

**Fakultet za informatiku i menadžment
SAVREMENE INFORMACIONE TEHNOLOGIJE**

MASTER STUDIJE

Master rad

-ANTIFORENZIČKE TEHNIKE I ALATI-

MENTOR:
Docent, dr Gojko Grubor

KANDIDAT:
Đuričkov Manja
Br.ind.: M 9465/08

Beograd, decembar 2009

ANTIFORENZIČKE TEHNIKE I ALATI

Sažetak

Zbog čestih i mnogostrukih načina zloupotrebe sadržaja koji se pušta kroz Internet, digitalni forenzičar mora znati koje su najčešće zloupotrebe i na koji se način one mogu otkriti. Na Internetu se često mogu sresti dve tehnike sakrivanja poruke sa različitim namenom. Steganografija, tehnika sakrivanja poruka unutar različitih digitalnih formata, najčešće je krivično delo. Tajne poruke su ili uputstva za sprovođenje kriminalnih dela ili su same po sebi kriminalno delo (npr. dečija pornografija). Za razliku od steganografije, digitalni vodeni pečat, koji se ne može u potpunosti definisati kao zaštita od izvršenja krivičnog dela, za cilj ima dokazivanje počinjenog krivičnog dela. Detektovanjem i izvlačenjem digitalnog vodenog pečata na verodostojan način, forenzičar može dokazati da je određeni digitalni fajl u vlasništvu oštećene strane. Cilj forenzičara jeste da u oba slučaja detektuje prisustvo sakrivene poruke i na taj način dođe do validnih dokaza.

Ključne reči

Steganografija, steganoanaliza, digitalni vodeni pečat, zaštita autorskih prava, najmanje značajan bit, digitalna forenzika, antiforenziki alati, antiforenzicke tehnike.

ANITOFRENSIC TECHNIQUE AND TOOLS

Abstract

Often and multiple ways of abuse of contents which are staged through the Internet, cause that the digital forensic must know what are the most often abuses and what are the ways they can be discovered. We can often meet two techniques for hiding message with different assignment on the Internet. Steganography, the technique for hiding messages within different digital format, is generally the most often criminal act. Secret messages are either the directions for practicing a criminal act or a criminal act itself (e.g. child pornography). Unlike steganography, digital watermark cannot be defined as the protection from a criminal act. Digital watermark rather has an aim to prove certain criminal act. By detection and extraction of the digital watermark in an authentic manner, a forensic can prove that a certain digital file is an ownership of the injured party. The aim of forensics is to detect presence of hidden message and reach the valid evidence that way.

Key words

Steganography, steganoanalysis, digital watermark, protect copyright, least significant byte, digital forensic, antiforensic tools, antiforensic technique.

