Correlation Based Technique*) **–** Slika sa vodenim pečatom, u ovoj tehnici, dobija se kada se u skrivenu sliku doda uzorak slučajnog pseudo šuma sa faktorom pojačanja. Sa porastom faktora pojačanja raste robustnost, ali opada kvalitet slike.

Maskiranje za vid nebitnih delova – Ova tehnika koristi nemogućnost ljudskog oka da razlikuje sitne detalje, naročito na onim delovima slike koji predstavljaju teksture. Na tim delovima slike, pošto je oko skoncentrisano na celinu, moguće je izmeniti intenzitet osvetljaja pojedinih piksela, a da oko ne primeti razliku. Ukoliko bi se označila područja koja su ispunjena jednom bojom, razlika bi se odmah primetila.

4.11. Tehnike za korekciju slike

Nakon ubacivanja skrivenih podataka u sliku, može doći do zamućenosti u određenom delu slike. Ovaj problem možemo rešiti tako što ćemo originalnu sliku malo potamniti, a zatim ubaciti skrivene podatke u istu. **Maskiranje i filtriranje** je jedna od najzastupljenijih tehnika u steganografiji, čiji se uspeh zasniva na činjenici da ljudsko oko teško uočava razlike među bojama slabije sjajnosti.

Dodavanje šuma je tehnika koja se zasniva na dodavanju belih tačaka ili izbeljivanju tamnijih. Kod krajnjeg korisnika se stvara utisak da je slika skenirana ili da je slabijeg kvaliteta, pa će ovakvu sliku retko ko detaljno analizirati. Bitno je, da se pri dodavanju šuma, ne menjaju bitovi koji nose skriveni podatak. Ova tehnika se smatra veoma efikasnom. Autori pečata često tvrde da njihovi pečati preživljavaju aditivne i nekorelisane multiplikativne šumove, međutim, mnogi ne napomenu koliku amplitudu šuma njihov pečat može zaista da podnese.

Korekcija boje piksela je tehnika koja upisuje skriveni podatak u svaki drugi piksel slike. Za korekciju slobodnog piksela gledaju se njegove originalne, ali i susedne boje, da bi se pronašla srednja vrednost boje. Kao rezultat dobićemo sliku koja izgleda skoro isto kao original, pa je verovatnoća da se otkrije tajni sadržaj minimalna. Ukoliko se podaci sakriju u svaki treći piksel, slika će još bolje izgledati, ali će biti srazmerno manje mesta. Nedostatak ove tehnike je što se mogu smestiti male količine podataka [23].

4.12. Geometrijske transformacije

Geometrijske transformacije su operacije koje se primenjuju na geometrijski opis objekta. S obzirom da menjaju sliku, smatraju se takođe i vrstom napada na vodene pečate. U geometrijske transformacije spadaju:

- **Translacija** (engl. *Translation*) – Translacija predstavlja refleksiju preko jedne ose, koja je praćena refleksijom preko druge ose, paralelne prvoj osi, i predstavlja potpuno kretanje, gde se svaka tačka slike pomera za istu vrednost u datom pravcu. Translacija se može takođe interpretirati kao pomeranje koordinatnog početka sistema.
- **Odsecanje** (engl. *Cropping*) – Ovo je jedan od najosnovnijih procesa kod digitalne obrade slike. Sastoji se od uklanjanja spoljnih delova slike radi poboljšanja pozacije i naglašavanja dotičnog predmeta, otklanjanja neželjenog dela sa slike, poboljšanja kvaliteta ili promene razmere slike. Ukoliko je napadač zainteresovan za neki određeni deo slike, on će primeniti ovu tehniku. Mnoge web stranice koriste segmentaciju slike, koja je zapravo i osnova za „Mosaic“ napad (ekstreman slučaj odsecanja slike).
- **Skaliranje** (engl. *Scaling*) – Skaliranje je česta operacija kod skeniranja otisnute slike. Takođe, obavezna je u pripremi slika za web izdavaštvo. Skaliranje može biti uniformno i neuniformno. Uniformno skaliranje je linearna transformacija koja uvećava ili umanjuje objekte, a pritom zadržava odnos veličina stranica slike. Neuniformno skaliranje menja oblik objekta i ne čuva odnos veličina stranica slike. Kod uniformnog skaliranja, rezultat je sličan originalu, jer je faktor skaliranja isti u svim pravcima. Međutim, ukoliko se razlikuje najmanje jedan od faktora skaliranja, dobiće se neuniformno skaliranje. Većina pečata otporna je na uniformno skaliranje.
- **Rotacija** (engl. *Rotation*) – Rotacija je transformacija koja se izvodi „okretanjem“ objekta oko fiksne tačke – centra rotacije. Rotacija se najčešće vrši za 90° i 180°. Rotacija za „mali“ ugao, posebno u kombinaciji sa odsecanjem, obično ne menja komercijalnu vrednost slike, ali može učiniti pečat neprepoznatljivim. Ova operacija je veoma česta u procesu skeniranja slika.
- **Smicanje** (engl. *Shearing*) – Smicanje je transformacija koja efektivno rotira određenu osu, tako da ose ne budu više upravne. Primenom smicanja na skup tačaka ravni, promeniće se svi uglovi između njih, i dužina bilo koje duži koja nije paralelna smeru premeštanja, dok će linije koje su paralelne sa osama ostati iste dužine. Dakle, smicanje nije isto što i rotacija. Smicanje će iskriviti oblik, ali neće sačuvati površinu geometrijske figure, uskađenost i relativno rastojanje kolinearnih tačaka.
- **Refleksija** (engl. *Reflection*) – Refleksija je mapiranje iz Euklidove ravni u istu ravan, što je izometrija sa hiperravni kao skup fiksnih tačaka, koji se naziva osa (kod 2D) ili ravan (kod 3D) refleksije. Izgled figure u refleksiji je njen odraz u ogledalu u osi ili ravni refleksije.
- **Okretanje** – Obrnuta slika (engl. *Flipped image*) se generiše od strane odraza originala preko horizontalne ose, dok se kod okrenute slike (engl. *Flopped image*), slika reflektuje preko vertikalne ose. Slike okrenute oko vertikalne ose su češće, jer mogu da se koriste za korekciju neprekidnih grešaka između slika koje ne mogu lako da se primete, dok je kod slike okrenute oko horizontalne ose to veoma očigledno.

4.13. Operacije za poboljšanje kvaliteta slike

Za poboljšanje kvaliteta slike mogu se koristiti različiti, pažljivo odabrani filtri i efekti za obradu slike. Prema načinu obrade slike, metode možemo podeliti na:

- Lokalne operacije nad pojedinačnim pikselima,
- Prostorne operacije nad grupom piksela,
- Operacije u frekventnom domenu.

Lokalne operacije nad pojedinačnim pikselima predstavljaju preslikavanje nivoa sivog piksela iz originalne slike u novi nivo sivog.

- **Modifikacija histograma** – Histogram je trakasti grafik koji služi za prikazivanje specifične vrednosti osvetljenosti za svaki piksel pojedinačno. U cilju kompenzovanja loših uslova osvetljenja, vrši se modifikacija histograma koja obuhvata rastezanje i izjednačavanje histograma. Tako će se poboljšati kvalitet slike, popraviti njena osvetljenost i kontrast.
- **Gama korekcija** – Ova operacija je vrlo česta i služi za poboljšanje kvaliteta slike, korekciju osvetljenosti i boje komponenti slike. Gama korekcija naročito je korisna za isticanje detalja iz tamnih oblasti slike, te njenom primenom dobijamo nove detalje u tamnim oblastima koji ranije nisu bili vidljivi.
- **Kvantizacija boja** – Ova operacija često se primenjuje u konverziji zapisa slika u GIF format, za prikazivanje na web stranicama.
- **Obnavljanje** – Primenjuje se za smanjenje efekata određene degradacije slike, ali se koristi i za uklanjanje degradacije koju je uneo pečat, što će ukloniti i sam pečat.

Kod prostornih operacija se u postupak izračunavanja jednog piksela uvodi i grupa piksela koja ga okružuje, a koja se naziva lokalno susedstvo. Vrlo često se prostorne operacije izvode konvolucijom slike i konačnog impulsnog odziva filtra koji se naziva prostorna maska. Zavisno od oblika i sadržaja prostorne maske, prostorne operacije mogu biti veoma raznovrsne i mogu imati različite namane.

- **Niskofrekventno filtriranje (Prostorno usrednjavanje) –** Ovo filtriranje se vrši tako što se vrednost svakog piksela zameni sa težinskom srednjom vrednošću lokalnog susedstva tog piksela. Slike dobijene na ovaj način imaju velika izobličenja. Prva vrsta izobličenja je karakteristična za male granične učestanosti i tada slika postaje neoštra, nejasna ili razmazana. Gubitak oštrine je posledica ukidanja visokih učestanosti, koje su odgovorne za prikaz ivica i detalja u slici. Drugi vrsta izobličenja manifestuje se pojavom lažnih varijacija nivoa sivog u okolini stvarnih ivica, nezavisno od vrednosti granične učestanosti. Ove varijacije su posledica oscilatornog karaktera impulsnog odziva idealnog filtra, što se može ublažiti modifikacijom postupka usrednjavanja, gde se zamenjuju samo one vrednosti piksela koje su znatno promenjene uticajem šuma. Ovaj postupak je pogodan za uklanjanje Gausovog šuma iz slike, pod uslovom da intenzitet šuma nije preterano veliki. Međitim, ukoliko je intenzitet šuma veliki, usrednjavanjem se znatno menjaju i vrednosti piksela koje nisu promenjene šumom, pa se može pokvariti subjektivni kvalitet slike i uticati na pečat unutar slike. Najčešće se primenjuje Gausov filtar.

- **Visokofrekventno filtriranje (Izoštravanje slike)** – Izoštravanje slike se može postići isticanjem visokih učestanosti u spektru slike. Postoje metode za izoštravanje slike koja se zasniva na primeni aproksimacije gradijenta koji predstavlja izvod funkcije slike i nosi informacije o ivicama. Takođe, postoje i metode koje maskiraju neoštre delove tako što oduzimaju sliku dobijenu niskofrekventnim filtriranjem od originalne slike. Da bi se dobio još bolji subjektivni kvalitet slike, visokofrekventno filtriranje često se kombinuje sa drugim metodama (npr. izjednačavanje histograma). Iako se sa izoštravanjem slike poboljšava vizuelni utisak posmatrača, ponekad se može pokvariti izgled slike. Takav slučaj se javlja kada originalna slika sadrži šum. Pošto šum ima širokopojasni, a često i visokofrekventni karakter, izoštravanjem se uticaj šuma još više pojačava i kvari izgled slike. Ovi filtri se smatraju jako dobrim za napade na neke vrste pečata, jer vrlo uspešno pronalaze i uklanjaju visokofrekventni šum, koji je pečat uneo u sliku. Veštiji napadi zasnovani su na Laplasovom operatoru.