SPISAK SLIKA

Slika 1.- <i>Naska</i> linije u Peru	11
Slika 2.- <i>Geoglyph</i> u selu <i>Cerro Sombrero</i> , arheološko nalazište <i>Arica, Chile</i>	11
Slika 3.- „Medveđa šapa“, šara na jorganu	12
Slika 4.- Opšti proces steganografije - stegosistem	14
Slika 5.- Klasifikacija steganografskih tehnika	15
Slika 6.- Jednostavna pulsno kodna modulacija	18
Slika 7.- RGB kocka	19
Slika 8.- U prozoru za izbor boje prikazani su nivoi RGB boje za odabranu boju	20
Slika 9.- Odnos steganografije i steganoanalize	26
Slika 10.- Ugrađivanje vodenog pečata	36
Slika 12.- Slika sa logom	Error! Bookmark not defined.
Slika 13.- Slika bez logoa	40
Slika 14.- Odnos između šifrovanja i kontrole kopiranja na bazi vodenog pečata	42
Slika 15.- Jednostavni primer audio vatermarkinga metodom proširenog spektra	50
Slika 17.- Proces ugrađivanja za umetanje predeformisanog vodenog pečata	53
Slika 18.- Ilustracija napada eliminisanjem i maskiranjem	58
Slika 19.- Prikaz značajne razlike između napada eliminisanjem i maskiranjem	58
Slika 20.- Tajna poruka „vojska 1.jpg“	64
Slika 21.- Izgled prozora wbStego programa u poslednjem koraku	64
Slika 22.- Nosilac tajne poruke .bmp formata	65
Slika 23.- Steganografski medijum .bmp formata	65
Slika 24.- Razlika u bitovima između slike „Water lilies.bmp“ i „Vodeni ljiljan.bmp“	66
Slika 27.- Upoređivanje histograma slika „Vodeni ljiljani.bmp“ i „Water lilies.bmp“	67
Slika 25.- Histogram slike „Water lilies.bmp“	66
Slika 26.- Histogram slike „Vodeni ljiljan.bmp“	66
Slika 28.- Hi-kvadrat napad na sliku „Vodeni ljiljani.bmp“	69
Slika 29.- Koraci sakrivanja tajne poruke alatom <i>Camouflage</i>	71
Slika 30.- Nosilac tajne slike .jpg formata	71
Slika 31.- Steganografski medijum .jpg formata	71
Slika 32.- Razlika u bitovima između slike „Water lilies.jpg“ i „Vodeni ljiljani.jpg“	72
Slika 33.- Upoređivanje histograma slika „Vodeni ljiljani.jpg“ i „Water lilies.jpg“	73
Slika 34.- Prikaz detekcije potpisa steganografskog programa	73
Slika 35.- Sakrivanje nasumično odabrane tajne poruke u nasumično odabranog stegonosioca	74
Slika 36.- Promena bitova zbog dešifrovanja	75
Slika 37.- Koraci za izvlačenje tajne poruke novom šifrom	75

SPISAK TABELA

Tabela 1.- Klasifikacija antiforezičkih metoda	9
Tabela 2.- Neki od uobičajenih digitalnih audio formata (Fries and Fries 2000)	18
Tabela 3.- Operativna tabela za tri prikazana <i>watermarking</i> scenarija	55
Tabela 4.- Operativna tabela za dve kategorije primene <i>watermarking</i> : privatni i javni	55
Tabela 5.- Osobine fajlova .bmp ekstenzije	65
Tabela 6.- Osobine fajlova .jpg ekstenzije	72

SPISAK DIJAGRAMA

Dijagram 1. – Godišnji broj listova izdatih na temu steganografije i DVP na osnovu IEEE ..	33
--	----

SADRŽAJ

ANTIFORENZIČKE TEHNIKE I ALATI	2
Sažetak	2
Ključne reči	2
ANITOFORENSIC TECHNIQUE AND TOOLS	2
Abstract	2
Key words	2
SPISAK SLIKA	3
SPISAK TABELA	3
SPISAK DIJAGRAMA.....	3
 1. METODOLOGIJA IZRADE MASTER RADA	6
Uvodne napomene i obrazloženje rada.....	6
Predmet rada.....	6
Cilj rada.....	6
Metodologija naučnog istraživanja.....	7
Metode i tehnike istraživanja	7
Istraživačke hipoteze	8
 2. ANTIFORENZIKA I ANTIFORENZIČKE TEHNIKE	9
ANTIFORENZIKA	9
STEGANOGRAFIJA I STEGANOANALIZA	10
2.1.1. Steganografija kroz istoriju	10
2.1.2. Savremena steganografija	13
2.1.3. Klasifikacija steganografskih tehnika	15
2.1.4. Kompjuterska steganografija	16
2.1.4.1. Specijalna svojstva kompjuterskih formata.....	16
2.1.4.2. Preobilje informacija u audio i video digitalnim signalima	16
2.1.5. Steganografija u digitalnim formatima	17
2.1.5.1. Steganografija u video formatima	17
2.1.5.2. Steganografija u audio formatima	17
2.1.5.3. Steganografija u dokumentima	19
2.1.5.4. Steganografija u slikama	19
2.1.6. Ugrađivanje vodenih pečata u sliku	21
2.1.6.1. Metodi za ubacivanje vodenog pečata u prostornom domenu	22
2.1.6.2. Metodi za ubacivanje pečata u transformacionom domenu	23
2.1.7. Metodi prenošenja informacija u digitalnim formatima	23
2.1.7.1. LSB supstitucija.....	24
2.1.8. Detekcija steganografije.....	25
2.1.8.1. Steganoanaliza	25
2.1.9. Tipovi napada na steganografske sisteme	29
2.1.10. Steganografski programi.....	30
2.1.11. Alati za detekciju steganografije	31
DIGITALNI VODENI PEČAT	32
2.1.12. Digitalni vodeni pečat kroz istoriju	32
2.1.13. Značaj DVP-a.....	34
2.1.14. Primena i osobine DVP-a	34
2.1.15. Primena DVP-a	36
2.1.15.1. Monitoring emitovanja	36