Filtriranje slike niskofrekventnim ili visokofrekventnim filtarskim funkcijama može se izvršiti i u prostornom i u frekventnom domenu. U prostornom domenu filtriranje se vrši konvolucijom slike sa maskom, koja u stvari predstavlja impulsni odziv filtarske funkcije. Najčešće se koriste maske malih dimenzija, jer amplitudska karakteristika takve filtarske funkcije nije mnogo selektivna, te je filtriranje lošije. Takođe, maske malih dimenzija utiču na mali broj aritmetičkih operacija pri filtriranju u ovom domenu.

U frekventnom domenu, filtriranje se vrši množenjem frekventnog spektra slike sa frekventnom karakteristikom filtra. Neželjene komponente spektra slike se mogu preciznije eliminisati, što ovo filtriranje čini znatno boljim. Međutim, broj računarskih operacija u frekventnom domenu je veći nego kod filtriranja u prostornom domenu, zbog izračunavanja direktne i inverzne dvodimenzionalne transformacije slike.

Frekventni sadržaj slike može se promeniti množenjem dvodimenzionalne DFT slike sa funkcijom prenosa linearnog filtra. Primenom inverzne transformacije dobiće se obrađena slika. Primenom DFT transformacije, funkcija prenosa definiše se tako da ne utiče na faznu karakteristiku spektra slike, tj. filtarska funkcija ima fazu jednaku nuli.

- **Uvećanje (Prostorna interpolacija) slike** – Replikacija (ponavljanje) piksela je najjednostavniji metod prostorne interpolacije, gde se svaki piksel duž linije ponavlja još jednom, a svaka tako dobijena linija se takođe ponavlja. Na taj način dobiće se stepen povećanja od dva puta duž svake koordinatne ose, tj. broj piksela u slici će se povećati četiri puta. Kod linearne interpolacije pretpostavlja se linearna zavisnost intenziteta između dva susedna piksela u istoj vrsti ili koloni. Primena linearne interpolacije daje znatno bolje rezultate od postupka uvećanja replikacijom piksela.
- **Smanjivanje (decimacija) slike** – Pre izvođenja postupka decimacije potrebno je izvršiti filtriranje filtrom čije su granične učestanosti manje od originalnih učestanosti odabiranja, po obe ose, za najmanje 2n puta. Najčešće korišćen filtar je niskofrekventni filtar, koji predstavlja jednostavan postupak usrednjavanja, kojim se grupa od 2x2 piksela zamenjuje jednim pikselom, čiji je intenzitet jednak srednjoj vrednosti intenziteta grupe piksela. Kod slika sa izraženijim visokofrekventnim sadržajem često je potrebno koristiti filtar bolje selektivnosti. Najčešće se koristi dvodimenzionalni FIR filtrar, zbog filtriranja konvolucijom filtra i slike u prostornom domenu.

U slučajevima kada transformacije kontrasta ili linerano filtriranje ne daju dobre rezultate, mogu se primeniti neke od metoda nelinearnog filtriranja, kao npr.:

- **Medijan filtriranje** – Kod medijan filtriranja vrši se zamena vrednosti piksela ulazne slike sa medijanom lokalnog susedstva tog piksela. Lokalno susedstvo, ili prozor nad kojim se obavlja medijan operacija, ima najčešće neparan broj elemenata i dimenzije 3x3, 5x5 ili 7x7 elemenata. Ovo filtriranje uspešno uklanja impulsni šum iz slike, koji se manifestuje u vidu izolovanih piksela ili linija u slici, a pri tom je sačuvana prostorna rezolucija slike.
- **Filtriranje korenovanjem** – Kod ovog filtriranja vrši se nelinearna transformacija modula transformacionih koeficijenata, dok se fazni spektar ne menja. Filtriranje korenovanjem ističe male ampritude u spektru, a potiskuje velike. U spektru tipičnih slika, korenovanje ističe visoke učestanosti.
- **Homomorfno filtriranje** – Kod homomorfnog filtriranja prvo se vrši logaritmovanje ulaznog signala, a zatim se na tako dobijeni signal primenjuju konvencionalni algoritmi linearnog filtriranja u prostornom ili frekventnom domenu. Na dobijeni signal primenjuje se eksponencijalna transformacija, čime se dobija obrađeni signal slike. Ova metoda filtriranja pogodna je za uklanjanje degradacije slike koje, nakon logaritmovanja, dobijaju aditivni karakter, te se mogu lakše eliminisati iz slike [26].

4.14. Sigurnost digitalnih vodenih pečata i vrste napada

Zbog postojanja širokog spektra softvera za procesuiranje slike, mogući su napadi na robustnost sistema sa vodenim pečatom. Svrha napada na digitalni vodeni pečat je uništavanje istog, sa ciljem da se ukinu zabrana od kopiranja, brisanje vlasnika dokumenta i ostale nelegalne radnje.

Objekat sa vodenim pečatom može biti izložen različitim malicioznim namernim ili nenamernim napadima. Neki od njih su sledeći:

- **Kompresija slike:** Koristi se da bi se smanjio prostor za smeštanje podataka i cena širine opsega koji je potreban za emitovanje slike. Metode kompresije sa gubicima su mnogo štetnije od metoda kompresije bez gubitaka, jer stvaraju nepovratne promene na slikama, pa je verovatnoća da će podaci vodenog pečata biti oporavljeni veoma mala. Metode kompresije bez gubitaka mogu oporaviti podatke vodenog pečata primenom inverzne operacije.
- **Transformacija slike:** Ovaj tip napada zove se još i sinhronizacioni ili geometrijski napad. U ovaj napad spadaju sve manipulacije koje utiču na geometriju slike, kao što su translacija, rotacija, skaliranje, odsecanje i horizontalno okretanje. Softver StirMark koristi male lokalne geometrijske distorzije da onesposobi detekciju vodenog pečata.
- **Poboljšanje slike:** Ovaj napad predstavlja skup operacija koje desinhronizuju informaciju vodenog pečata u slici. U ove napade spadaju izjednačavanje histograma, izoštravanje, izglađivanje, median filtriranje i povećanje kontrasta.
- **Degradacija slike:** Ovaj napad uklanja delove slike i na taj način oštećuje robustnost vodenog pečata. Delovi koji su zamenjeni mogu nositi podatke vodenog pečata. Primeri za ovu operaciju su parcijalno odsecanje, uklanjanje redova i kolona, kao i umetanje Gausovog šuma.

- **Promena slike i brisanje linija:** Kod ovog napada, napadač može da pomera pečat horizontalno ili vertikalno, ili da obriše ceo niz piksela, kako bi uništo informaciju koju vodeni pečat nosi [27]. Veoma je efikasan protiv jednostavnih implementacija pečata koji rade na principu raspršenog spektra u prostornom domenu.
- **Napad niskopropusnog filtriranja:** Ukoliko se, na sliku sa vodenim pečatom, primeni niskopropusno filtriranje, rezultat će biti drugačija mapa sastavljena od šuma.
- **Napad interference:** Ovaj napad pridodaje šum na objekat sa vodenim pečatom. Primeri ovog napada su kompresija sa gubitkom, kvantizacija, potiskivanje šuma, konverzija i beli šum.
- **Napad uklanjanja:** Ovaj napad uklanja podatak vodenog pečata iz objekta koji sadrži vodeni pečat, koristeći činjenicu da je vodeni pečat dodatni signal šuma koji je prisutan u originalnom signalu.
- **Lažni napad:** Rezultat ovog napada je umetanje i brisanje objekta, promena pozadine slike, a kao krajnji cilj, zamena slike.
- **Napad na sigurnost:** Algoritam se smatra sigurnim ukoliko utisnuta informacija vodenog pečata ne može biti uništena, detektovana ili zaboravljena. Međutim, ukoliko je algoritam poznat, napadač može da proceni i primeni modifikacije koje će učiniti vodeni pečat ne važećim, što predstavlja napad na sigurnost.
- **Napad na protokol:** Za razliku od predhodnih napada, ovaj napad nema za cilj da uništi niti da onesposobi detekciju utisnute informacije, već daje prednost semantičkom nedostatku u implementaciji vodenog pečata.
- **Kriptografski napad:** Ova vrsta napada bori se sa razbijanjem sigurnosti i slični su onima koji se primenjuju u kriptografiji. Kriptografski napad koristi iscrpnu nasilnu metodu (engl. *Brute force*) u pronalaženju tajnog ključa vodenog pečata. U ovu vrstu napada spada i oracle napad (engl. *Oracle attack*), gde napadač koristi sopstveni detektor za uklanjanje vodenog pečata.
- **Aktivni napadi:** Kod ovog napada, haker namerno pokušava da ukloni vodeni pečat ili da ga jednostavno učini nemogućim za detekciju. Ovo predstavlja veliki problem u zaštiti autorskih prava, zaštiti od kopiranja i kod aplikacija otiska prsta.
- **Pasivni napad:** Za razliku od predhodnog napada, u ovom slučaju napadač samo pokušava da odredi da li je oznaka vodenog pečata prisutna ili nije.
- **Koluzioni napad:** Cilj hakera je isti kao i kod aktivnog napada, samo je metoda malo drugačija. Napadač koristi nekoliko kopija istog podatka sa različitim vodenim pečatima, kako bi napravio novu kopiju bez vodenog pečata. Ovo predstavlja problem kod primene aplikacija otiska prsta, ali nije široko rasprostranjen zato što napadač mora da ima pristup višestrukim kopijama istog podatka [20].

4.15. Otpornost digitalnih vodenih pečata na napade

Osim što mora da bude otporan na uobičajene transformacije kroz koje dati signal prolazi, vodeni pečat može biti podvrgnut i procesiranju signala koje je isključivo namenjeno uklanjanju pečata. Otpornost pečata se može proveriti pomoću pitanja: da li je pečat prisutan u podacima nakon što signal pretrpi promene i može li ga detektor pečata detektovati. Mnogi pečati ostaju u podacima nakon geometrijskih promena. Algoritmi detekcije mogu detektovati pečat samo ako se geometrijska promena prethodno ukloni, u suprotnom, detektor neće moći da detektuje pečat.

Koliko će tehnika označavanja otpornim vodenim pečatom biti efikasna može se oceniti prema veličini i kompleksnosti vodenog pečata, statističkoj nevidljivosti, neprimetnosti, sigurnoj detekciji, otpornosti na uklanjanje, otpornosti na distorziju, mogućnosti izmene i višestrukosti označavanja vodenog pečata. Svi ovi parametri su bitni za postizanje funkcionalnosti pečata [24].