2.1.15.2.	Identifikacija vlasnika.....	38
2.1.15.3.	Dokazivanje vlasništva	38
2.1.15.4.	Praćenje transakcija (otisak prsta).....	39
2.1.15.5.	Autentifikacija sadržaja	40
2.1.15.6.	Kontrola kopiranja.....	41
2.1.15.7.	Kontrola uređaja.....	43
2.1.15.8.	Unapređivanje zaostalog.....	43
2.1.16.	Osobine sistema DVP-a.....	44
2.1.16.1.	Delotvornost ugrađivanja.....	44
2.1.16.2.	Verodostojnost	44
2.1.16.3.	Korisni podaci (data payload)	45
2.1.16.4.	Detekcija na slepo ili poznato	45
2.1.16.5.	Lažno pozitivni odgovori (ocene)	45
2.1.16.6.	Otpornost.....	46
2.1.16.7.	Sigurnost	46
2.1.16.8.	Šifre i ključevi digitalnog vodenog pečata.....	46
2.1.16.9.	Promene i višestrukost vodenog pečata.....	47
2.1.16.10.	Trošak	48
2.1.17.	Sigurnost i otpornost DVP-a.....	48
2.1.17.1.	Otpornost DVP-a.....	49
2.1.17.2.	Sigurnost DVP-a.....	54
2.1.17.3.	Pretpostavke o suparniku	59
2.1.17.4.	Sprečavanje napada i bitniji napadi na sigurnost sistema DVP-a	61
3.	ISTRAŽIVAČKI RAD: STUDIJE SLUČAJA.....	61
3.1.	Antiforenzički alat <i>Evidence Eliminator</i>	61
3.2.	Studija slučaja I: Detekcija i izvlačenje tajne poruke iz <i>.bmp</i> formata.....	64
3.3.	Studija slučaja II: Detekcija i izvlačenje tajne poruke iz <i>.jpg</i> formata	70
4.	ZAKLJUČCI.....	76
5.	LITERATURA	78

1. METODOLOGIJA IZRADE MASTER RADA

Uvodne napomene i obrazloženje rada

Kako je forenzika napredovala i razvijala se kao istraživačka disciplina, antiforenzike tehnike i alati razvijali su se uporedo sa njom. Ne postoji jedinstvena definicija antiforenzičke tehnike, ali se može generalizovati kao bilo koji pokušaj da se kompromituje dostupnost ili korisnost dokaza u forenzičkom procesu, kao i da se sam taj proces oteža, ili čak onemogućuje.

Osnovni ciljevi antiforenzičke su:

- Izbegavanje detekcije
- Remećenje sakupljanja dokaza
- Povećanje vremena istraživanja
- Bacanje sumnje na forenzički izveštaj ili svedočenje
- Korišćenje alata za napad na istražitelje ili organizaciju
- Obaranje alata kako se ne bi ustanovilo njegovo prisustvo i
- Ne ostavljanje traga da je antiforenziki alat korišćen.

Antiforenzika se može podeliti u više podoblasti:

- Sakrivanje podataka
- Brisanje podataka prepisivanjem (engl.- *wiping*)
- Uništavanje tragova i
- Napad protiv alata kompjuterske forenzike.