Otpornost se može postići ukoliko se pečat postavi u perceptualno bitno područje slike, jer je kvalitet slike očuvan samo ako su perceptualno bitna područja slike zadržana. Perceptualno nebitna područja slike mogu biti uklonjena, a da se pri tom ne naruši kvalitet slike. Međutim, pečati koji se nalaze u ovom području, neće biti otporni i moći će lako da se uklone.

Otpornost digitalnih vodenih pečata na napade se može postići pomoću:

- **Privatnog pečata** – Kod ovog sistema neoznačeni sadržaj za dekodovanje i pseudo-slučajni ključ, koji generiše pečat, poznati su samo pošiljaocu i primaocu. Za razliku od javnih pečata, gde svako može da dekoduje pečat, privatni pečat je otporniji na napade. Ukoliko je dostupna samo jedna označena kopija sadržaja, da bi se uništio pečat, jedini mogući napad je dodavanje šuma u sliku. Red veličine dodatog šuma potrebnog da bi se pečat sigurno uništio je toliko velik da znatno narušava kvalitet slike. Ukoliko imamo više kopija istog sadržaja označenog različitim pečatima, moguć je napad kao što je računanje srednje vrednosti svih kopija. U slučaju da su raspoložive sve informacije potrebne za dekodovanje pečata, najjednostavniji napad je invertovanje postupka označavanja.
- **Asimetričnog kodera/dekodera** – Ukoliko uklanjanje javnog pečata zahteva invertovanje procesa kodovanja, poželjno je da proces kodovanja bude što više kompleksan, naročito ako se pečat unosi samo jednom. Međitim, ukoliko dekoder funkcioniše u realnom vremenu, neophodno je da proces dekodovanja bude znatno jednostavniji od kodovanja.
- **Neinvertibilnog pečata** – Ukoliko je pečat generisan pomoću sadržaja koji se označava, tada reverzni proces brisanja pečata nije moguć bez posedovanja originalnog, neoznačenog sadržaja. Na taj način se sprečava da potencijalni napadač, u označenom sadržaju, potraži neki set vrednosti i proglasi ga za svoj pečat, i tako stvori konfuziju ko zapravo ima originalni sadržaj i ko je prvi ubacio pečat u isti.

Pečati zavisni od sadržaja se koriste ukoliko korisnik poseduje veći broj dokumenata označenih istim ključem. Pečat se maskira pomoću pseudo-slučajnih sekvenci kako bi se postigla što veća sličnost pečata i slučajnog šuma. Što je sličnost veća, pečat je teže otkriti, a samim tim i ukloniti. Na ovaj način se sprečava otkrivanje pečata primenom statističkih metoda.

Veličina pečata predstavlja količinu podataka koja se može ubaciti u zadati signal. Međutim, ubacivanjem veće količine podataka u zadati signal, neki od bitova biće manje zaštićeni, te će imati manje originalnih bitova za maskiranje. Veličina pečata i njegova otpornost su uglavnom obrnuto proporcionalne, pa je potrebno napraviti kompromis između njih. Ovaj parametar je posebno važan za javne pečate.

Ponekad je poželjno izmeniti pečat nakon unošenja, kao npr. kod digitalnih video diskova, čijim označavanjem bi se omogućila samo jedna kopija sadržaja. Nakon napravljene kopije, potrebno je izmeniti pečat na originalu da bi se onemogućilo dalje kopiranje. To se može postići tako što će se prvobitni pečat ukloniti i ubaciti novi, ili ubaciti novi pečat koji bi zabranio kopiranje. U prvom slučaju sistem nije otporan na napade, jer je moguće ukloniti pečat. Novi, jedinstveni pečat se može ubaciti u sadržaj u svakoj tački distributivnog lanca, pa je postojanje višestrukih pečata, koji omogućuju praćenje sadržaja, veoma poželjno.

Poželjno je da pečat omogućuje veliki broj valjanih pečata. Što je broj mogućih pečata veći i što su međusobno više različiti, to su veće mogućnosti primene sistema, a verovatnoća tačne detekcije pečata u označenom materijalu bolja.

4.16. Primena metode srednje vrednosti piksela protiv geometrijskog napada

Kanphade i Narawade (2013), predstavili su metodu vodenog pečata koja primenjuje tehniku srednje vrednosti piksela. Koristi se u vojsci, kao i za zaštitu autorskih prava. S obzirom da potpuni oporavak vodenog pečata nije moguć, ova metoda omogućije njegov oporavak sa kompromisom u kvalitetu. Predložena metoda srednje vrednosti je robusna i polu-reverzibilna. Izabran je najniži nivo piksela kako bi se dobila glatkoća originalnog izgleda i bolja vizuelna percepcija. Kombinacija unapređene geometrijske transformacije i predznanja o geometrijskim transformacijama, povećava robusnost protiv geometrijskih napada. Rezultati su pokazali da je predloženi metod vodenih pečata, osim što je polu-reverzibilan, veoma robustan protiv različitih vrsta napada kao što su rotacija, skaliranje i translacija. Osim toga, ograničen je kvalitet slike sa vodenim pečatom, kapacitet utiskivanja je optimalan i složenost je manja.

Metoda LSB supstitucije daje bolji kvalitet slike sa vodenim pečatom, ali nije robusna na geometrijske napade. DCT metoda pruža ograničen kvalitet i robustnost, dok CDMA metoda daje slab kvalitet i prihvatljivu robustnost na napade. DWT metoda, isto tako, daje slab kvalitet slike sa vodenim pečatom i malu robustnost. Dakle, ove metode daju umeren kvalitet slike sa vodenim pečatom i izglađuju sliku. Bitovi su direktno ubačeni u LSB skrivene slike. Metoda LSB supstitucije daje veći PSNR u poređenju sa drugim metodama.

Ponuđene metode vodenog pečata su pogodnije za primenu u medicini jer daju bolji kvalitet za snimke u medicini, ali daju lošiji kvalitet za crtane slike. Rezultati su pokazali da je predložena metoda vodenog pečata jednostavna i polu-reverzibilna. Sličnost obnovljenog i originalnog vodenog pečata je 100%. Slika ima kvalitetnu vizuelnu percepciju i tehnički je usavršena [1].

5. BIOMETRIJSKI VODENI PEČATI

Bezbednost i autentičnost biometrijskih podataka je postala sve kritičnija sa rasprostanjenom primenom biometrije. Utvrđivanje autentičnosti originalnog biometrijskog podatka je takođe ključni problem, naročito kada senzori i ekstraktori karakteristika (ili generator šablona) nisu integrisani. S obzirom da su tradicionalne metode za autentičnost podataka (npr.: kriptografske heš funkcije ili provera autentičnosti poruke) veoma osetljive na svaki bit ulaznog podatka, u ovom slučaju ne mogu se primeniti. Informacija koju nosi biometrijska slika se zadržava, čak i kada podaci prođu kroz operacije za očuvanje sadržaja (kompresija i poboljšanje kvaliteta).

Pravljenje kompromisa između robustnosti i bezbednosti je učinilo da sistem postane ranjiv na mnoge pretnje. Digitalni vodeni pečati predstavljaju najbolje rešenje za ovaj problem. Vodeni pečat je sve istaknutiji bezbednostni alat koji se uspešno primenjuje na veliki broj aplikacija, radi zaštite originalnih multimedijskih podataka, kao što su zaštita autorskih prava i autentifikacija sadržaja. Pomoću metode robustnog vodenog pečata utiskuju se tajne informacije u host sliku, tako da se sadržaj vodenog pečata može oporaviti nakon što pretrpi umerene distorzije.

Jain et al. (2003) predložio je uvođenje vodenog pečata kao dodatnu odbranbenu liniju. Pomoću vodenog pečata može efikasno da se unapredi bezbednost i pouzdanost biometrijskog sistema. Prednosti vodenih pečata za zaštitu biometrijskih podataka su:

- Sakriven neprimetno u host podatku, vodeni pečat može da posluži kao verodostojni token u forenzici za bezbedno čuvanje. Takođe, može da obezbedi mehanizam za praćenje, u slučaju presretanja podataka, za identifikaciju porekla biometrijskog podatka.
- Informacija vodenog pečata se spaja sa host podatkom, te ne zahteva dodatno skladištenje ili prenos sredstava. Takođe, verifikacija „na licu mesta“ ne zahteva privilegije pri pristupu bazi biometrije i vodenog pečata.
- Vodeni pečati ne utiču na druge bezbednosne alate, pa se na podatak vodenog pečata ili na pečatirani host podatak mogu primeniti kriptografske operacije ili tehnike za zaštitu šablona.

Prema funkcionalnosti biometrijskih vodenih pečata, postojeće tehnike se mogu podeliti na dve grupe:

1. **Multimodalna autentifikacija** – Ova metoda ugrađuje podatak vodenog pečata u biometrijski uzorak, kao dodatnu informaciju identitetu, za povećanje performansi autentifikacije. Da bi obezbedio bezbedan prenos šablona lica, Jain et al. (2003) je utisnuo svojstvene koeficijente lica u sliku otiska prsta. Izvučeni vodeni pečat može uspešno da pomogne sistemu pri identifikaciji. Vatsa et al. (2005) je utisnuo karakteristike lica u sliku otiska prsta pomoću metode zasnovane na DWT-SVM, kako bi unapredio tačnost multimodalne autentifikacije. Maiorana et al. (2007) je utisnuo dinamičke karakteristike potpisa u statičnu sliku potpisa pomoću robusne DCT-Radon transformacije. Mogu se razmotriti različite karakteristike potpisa za veću pouzdanost pri autentifikaciji. Vatsa et al. (2009) je primenio RDWT algoritam sa tri nivoa, kako bi utisnuo MFCC karakteristike glasa u kolor sliku lica, i tako povećao robustnost, bezbednost i preciznost mutimodalne biometrijske verifikacije. Ma et al. (2010) utisnuo je minucije otiska prsta u sliku lica.

Verodostojnost podataka se može utvrditi proverom validnosti izvučenog šablona sa minucijom otiska prsta.

2. **Dvofaktorska autentifikacija** – Kod ove metode uvodi se dodatna šema za autentifikaciju kako bi se povećala bezbednost sistema. Noore et al. (2007) je predstavio tehniku za verifikaciju pri čuvanju i zaštitu integriteta slike otiska prsta, koristeći podatke lica i demografskog teksta kao višestruki vodeni pečat. Izvučena slika lica i binarnog teksta vodenog pečata mogu poslužiti kao dodatna informacija za potvrđivanje identiteta. Kim et al. (2009) je utisnuo malu sliku lica u sliku otiska prsta kao verodostojni token. Slika vodenog pečata se izvlači za vreme autentifikacije, kako bi se potvrdio integritet otiska prsta i slike lica. Ratha et al. (2001) je primenio metodu odgovor/izazov na sliku otiska prsta, kako bi autentifikovao njegov izvorni senzor. Ukoliko je slika neovlašćena ili dolazi iz nepouzdanog senzora, server će, zbog nedostatka vodenog pečata, detektovati bezbednostnu pretnju. Ova vrsta tehnike efikasno garantuje autentičnost podataka. Međutim, biometrijski šablon vodenog pečata može da posluži jedino kao konvencionalni autentifikacioni token (kao npr.: logo, heš kod).

Nedostatak oba pristupa je taj što se izvučeni šablon direktno koristi za identifikaciju, bez proveravanja verodostojnosti, tako da vodeni pečat poboljšava performanse prepoznavanja pod uticajem distorzije i napada, što ne obezbeđuje dodatnu sigurnost.

Problem ranjivosti podataka biometrijskog sistema može se rešiti zaštitom šablona. Na taj način se vektorske karakteristike biometrije transformišu u tajni domen, što garantuje sigurnost podataka. Međutim, u nekim slučajevima biometrijske podatke bi trebalo čuvati u eksplicitnom obliku, a ne kao kao šifrovani šablon (slika lica na pasošu, slike otiska prsta koji se čuvaju za pravne dokaze).

Povećanje kapaciteta vodenog pečata za obilnije identifikacione informacije, uticaće na smanjenje robustnosti vodenog pečata. Podaci vodenog pečata se koriste samo iz pouzdanih baza ili komunikacionih okruženja, gde su distorzija ili napad malo verovatni.

5.1. Primena vizuelne kriptografije i transformacija radi bezbedne biometrijske autentifikacije

Vizuelna kriptografija je posebna tehnika šifrovanja koja omogućava skrivanje informacija unutar slike, tako da je korisnik, uz odgovarajući ključ, može dešifrovati bez upotrebe računara ili dodatnog izračunavanja. Ova tehnika koristi slojeve identičnih ili dodatnih komplementarnih piksela i predstavlja vizuelnu varijantu operacije XOR [4]. Primenjuje se u mnogim aplikacijama, pa tako, osim za skrivanje informacija, koristi se i za opšti pristup objektima, vizuelnu autentifikaciju i identifikaciju.

Pronađene su različite vrste vizuelne kriptografije. Naor i Shamir (1994) prvi su rešili problem skrivanja tajnih poruka primenom vizuelne kriptografije. U predloženoj metodi, tajna poruka je podeljena u dva sloja, odštampana na dve providne folije. Verheul i Tilburg (1997) predložili su metodu vizuelne kriptografije za sliku u boji. Nedostatak ove metode je loš kvalitet obnovljene slike i slojevi koji nemaju nikakvo značenje. Zato su naučnici unapredili ovu metodu skrivanjem kolor slike u nekoliko slika sa značenjem.

Najpoznatija steganografska metoda je LSB supstitucija, koja zamenjuje bit piksela sa najmanjim značenjem sa tajnom informacijom. SLSB (engl. *Selected Least Significant Bit*) je LSB metoda sa poboljšanim performansama. Ova metoda selektuje samo jednu boju od tri, u svakom pikselu slike, kako bi se sakrila tajna poruka. Algoritam koristi dva LSB piksela da smesti tajnu poruku u zelenu boju piksela koja je najpogodnija za utiskivanje.

Bhirud i Prabhu (2013) primenili su DWT metodu i vizuelnu kriptografiju kako bi sakrili sliku irisa. Slika irisa se utiskuje u sliku koja se pomoću DWT deli na četiri dela i na kraju kompresuje. Za utiskivanje tajne poruke primenjena je metoda tri bita sa najmanjim značenjem (engl. *Three Least Significant Bit*).

Rezultati su pokazali da primena ove metode štiti iris i tajnu poruku od krađe identiteta. Dobri rezultati su postignuti kombinovanjem DWT i Haar filtra. Dobijena je slika sa umanjenim brojem piksela u poređenju sa originalnom slikom irisa, dok je kvalitet slike održan primenom Haar transformacije [31].

Primenom DWT, razlaganjem irisa na dva nivoa, može se dobiti dobar kvalitet slike irisa i skrivene slike sa smanjenim zahtevanim opsegom, bez kompresije krajnje pečatirane slike. Primenom metode zamene tri bita sa najmanjim značenjem povećava se veličina tajne poruke pri utiskivanju, a da pritom kvalitet slike irisa ostane isti.

5.2. Biometrijski vodeni pečat zasnovan na prioritetu bita

Algoritam za vidljive vodene pečate u DCT domenu deli osnovnu sliku u različite blokove, koji su klasifikovani pomoću perceptualnih metoda i čiji DCT koeficijenti su modifikovani. Kod amplitudne modulacije za kolor slike, koristi se plavi kanal za utiskivanje informacija, koje će biti ponovo dobijene u procesu dekodovanja primenom tehnike susedne aproksimacije. Primenjuje se kod nevidljivih vodenih pečata. Međutim, ova metoda ne uzima u obzir problem prioriteta bitova.

Kod biometrijskih vodenih pečata, biometrija se pretvara u niz bitova, koji se zatim utiskuju u osnovnu sliku. Na primer, za utiskivanje niza bitova 0010 0001, primenjene su dve tehnike vodenog pečata. Nakon šifrovanja i dešifrovanja, primenom prve tehnike vodenog pečata, dobiće se niz bitova 0100 0001, sa greškom na drugom i trećem bitu. Primenom druge tehnike, dobiće se niz bitova 0010 0010, sa greškom na poslednja dva bita. Ukoliko broj pogrešnih bitova ukazuje na grešku, onda i tehnika dva vodena pečata daje istu grešku (dva pogrešna bita). Međutim, ako se ovaj utisnuti niz bitova pretvori u 8-bitni intedžer, a razlika između dva intedžera ukazuje na grešku, onda prva metoda vodenog pečata daje veću grešku od druge.

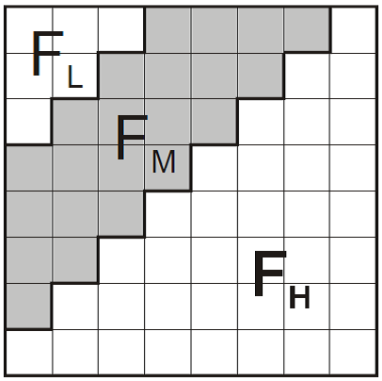
Hoang, Tran i Sharma (2008) predložili su metodu vodenog pečata koja se zasniva na amplitudskoj modulaciji i prioritetu nivoa bitova za biometrijske vodene pečate. Predloženo je da bitovi sa najvećim prioritetom budu utisnuti u sliku na određenoj poziciji, kako bi procenat greške pri vađenju podataka bio nizak. U poređenju sa metodom digitalnog vodenog pečata zasnovanoj na amplitudskoj modulaciji, rezultati predložene metode su pokazali značajno smanjenje grešaka (približno nula) i da nikakve promene nisu uticale na biometrijski autentifikacioni sistem. Predložena metoda je veoma korisna kod biometrijskih aplikacija, za utiskivanje numeričkih vrednosti uzorka (otiska prsta, irisa ili glasa) u sliku [28].

5.3. Primena algoritma robustnog vodenog pečata zasnovanog na DCT za obezbeđivanje sigurnosti slike irisa

Zhao i Koch (1995) predstavili su metodu razmene koeficijenata srednjeg opsega (engl. *Middle Band Coefficient Exchange*, **MBCE**). Nakon toga, Hsu i Wu (1996) su primenili DCT za utiskivanje koeficijenta srednjeg opsega. Algoritam šifruje jedan bit binarnog objekta vodenog pečata u jedan pod blok 8 x 8 host slike, tako da razlika dva koeficijenta srednjeg opsega bude pozitivna u slučaju da je šifrovana vrednost 1. U suprotnom, dva koeficijenta srednjeg opsega će se izmeniti.

Tehnika vodenog pečata u DCT domenu deli sliku na tri frekventna opsega (Slika 5.3.1), pa je utiskivanje informacija vodenog pečata u određeni frekventni opseg mnogo lakše (Langelaar et al., 2000). Pošto se DCT primeni na sliku, uzima se blok dimenzije 8 x 8.

Opseg niskih frekvencija F_L nosi najbitniji vizuelni deo slike, dok je opseg visokih frekvencija F_H podložan napadima šumom i uklanjanju kompresijom. Najpogodniji opseg za utiskivanje informacija vodenog pečata je opseg srednjih frekvencija F_M, jer ne utiče na bitne vizuelne delove slike, a komponente visokih frekvencija ne izlaže previše uklanjanju kada su na meti napada (Hernandez et al., 2000).



Slika 5.3.1: Frekventne oblasti u 8 x 8 DCT bloku

Za opseg srednjih frekvencija F_M biraju se dve lokacije iz DCT bloka ($DCT_{(U1;V1)}$ i $DCT_{(U2;V2)}$) kao oblasti za poređenje. Pošto se tekst vodenog pečata konvertuje u binarnu sliku, proveravaju se vrednosti piksela. Ukoliko se relativna veličina svakog koeficijenta ne slaže sa bitom koji treba da se šifruje, koeficijenti se zamenjuju. Ako je vrednost piksela u binarnom tekstu 1, DCT koeficijent se zamenjuje tako da bude $DCT_{(U1;V1)} > DCT_{(U2;V2)}$. Ukoliko je vrednost 0, koeficijent se zamenjuje tako da bude $DCT_{(U1;V1)} < DCT_{(U2;V2)}$. Ova šema skriva podatke vodenog pečata tako što 0 i 1 tumači sa relativnim vrednostima dve fiksne lokacije ($DCT_{(U1;V1)}$ i $DCT_{(U2;V2)}$) u oblasti srednjih frekvencija F_M, umesto ubacivanja bilo kakvih podataka. Ovakva zamena koeficijenata neće uticati značajno na sliku vodenog pečata, jer DCT koeficijenti srednjih frekvencija imaju slične magnitude (Zhao i Koch, 1995; Johnson i Katzenbeisser, 2000). Kod izvlačenja slike, ponovo se uzima 8 x 8 DCT slike, pa će se 1 dekodovati ako je $DCT_{(U1;V1)} > DCT_{(U2;V2)}$, a 0 ukoliko je $DCT_{(U1;V1)} < DCT_{(U2;V2)}$. Tako će se formirati vodeni pečat.