Podela antiforenzičke se dalje može vršiti prema njenom usmerenom delovanju na dokaze:

- Uništavanje dokaza
- Sakrivanje dokaza
- Eliminisanje izvora dokaza
- Falsifikovanje dokaza

U ovom radu će se ukratko predstaviti navedene podoblasti antiforenzičke i njena podela prema delovanju na dokaze, dok će se detaljnije razmatrati tehnika zastupljena u podoblasti sakrivanja podataka – steganografija, i digitalni vodeni pečat kao jedna od tehnika koja je često meta napada falsifikovanjem. Pored toga, predstavljen će biti antiforenziki alat *Evidence Eliminator*TM zbog njegove široke primene i zbog toga što je on namenski pisan i dizajniran da uništi potencijalne dokaze.

Predmet rada

Predmet rada je istraživanje antiforenzikičkih tehnika: steganografije i digitalnog vodenog pečata, i alata za otežavanje forenzičke istrage.

Ciljevi rada

Naučni cilj ovog rada je sistematizacija metoda i tehnika steganografije i steganoanalize, definisanje i približavanje terminologije potrebama korisnika, kao i sistematizacija oblasti primene digitalnog vodenog pečata i njegovih osobina i upoređivanje otpornosti i sigurnosti vodenog pečata.

Konkretan cilj ovog rada je predstavljanje steganografije i njenih tehnika, sa namerom da se definišu poznati načini sakrivanja tajnih podataka, a koji se mogu zloupotrebiti u elektronskom okruženju od strane kriminalaca i detekciju skrivenih poruka u različitim tipovima elektronskih formata. Pored toga će se kroz oblasti primene digitalnog vodenog pečata predstaviti mogućnosti njegove upotrebe u svrhe dokazivanja počinjenog kompjuterskog kriminala i njegov potencijal za zaštitu intelektualne svojine u elektronskom okruženju.

Metodologija naučnog istraživanja

Naučno istraživanje predstavlja sistematski, kritički, kontrolisani i ponovljivi proces u kom stičemo nova znanja, koja su neophodna za identifikovanje, određivanje i rešavanje naučnih problema. Principi kojima se treba rukovoditi u tom procesu su:

Sistematičnost - dobra uređenost istraživanja i obezbeđivanje prirodnog i logičkog sleda procesa

Kontrolisanost - sprovođenje istraživanja u što je moguće boljim i nadziranim uslovima, kako bi se isključile alternativne mogućnosti

Kritičnost - sve važne tvrdnje o pojavama, procesima, odnosima i svojstvima moraju se ozbiljno, iskreno i strogo procenjivati, proveravati i obrazložiti.

Osnovne podele naučnog istraživanja su sledeće:

- Prema prirodi istraživanja (teorijska i empirijska)
- Prema cilju istraživanja (fundamentalna i primenjena)
- Prema funkciji istraživanja (eksplorativna i usmerena proveravanju hipoteza).

Obzirom na temu rada i činjenicu da se radi o materiji koja kod nas u državi ne izaziva veliko interesovanje, koja se može okarakterisati kao borba protiv najčešće sprovedenih kriminalnih aktivnosti na Internetu, za izradu rada se uglavnom koriste fundamentalna i primenjena istraživanja. Fundamentalna istraživanja radi sticanja novih znanja o ovoj oblasti, a primenjena istraživanja radi sticanja novih znanja i rešavanja određenih problema u ovoj naučnoj oblasti.

Na početku istraživanja potrebno je precizno identifikovati problem koji istražujemo. U ovom slučaju, problem definišemo kao kompjuterski incident koji se dogodio i za koji nam je potrebno znanje o antforenzičkim tehnikama i alatima kako bismo ga identifikovali. Takođe, definišaćemo cilj našeg istraživanja, kao proveru određenih teorija i delova teorija u digitalnoj forenzici.

Istraživanje se sastoji iz sledećih faza:

1. pripremne faze, teorijskog karaktera
2. prikupljanja i obrade podataka
3. interpretacije rezultata i izvođenja zaključaka.