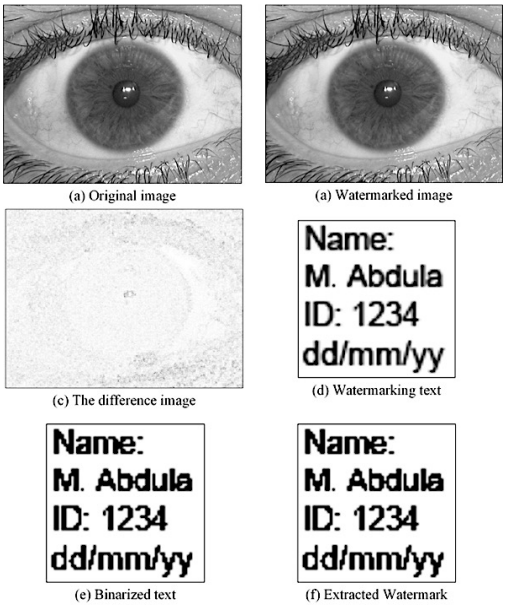
Ukoliko se koristi samo jedan par koeficijenata za sakrivanje podatka vodenog pečata, napadač može, analizom nekoliko pečatiranih kopija slike, predvideti lokaciju koeficijenata i uništiti ih. Abdullah, Dlay i Woo (2015) su rešili ovaj problem izborom tri para koeficijenta iz opsega srednjih frekvencija i tako povećali redudansu i robustnost šeme na različite napade.

Da bi povećali robustnost algoritma vodenog pečata, autori su predložili dodavanje konstante k tako da bude $DCT_{(U1;V1)} - DCT_{(U2;V2)} < k$. Izborom vrednosti konstante k povećava se jačina vodenog pečata. Povećanje konstante k će degradirati sliku, ali će smanjiti verovatnoću greške u fazi detekcije. Pokazalo se da vrednost konstante k=15 najbolja za percepciju nasuprot robustnosti [29].

Jedan bit teksta vodenog pečata sakriće se u svaki 8 x 8 blok slike. Kao objekat vodenog pečata uzima se jednodimenzionalni niz nula i jedinica. Korisnikove informacije (ime, broj lične karte i datum rođenja) nosi slika teksta vodenog pečata.

Dobar algoritam vodenog pečata mora biti neprimetan korisniku i ne bi trebao značajno da utiče na performanse poređenja biometrijskog sistema. Treba pouzdano da detektuje utisnutu informaciju, čak i kod degradirane slike vodenog pečata.

Objekat sa vodenim pečatom mora biti neprimetan korisniku. Na slici 5.3.2 (c) je prikazana razlika između originalne slike i slike sa vodenim pečatom. Razlika se ne može videti bez pomoći tehnike za obradu slike. Prosečna vrednost PSNR, između orginalne slike i slike sa vodenim pečatom, iznosi 37.69, dok prosečna vrednost BER iznosi 0.257%. Prosečna vrednost PSNR i BER izvučenog teksta vodenog pečata je 84.25 i 0.0244%.



Slika 5.3.2: Percepcija slike vodenog pečata

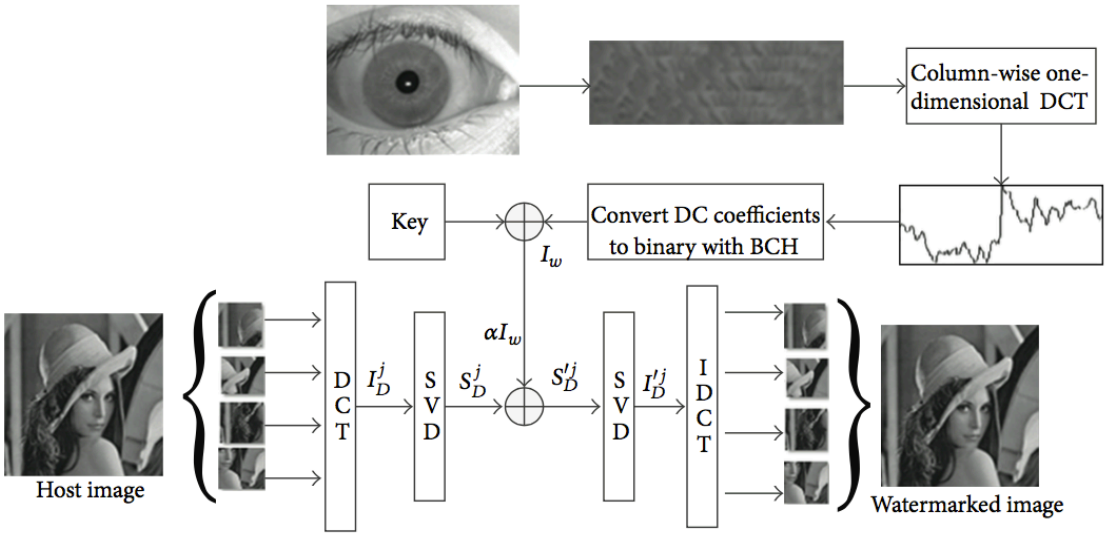
Ova metoda vodenog pečata je višestruko korisna za biometrijski sistem. Na primer, biometrijske karakteristike i informacije korisnika su uglavnom smeštene u nezavisnu bazu podataka. Vodeni pečat integriše biometrijske karakteristike sa ličnim informacijama u fajl, iz kojeg dozvoljava istovremeno smeštanje i izvlačenje. Takođe, iz izvučenog teksta se može verifikovati integritet biometrijskih karakteristika.

Predloženi algoritam ne zahteva originalnu sliku za izvlačenje vodenog pečata. Takođe, robustan je na JPEG kompresiju, filtriranje i šum. Ova metoda je lako primenjiva na sve biometrijske slike, ne utiče značajno na kvalitet slike irisa i na performanse poređenja biometrije.

5.4. Vodeni pečat biometrije irisa zasnovan na razlaganju jedinstvene vrednosti i DCT

Lu, Qu i Karimi (2014) predložili su šemu za povećanje bezbednosti, koja se više fokusira na prepoznavanje irisa nego na digitalne vodene pečate. Na biometrijski uzorak irisa primenjuje se DCT transformacija, a zatim se dobijena vrednost šifruje u BCH kod za kontrolisanje grešaka. Host slika se deli na četiri jednaka bloka. BCH kod se, pomoću ključa, utiskuje u jedinstvene vrednosti svakog koeficijenta host slike, koja je dobijena pomoću DCT. Pošto su DCT koeficijenti slike sa vodenim pečatom izmenjeni, na sliku se primenjuje inverzna kosinusna transformacija (IDCT) (Slika 5.4.1). Jačina vodenog pečata zavisi od ključa.

Rezultati su pokazali da predložena metoda može efikasno da izvuče vodeni pečat i ilustruje njegovu sigurnost i robustnost [30].



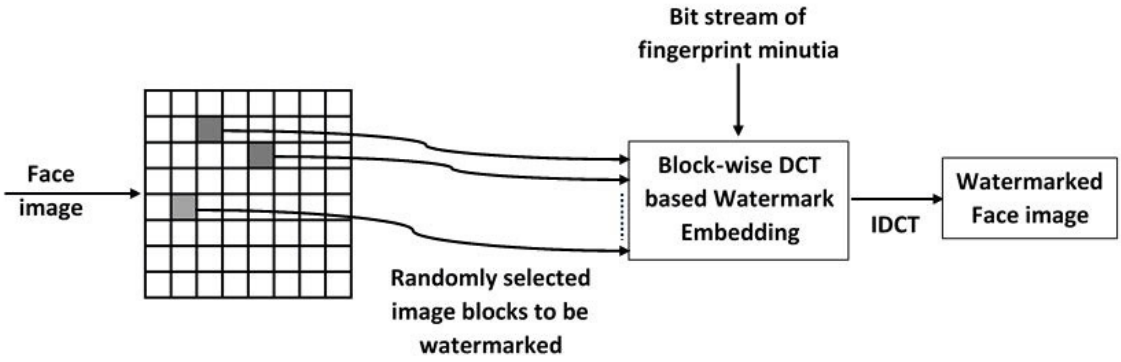
Slika 5.4.1: Proces utiskivanja vodenog pečata

5.5. Metoda vodenog pečata zasnovana na spajanju biometrija

Ghouzali (2015) predstavio je metodu vodenog pečata koja utiskuje informacije minucija otiska prsta u host sliku lica unutar DCT domena. Prvo se izvlače minucije iz slike otiska prsta, a zatim se svaka tačka minucije pretvara u niz bitova i koji se nasumično utiskuju u različite DCT blokove host slike lica.

Rezultati su pokazali da je predložena metoda efikasna u autentifikaciji i da ne degradira performanse u pristupu prepoznavanja originalnog lica, a da pritom štiti biometrijske podatke od neautorizovane manipulacije. Takođe, ukoliko se izdvoji podatak vodenog pečata koji sadrži minucije otiska prsta, isti mogu koristiti u autentifikaciji kao „druga linija odbrane“ host slike lica [36].

Međutim, predloženi sistem je ranjiv na sve vrste napada u klasičnim unimodalnim sistemima. Ukoliko se vodeni pečat utisne predloženom metodom pomoću korisničkog ključa, moguće je sprečiti napad presretanja podataka. Generator slučajnih brojeva, inicijalizovan sa tajnim korisničkim ključem, određuje koji će DCT blok slike biti pečatiran. Predložena metoda je data na slici 5.5.1.



Slika 5.5.1: Predložena šema DCT vodenog pečata zasnovana na biometriji

Predloženi autentifikacioni sistem obuhvata dve faze: fazu upisivanja i fazu verifikacije. U fazi upisivanja, korisnik predstavlja sistemu svoje biometrijske osobine, a zatim se pristupa procesu utiskivanja vodenog pečata. Dobijena pečatirana slika se smešta u bazu podataka umesto originalnog šablona, a zatim se na pečatiranu sliku lica primenjuje OLPP metoda kako bi se dobio podprostor malih dimenzija.

U fazi verifikacije primenjuje se isti proces utiskivanja vodenog pečata na već dobijene biometrijske osobine, nakon čega se pečatirana slika lica šalje u podprostor OLPP projekcije. Korisnik će dobiti dozvolu za pristup jedino ukoliko se vektorske karakteristike smeštene i testirane pečatirane slike lica poklapaju.

Za razliku od tehnike vodenog pečata zasnovanog u prostornom domenu, u frekventnom domenu koeficijenti su malo izmenjeni, što se neprimetno odražava na sliku i povećava joj robustnost na napade.

Kod slike vodenog pečata, koja je zasnovana na DCT raspodeli blokova, host slika se deli u blokove veličine 8 x 8 koji idealno odgovaraju JPEG kompresiji i obezbeđuju najmanje izobličenje slike. Pri autentifikaciji slike vodenog pečata treba paziti da se ne ugrozi preciznost performansi, jer utiskivanje vodenog pečata može uticati na karakteristična svojstva skrivene slike. Takođe, vidljivi efekat osvetljenosti cele slike ne bi trebalo da menja DC koeficient. U predloženoj tehnici vodeni pečat se utiskuje u koeficijente srednjih frekvencija DCT bloka, radi održavanja dobrog kompromisa između tačnosti performansi, neprimetnosti i robustnosti.

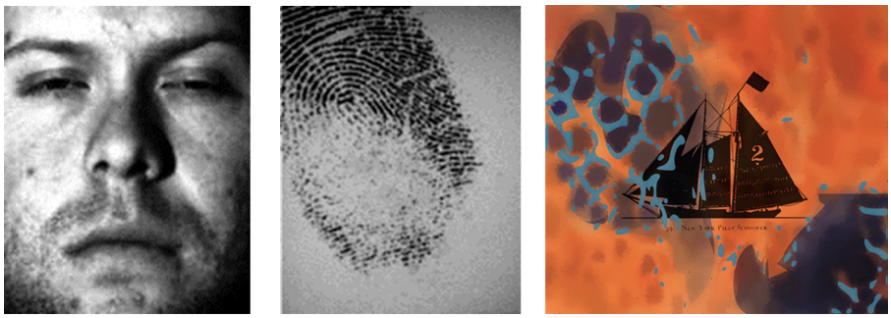
Metode za smanjenje dimenzionalnosti mogu da detektuju i analiziraju moguće prisutne strukture koje su skrivene u multidimenzionalnim podacima, pa je dobro koristiti ih za izdvajanje značajnih informacija iz velike količine podataka. Projekcija očuvanja lokaliteta (engl. *Locality Preserving Projection*, LPP) je predložena kako bi se uzorci transformisali u novi mali podprostor. Pritom, uzorci koji su bili susedni u originalnom prostoru, biće susedni i u novom prostoru. Tako je sačuvana lokalna struktura uzoraka. Međutim, podatke je teško rekonstruisati jer su osnovne funkcije, dobijene pomoću LPP metode, ne ortogonalne. Primenjuje se široko u aplikacijama za prepoznavanje uzoraka.

Predložena je metoda ortogonalne projekcije očuvanja lokaliteta (engl. *Orthogonal Locality Preserving Projection*, OLPP) koja ima istu teorijsku osnovu kao LPP metoda, samo su osnovne funkcije ortogonalne. Naziva se još i ortogonalna Laplasova matrica (engl. *Laplacianface*). Primenjuje se za izvlačenje najbitnijih karakteristika potrebnih za identifikaciju pečatiranih slika lica.

5.6. Primena vodenog pečata i steganografije u zaštiti multimodalnih biometrijskih podataka

Whitelam, Osia i Bourlai (2013) povećali su sigurnost multimodalnih biometrijskih podataka tako što su predložili višeslojnu strukturu, kombinovanjem tehnika vodenog pečata i steganografije. Za šifrovanje vodenog pečata i steganografske slike korišćena je amplitudska modulacija, zasnovana na radu (Kutter, 1997), koja više puta utiskuje informaciju u prostorni domen slike i ima široku primenu pri obradi signala u oblasti telekomunikacija.

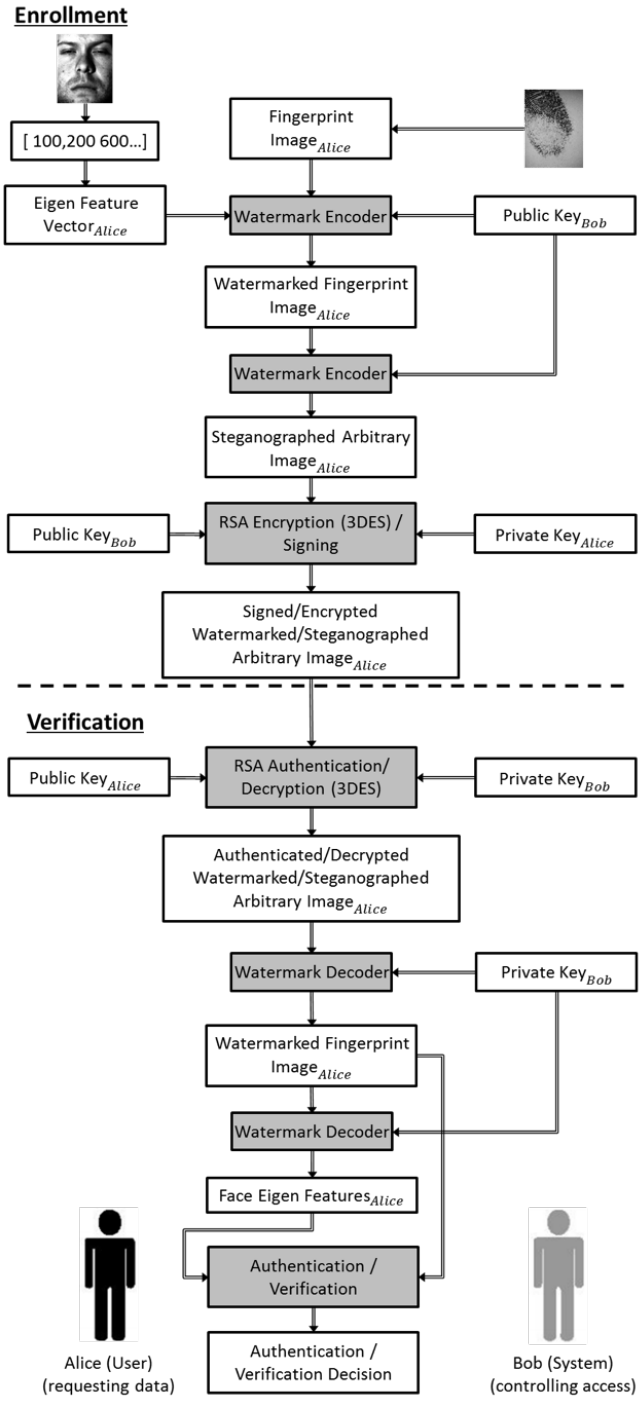
Svojstvene karakteristike lica se konvertuju u neprekidni niz bitova, koji se zatim utiskuju u sliku otiska prsta, primenom tehike šifrovanja dizajnirane specijalno za biometrijske vodene pečate. Nakon toga se, primenom steganografske tehnike, dobijeni pečatirani podaci otiska prsta/lica sakrivaju u proizvoljnu sliku koja nije bitna za biometriju ili forenziku (Slika 5.6.1).



Slika 5.6.1: Primena tehnike vodenog pečata i steganografije: (a) slika lica, (b) slika otiska prsta, (c) proizvoljna slika

Pečatirana slika otiska prsta/lica se pretvara u binarni niz, a zatim se koristi maksimalni intenzitet piksela da bi se odredio broj bitova potrebnih za steganografiju. Mesto utiskivanja se nasumično određuje preko sve tri boje kanala proizvoljne slike. Ovo daje dodatnu sigurnost korisniku ukoliko podaci budu kompromitovani, uzimajući u obzir da ne postoji indikacija da su biometrijski podaci prisutni [32].

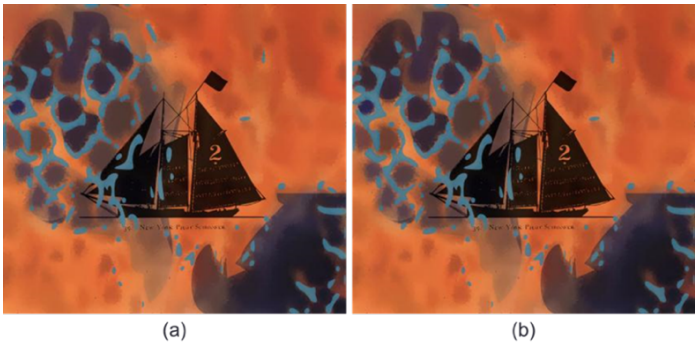
Strukturna šema sistema je široko primenljiva u slučajevima kada je potrebna biometrijska autentifikacija, kao što je centralizovano upravljanje identitetima ili POE (engl. *Point-of-Entry*) autentifikacija. Na slici 5.6.2 prikazana je faza upisivanja i verifikacije potencijalnog procesa autentifikacije.



Slika 5.6.2: Struktura sistema upisivanja i verifikacije podataka

Da bi pristupila zaštićenom resursu, Alisa šalje zahtev Bobu. Alisa obezbeđuje svoje autentifikacione podatke (otisak prsta i svojstvene karakteristike lica). Koristeći Bobov javni ključ za dobijanje lokacije vodenog pečata, svojstvene karakteristike lica se utiskuju u sliku otiska prsta. Dobijena pečatirana slika otiska prsta se može, pomoću istog javnog ključa, utisnuti u proizvoljnu

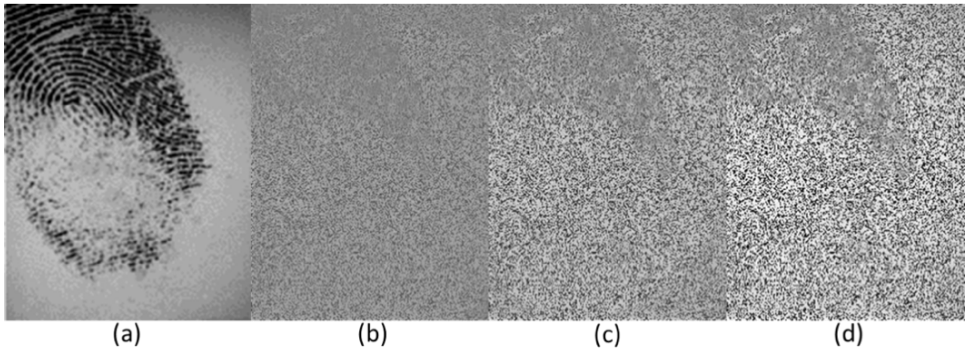
sliku. Na slici 5.6.3 prikazana je razlika između originalne i pečatirane proizvoljne slike, sa jačinom pečatiranja q=0.045 i ponavljanjem n=35.



Slika 5.6.3: (a) originalna slika, (b) slika sa utisnutim otiskom prsta kao vodenim pečatom

Koristeći RSA šifrovanje kroz PKI, Alisin privatni i Bobov javni ključ, steganografski biometrijski podaci su dodatno obezbeđeni. Podaci se zatim elektronski skladište u centralnu bazu podataka ili fizički na obezbeđen token (npr. lična karta). Sistem će, nakon toga, obraditi korisnikov identitet i šifrovane podatke.

Bob dešifruje steganografsku sliku koristeći Alisin javni ključ i njegov privatni ključ. Slika otiska prsta i svojstvene karakteristike lica se mogu izvući pomoću Bobovog privatnog ključa za dobijanje lokacije vodenog pečata. Izvučena slika otiska prsta i svojstvene karakteristike lica, mogu se iskoristiti za proveru autentičnosti podataka. Na slici 5.6.4 je prikazana razlika uzorka otiska prsta, primenom različite jačine šifrovanja (q).