Metode i tehnike istraživanja

Metod predstavlja način, put, kojim smo istraživanjem došli do određenih saznanja, otkrili i izložili određenu naučnu istinu, koja se primenjuje u nekoj nauci, u ovom slučaju digitalno-forenzičkoj. Jedna od podela metoda je:

- Posebni naučni metodi i naučni postupci (analitičko-sintetički metod, metodi apstrakcije i konkretizacije, metodi generalizacije i specijalizacije, metodi klasifikacije, metodi indukcije, dedukcije kao metoda saznanja i dijalektičko jedinstvo indukcije i dedukcije)
- Opšti naučni metodi (statistička metoda, metoda modelovanja i analitičko-deduktivna metoda)
- Osnovni opšti metodi društvenih nauka (pozitivistički metod, metod razumevanja, komparativni metod, metod idealnih tipova, metodološki funkcionalizam i strukturalizam i dijalektički metod).

Metodi korišćeni u radu na ovom istraživanju su: analitičko-sintetički i logički.

Eksperimentalni metodi su oni koji se mogu upotrebiti u istraživanju predmeta koji su podobni za istraživanje eksperimenta. U njih svakako spadaju metodi kojima se može ostvariti neposredan fizički kontakt sa predmetom - realnom stvari. To su analiza i sinteza, apstrakcija i konkretizacija i indukcija.

Pod sintetičkim (sintetizujućim) osnovnim metodima podrazumevamo one koji se zasnivaju na sintezi, te čiji su metodski postupci razni oblici primene sinteze, odnosno postupaka spajanja, pripajanja, povezivanja, objedinjavanja itd.

Sinteza, po definiciji, jeste spajanje više činilaca u jednu celinu. Kao osnovni metod naučnih saznanja sinteza je shvatanje - saznanje složenih celina preko njihovih pojedinačnih i posebnih delova, njihovim spajanjem, tj. njihovim stavljanjem u razne moguće odnose i veze.

Tehnike istraživanja predstavljaju sistematsko i svrsishodno jedinstvo postupaka i instrumenata. Međutim, ovaj deo naučnog metoda podrazumeva: ocenu, sređivanje, obradu podataka i zaključivanje na osnovu njih. U tom pogledu postoji povezanost i međuzavisnost između metoda prikupljanja i metoda obrade podataka. Sa aspekta nauke podaci, odnosno dokazni materijali, sastoje se od informacija do kojih istraživač može da dođe.

Istraživačke hipoteze

Osnovna hipoteza rada

Zbog široke dostupnosti Interneta i raznih programa za obradu audio, video, slikovnog ili tekstualnog formata, otvara se mogućnost za masovno falsifikovanje istih, kao i mogućnost da se kroz mrežu puštaju sadržaji koji nose tajne poruke. Upotrebom odgovarajućih antiforenzičkih alata i tehnika oba kriminalna dela se mogu sprovesti tako da budu teško detektibilna.

Generalna hipoteza

Pretpostavka od koje polazimo u ovom istraživanju je da se kompjuterski incident dogodio i da je neophodno pribaviti dokaze koji bi bili validni u sudskom postupku, pridržavajući se procedura digitalne forenzike.

Posebna hipoteza

Poznavanjem i upotrebom odgovarajućih forenzičkih alata možemo na validan način dokazati da su na određenom računaru, sa Windows operativnim sistemom, vršena određena kriminalna dela.

Pojedinačna hipoteza

Kao pojedinačnu hipotezu, uzećemo pretpostavku da je na računaru izvršena povreda intelektualnih prava i da je isti računar korišćen za postavljanje slika sa tajnim sadržajem na određenom sajtu. Na istom računaru se nalaze programi koji ukazuju na to da vlasnik koristi računar u nelegitimne svrhe falsifikovanja kao i program *Evidence Eliminator*TM. Upotrebom odgovarajućeg alata možemo prikupiti validne dokaze o izvršenim prestupima.

Radna hipoteza:

Steganografija i digitalni vodeni pečat, kao antiforenzičke tehnike, mogu se koristiti u nelegalne svrhe.