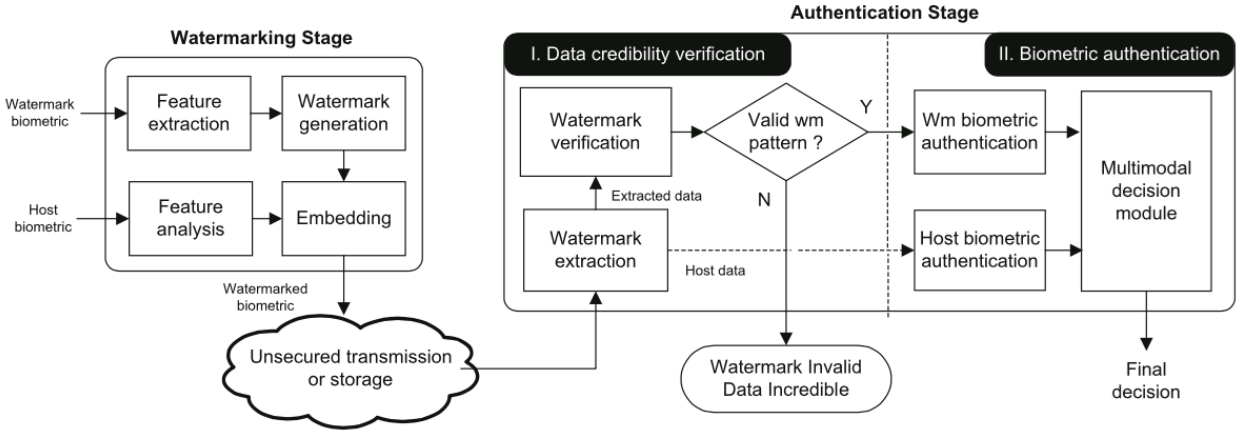


Slika 5.6.4: Razlike uzorka primenom različite jačine šifrovanja (a) originalna slika, (b) q=0.015, (c) q=0.030, (d) q=0.045

Primenom svojstvenih karakteristika lica i otiska prsta može se povećati bezbednost multimodalnog verifikacionog sistema. Sa završetkom procesa sistem će biti obezbeđen sa više slojeva autentifikacije (kriptografija, vodeni pečat, steganografija i multimodalna biometrijska verifikacija). Kriptografija obezbeđuje integritet podataka i neporecivosti porekla, kroz PKI. Za razliku od kriptografije, vodeni pečati i steganografija će omogućiti posebne slojeve za praćenje, jer dešifrovana slika ima vodeni pečat koji otkriva poreklo slike.

5.7. Primena dvostepene multimodale autentifikacije zasnovane na talasnoj kvantizaciji vodenog pečata za unapređenje bezbednosti biometrije

Ma, Li, Wang, Zhang i Huang (2012) su, radi povećanja sigurnosti i pouzdanosti biometrijskih sistema, predložili metodu vodenog pečata zasnovanu na dvostepenoj autentifikaciji (Slika 5.7.1). Tokom procesa prikupljanja podataka, karakteristike lica se utiskuju u sliku otiska prsta. Autentičnost unesenih podataka se utvrđuje proverom validnosti izvučenog vodenog pečata. Samo ukoliko su podaci autentični, sistem će preći u sledeću fazu autentifikacije, kada pečatirano lice služi kao dodatna informacija radi lakše biometrijske autentifikacije. U ovom procesu, predložena je metoda vodenog pečata zasnovana na talasnoj kvantizaciji, koja povećava robustnost uz relativno veliki kapacitet vodenog pečata [33].



Slika 5.7.1: Blok šema utiskivanja vodenog pečata zasnovana na dvostepenoj biometrijskoj autentifikaciji

Proverom validnosti izvučenog vodenog pečata, verifikuje se verodostojnost podataka. Na taj način se povećava otpornost sistema na zlonamerne napade kao što su neovlašćeni pristup i falsifikovanje. Za pouzdanu verifikaciju se može primeniti klasifikacija šablona (vodenog pečata) umesto pretraživanja baze, kao kod konvencionalnih vodenih pečata. Prisutnost vodenog pečata može da se otkrije pomoću detektora, koji će, u potpunosti, da uporedi izvučeni šablon sa svim uzorcima vodenog pečata u bazi podataka, kako bi pronašao onaj sa najvećim podudaranjem. Međutim, zbog prisustva šuma, malo je verovatno da će izvučeni vodeni pečat biti identičan originalnom.

Nakon što se uspostavi autentičnost podataka, kao dodatna informacija identitetu može da posluži vodeni pečat lica, kako bi se olakšala biometrijska autentifikacija. Međutim, vodeni pečat lica je izuzetno semplovana slika, te predstavlja veliki izazov primeniti je za identifikaciju. Kao rešenje za problem prepoznavanja vodenog pečata lica primenjena je metoda klasifikacije zasnovana na raštrkanom prikazu (engl. *Sparse Representation Based Classification*, SRC).

5.8. Vodeni pečati zasnovani na SDPQ metodi

Lin et. al (2008) je predstavio algoritam za slepe vodene pečate, zasnovan na značajnoj razlici kvantizacije talasnog koeficijenta (engl. *Significant Difference Quantization*, SDQ), koja je dala dobre rezultate u oblasti zaštite autorskih prava. U blok je grupisano svakih sedam nepreklapajućih talasnih koeficijenata host slike. Značajne koeficijente predstavljaju dva najveća koeficijenta u bloku, dok je njihova razlika značajna razlika. Maksimalni lokalni talasni koeficijent u bloku je kvantizovan, tako što je izvršeno poređenje vrednosti značajne razlike u bloku sa srednjom vrednošću značajne razike u svim blokovima. Koeficijenti su toliko kvantizovani da njihova značajna razlika, između bitova vodenog pečata 0 i 1, daje veliku energetsku razliku koja može da se upotrebi za izvlačenje vodenog pečata [34].

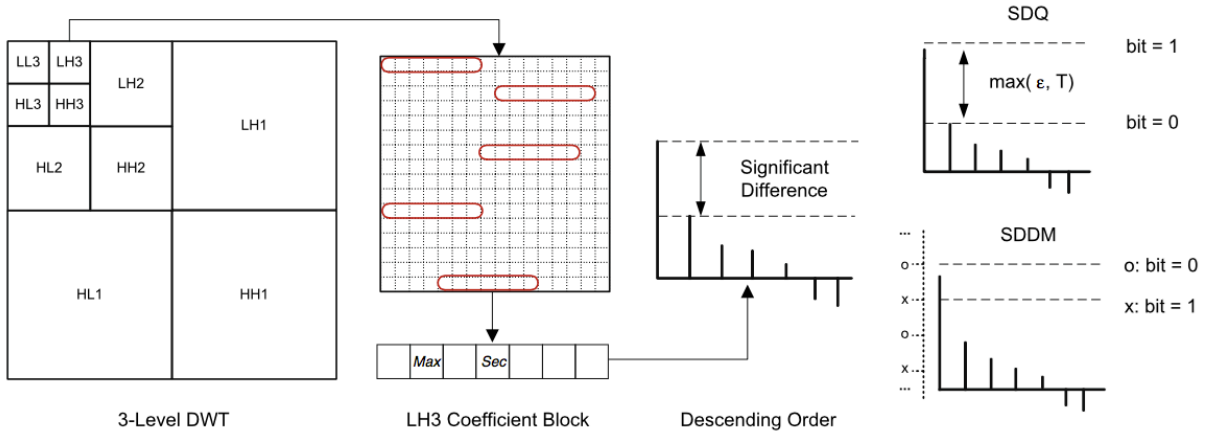
Tehnika utiskivanja u razložene blokove SDQ metode ima veliki kapacitet i obezbeđuje robustnost vodenog pečata. Uglavnom je pogodna za prirodne slike, jer su njihove vrednosti značajne razlike relativno male (~10-20), dok je kod slike otiska prsta srednja vrednost značajne razlike veća za oko deset puta. Međutim, izjednačavanje najveće i sledeće veće vrednosti u grupi, izazvaće veliku distorziju. Značajni DWT koeficijenti slike otiska prsta često ukazuju na lokalne varijacije struktura (grebeni ili jedinstvene tačke), pa bi velike promene uticale na diskriminišuće karakteristike host slike otiska prsta. Meerwald et al. (2009) je ukazao na problem grupisanja susednih koeficijenata u blokove, koji mogu omogućiti napadaču pristup lokacijama za utiskivanje.

Kako bi rešili ovaj problem, Ma, Li, Wang, Zhang i Huang (2012) su predložili šemu vodenog pečata zasnovanu na značajnoj razlici pariteta kvantizacije (engl. *Significant Difference Parity Quantization*, SDPQ). Značajna razlika se podešava pomoću tehnike diter modulacije, kako bi se utisnuo bit vodenog pečata (0 ili 1).

Proces utiskivanja vodenog pečata obuhvata:

1. **Razlaganje talasima** – Na host sliku se primenjuje razlaganje talasima na tri nivoa. Usvojen je talas CDF-9/7 za bolju uglađenost.
2. **Selekcija koeficijenata** – Koeficijenti, *LH3* i *HL3* podopsega, se nasumično mešaju po utisnutom tajnom ključu, grupišući koeficijente koji se ne preklapaju u blokove sa unapred definisanom veličinom. Nakon toga se dodeljuje jedan blok za svaki bit vodenog pečata.
3. **Utiskivanje vodenog pečata** – Za svaki bit vodenog pečata računa se vrednost značajne razlike odgovarajućeg bloka i kvantizuje njegova najveća vrednost.
4. **Inverzna talasna transformacija** – Oporavlja koeficijente vodenog pečata sa utisnutim tajnim ključem.

Autori, Ma, Wang, Li, Zhang i Huang (2014), primenili su šemu vodenog pečata zasnovanu na značajnoj razlici diter modulacije (engl. *Significant Difference Dither Modulation*), za rešavanje pomenutih problema i dalji napredak [35]. Na slici 5.8.1 je dat šematski prikaz SDQ i SDDM metode za utiskivanje vodenog pečata.



Slika 5.8.1: Prikaz SDQ i SDDM metode za utiskivanje vodenog pečata

5.9. Bezbednostni problemi biometrijskih vodenih pečata

Napadi na vodene pečate se mogu podeliti na:

1. **Neovlašćena detekcija** (engl. *Unauthorized detection*) – Napadač otkriva da određeni podaci sadrže vodeni pečat tj. da vodeni pečat prenosi tajnu informaciju skrivenu u host podatku. Ukoliko je tajna informacija izložena, sistem se smatra razbijenim. Ovakva vrsta napada obično se događa u steganografskim scenarijima.
2. **Neovlašćeno uklanjanje** (engl. *Unauthorized removal*) – Svrha ovog napada je da uništi vodeni pečat ili da ga učini nemogućim za detekciju. Napadač uklanja autorski znak legitimnog korisnika radi korišćenja/distribucije medijskih podataka bez autorizacije. Ovakva vrsta napada uglavnom se događa u zaštiti autorskih prava i DRM aplikacijama.
3. **Neovlašćeno izvlačenje** (engl. *Unauthorized extraction*) – Kod ove vrste napada, napadač će pokušati da izvuče tajne informacije vodenog pečata.
4. **Neovlašćeno utiskivanje** (engl. *Unauthorized embedding*) – Kod ove vrsta napada, napadač utiskuje legitiman vodeni pečat u lažne podatke, kako bi spajanjem napravio važeću kopiju, koja može da prođe verifikacioni sistem.

Vodeni pečat koristimo kao verodostojni token. Uzorak koji ima vodeni pečat je javno prepoznatljiv. Oštećenje ili odsustvo vodenog pečata učiniće autentifikaciju neuspešnom.

Bezbednost informacija vodenog pečata kod neautorizovanog izvlačenja, može biti zagarantovana šemom utiskivanja koja zavisi od ključa (engl. *Key-dependent embedding scheme*). Sekvence vodenog pečata se šifruju pre utiskivanja ili se nasumice izabere pozicija utiskivanja po tajnom ključu. Ukoliko napadač dođe do algoritma za izvlačenje, neće moći da dođe do informacije vodenog pečata, zato što je dodatno zaštićena tajnim ključem. U ovom slučaju je veoma bitno kakva se procedura koristi za održavanje tajnosti ključa, ali i da se kompromitovani ključevi zamene. Takođe, mogu se uvesti dodatni bezbednostni protokoli kao što su poverenje u treću stranu (engl. *Trusted Third Party*) ili šifrovanje javnih ključeva.

Problem falsifikovanja pečatirane slike otiska prsta, koja sadrži karakteristiku lica, se može rešiti, ukoliko se na skrivene podatke vodenog pečata primeni tehnika za zaštitu šablona (biometrijsko heširanje ili vremenski pečat). Bezbednost sistema može se podići na viši nivo kombinovanjem različitih tehnika.

6. ZAKLJUČAK

U ovom radu bavili smo se primenom digitalnog vodenog pečata radi dodatne zaštite biometrijskih podataka u biometrijskim autentifikacionim servisima. Takođe, ostvaren je doprinos u dodatnoj zaštiti privatnosti kod biometrijskih sistema koji obavljaju autentifikaciju bez čuvanja biometrije u bazi podataka. Polazeći od teorijskih osnova biometrije i digitalnih vodenih pečata, napravljen je detaljan pregled sa aktuelnim stanjem u oblasti biometrijskih vodenih pečata, koja primenjuje ove dve tehnologije i tako stvara novo područje za istraživanje.

Ovim radom ostvareni su sledeći doprinosi:

- pregled trenutnog stanja u oblasti biometrijskih podataka
- pregled trenutnog stanja u oblasti digitalnih vodenih pečata
- primena steganografskih tehnika i kriptografije
- pregled trenutnog stanja u novoj oblasti, poznatijoj kao „Biometrijski vodeni pečati“ sa uvidom u više naučno istraživačkih radova u kojima su predloženi različiti scenariji ili generičke šeme za kombinovanje biometrije i digitalnih vodenih pečata.

6.1. Predlog za budući rad

U budućem radu analiziraće se mogućnosti za razvoj sopstvenog rešenja koje će demonstrirati upotrebu ovog BDP sistema u modernim servisima autentifikacije zasnovanim na biometriji.

7. LITERATURA

[1] R. D. Kanphade, N. S. Narawade, „Robust Semi-Reversible Watermarking Using Pixel Averaging Method Against Geometric Attack“, *The IUP Journal of Telecommunications*, Vol. V, No. 1, pp. 46 – 55, 2013.

[2] R. D. Kanphade, N. S. Narawade, „Robust Reversible Watermarking Against Geometric Attack Using Geometric Transformation Correction Applied on Spatial Domain Methods“, *The IUP Journal of Telecommunications*, Vol. V, No. 3, pp. 47 – 56, 2013.

[3] M. Gupta, D. T. Gupta, V. Saxena, „A Wavelet-Based Watermarking Scheme for Color Images“, *The IUP Journal of Telecommunications*, Vol. V, No. 2, pp. 56 – 66, 2013.

[4] M. Veinović, S. Adamović, **Kriptologija I**, Univerzitet Sigidunum, Beograd, 2013.

[5] M. Milosavljević, S. Adamović, **Kriptologija II**, Univerzitet Sigidunum, Beograd, 2014.

[6] E. Leeuw, S. Fiscber, J. Tseng, J. Borking, **Policies and Research in Identity Management**, Springer, 2008.

[7] S. Paunović, D. Starčević, „Biometrijski sistemi za utvrđivanje identiteta“, INFOTECH 2013, Aranđelovac, 2013.

[8] I. Milenković, O. Latinović, U. Šošević, D. Simić, „Primena kriptografije u biometrijskim sistemima“, INFOTECH 2013, Aranđelovac, 2013.

[9] B. Popović, D. Ranđelović, M. Bunđur, „Izazovi vezani za privatnost i bezbednost prilikom upotrebe biometrike“, ZITEH '10, Beograd, 2010.

[10] Ž. Radmilović, „Biometrijska identifikacija“, Policija i sigurnost, god. 17 – br. 3-4/08, str. 159 – 180, MUP RH, Zagreb, 2008.

[11] CARNet CERT, LS&S (2006), CCERT-PUBDOC-2006-09-167, „Biometrija“, Revizija v1.1, Hrvatska Akademska Istraživačka Mreža, Zagreb, 2006.

[12] I. Fratrić, Doktorski rad, „Biometrijska verifikacija osoba temeljena na značajkama dlana i lica dobivenim iz video sekvenci“, Fakultet elektrotehnike i računarstva, Zagreb, 2011.

[13] S. Mesarović, Magistarska teza, „Multimodalni biometrijski sistemi“, Fakultet za poslovnu informatiku, Beograd, 2007.

[14] http://www.aware.com/resources/

[15] http://www.morpho.com/en

[16] D. Uljarević, M. Veinović, „Digitalna steganografija JPEG slika primenom DCT transformacije“, INFOTECH 2013 ICT Conference & Exhibition, Aranđelovac, 2013.

[17] V. Vučković, Doktorska disertacija, „Optimalna snaga žiga belog Gausovog šuma“, Matematički fakultet, Beograd, 2010.

[18] H. Šalković, Diplomsli rad br. 618, „Primjena digitalnog vodenog žiga u zaštiti vlasništva slika u digitalnom zapisu“, Fakultet elektrotehnike i računarstva, Zagreb, 2013.

[19] M. Petrović, **Osnovi televizije - Priručnik za laboratorijske vežbe**, Visoka škola elektrotehnike i računarstva, Beograd, 2010.

[20] P. Singh, R. S. Chadha, „A Survey of Digital Watermarking Techniques, Applications and Attacks“, *International Journal of Engineering and Innovative Technology*, Volume 2, Issue 9, pp. 165 – 175, March 2013.

[21] Nacionalni CERT, LSS, NCERT-PUBDOC-2010-08-310, „Digitalni vodeni žigovi“, Hrvatska Akademska Istraživačka Mreža, Zagreb, 2010.

[22] M. Topalović, Diplomski rad, „Digitalni vodeni žig“, Univerzitet Vitez, Travnik, 2012.

[23] M. Đuričkov, Master rad, „Antiforenzičke tehnike i alati“, Fakultet za informatiku i menadžment, Beograd, 2009.

[24] A. Samčović, G. Murić, „Primena tehnike digitalnog vodenog žiga u zaštiti vlasništva nad slikama“, Konferencija o bezbednosti informacija BISEC 2013, str. 64 – 69, Beograd, 2013.

[25] J. Tašić, Diplomski rad, „Primena digitalnih vodenih pečata radi zaštite digitalnih dokumenata i skrivanja tajnih informacija“, Fakultet za informatiku i računarstvo, Beograd, 2014.

[26] M. Popović, **Digitalna obrada slike**, Akademska misao, Beograd, 2006.

[27] J. S. Pan, H. C. Huang, L. C. Jain, **Intelligent Watermarking Techniques,** World Scientific, 2004.

[28] T. Hoang, D. Tran, D. Sharma, „Bit Priority-Based Biometric Watermarking“, *IEEE International Conference on Communications and Electronics*, pp. 191 – 195, 2008.

[29] M. Abdullah, S. Dlay, W. Woo, „Securing Iris Images with a Robust Watermarking Algorithm based on Discrete Cosine Transform“, *International Conference on Computer Vision Theory and Applications*, pp. 108 – 114, 2015.

[30] J. Lu, T. Qu, H. R. Karimi, „Novel Iris Biometric Watermarking Based on Singular Value Decomposition and Discrete Cosine Transform“, *Mathematical Problems in Engineering*, vol. 2014, Article ID 926170, 6 pages, 2014.

[31] P. Bhirud, N. Prabhu, „Secured Biometric Authentication using Visual Cryptography and Transforms“, *International Journal of Computer Applications*, vol. 77, no. 8, pp. 23 – 28, 2013.

[32] C. Whitelam, N. Osia, T. Bourlai, „Securing Multimodal Biometric Data through Watermarking and Steganography“, *IEEE International Conference on Technologies for Homeland Security*, pp. 61 – 66, 2013.

[33] B. Ma, C. Li, Y. Wang, Z. Zhang, D. Huang, „Enhancing Biometric Security with Wavelet Quantization Watermarking based Two-stage Multimodal Authentication“, International Conference on Pattern Recognition, pp. 2416 – 2419, 2012.

[34] W. Lin, S. Horng, T. Kao, P. Fan, C. Lee, Y. Pan, „An Efficient Watermarking Method Based on Significant Difference of Wavelet Coefficient Quantization“, *IEEE Transactions on Multimedia*, vol. 10, no. 5, pp. 746 – 757, 2008.

[35] B. Ma, Y. Wang, C. Li, Z. Zhang, D. Huang, „Secure multimodal biometric authentication with wavelet quantization based fingerprint watermarking“, In: *Multimedia Tools and Applications*, vol. 72, no. 1, pp. 637 – 666, Springer, New York, 2014.

[36] S. Ghouzali, „Watermarking Based Multi-biometric Fusion Approach“, C2SI 2015, LNCS, vol. 9084, pp. 342 – 351, Springer, Switzerland, 2015.