Kapacitet steganografskih tehnika za sakrivanje informacija u uobičajene, svakodnevne elektronske i fizičke sadržaje, može se iskoristiti za sakrivanje nedozvoljenog sadržaja, kao što su pornografske slike ili za umetanje teksta s ciljem da se tajno sprovede kriminalno delo.

Zbog mnogobrojne primene digitalnog vodenog pečata veliki deo sadržaja koji se pušta kroz saobraćaj na internet može se obeležiti na takav način da bude nevidljiv i neodvojiv od fajla u koji je ubačen, ali često pečat nije dovoljno jak da preživi određene deformacije i na taj način se uništava. Ovim postupkom pruža se mogućnost falsifikovanja dela zaštićenih vodenim pečatom što predstavlja kriminalni akt.

2. ANTIFORENZIKA I ANTIFORENZIČKE TEHNIKE

ANTIFORENZIKA

Kao što je pomenuto, ne postoji jedinstvena definicija antiforenzike. Ona je relativno skoro prepoznata kao legitimno polje proučavanja i iz tog razloga postoji veliki broj definicija. Jedna od široko prihvaćenih definicija dolazi od Dr. Marka Rodžersa¹ sa Purdu univerziteta. On koristi tradicionalni „mesto zločina“ pristup kako bi definisao antiforenziku: „Pokušaj da se negativno utiče na postojanje, značenje i/ili kvalitet dokaza sa mesta zločina, ili otežavanje, čak onemogućavanje, analize i ispitivanje dokaza.“ Skraćenu definiciju dao je Skot Berinato u svom članku, Napredak antiforenzike: „Antiforenzika je više od tehnologije. Ona je kriminalni pristup koji se može posmatrati na sledeći način: Otežajte im da vas pronađu i onemogućite da dokažu da su vas oni pronašli“.

Peron i Legari² definišu antiforenziku kao pokušaj da se...“ograniči identifikacija, prikupljanje, upoređivanje i validacija elektronskih podataka“ kako bi se otežala kriminalna istraga. Grugq definiše antiforenziku kao...“pokušaj da se ograniči količina i kvalitet forenzičkih dokaza“. S obzirom na to da nijedna od ovih definicija nije kompletna, iz njih bi mogla da se izvede opšta **definicija**: Antiforenzika predstavlja bilo koji pokušaj da se kompromituju raspoloživost i korisnost dokaza u forenzičkom procesu.

Kompromitovanje dostupnosti dokaza uključuje bilo koji pokušaj sprečavanja dobijanja dokaza, sakrivanje postojećih dokaza ili bilo koju drugu manipulaciju dokazima kako bi se osiguralo da oni ne budu dostupni istražiteljima. Korisnost može biti kompromitovana brisanjem samih dokaza ili uništavanjem njihovih integriteta.

Opšta klasifikacija antiforenzičkih metoda se može sistematizovati iz podela od strane Rodžersa i Perona i ona je predstavljena u tabeli br.1.

Tabela 1.- Klasifikacija antiforenzičkih metoda

Naziv	Uništavanje dokaza	Sakrivanje dokaza	Eliminisanje izvora	Falsifikovanje
MACE promena	Pražnjenje MACE informacija ili prepisivanje sa nekorisnim podacima			Prepisivanje sa podacima koji obezbeđuju zbunjujuće informacije istražiteljima
Uklanjanje/prepisivanje fajlova	Prepisivanje sadržaja sa beskorisnim podacima	Brisanje fajlova		
Enkapsulacija podataka		Sakrivanje smeštanjem fajlova unutar drugih fajlova		
Krađa naloga (Account hijacking)				Dokaz je kreiran tako da izgleda kao da je druga osoba učinila prekršaj
Bomba slika/fajl				Dokaz je kreiran sa pokušajem da se kompromituje analiza slike
Onemogućavanje upisivanja			Informacije o aktivnostima	

¹ Rogers M. Anti-forensics, 2005. [43]

² Peron CSJ, Legary M, 2005.[40]

			nikada se ne snimaju	
--	--	--	-------------------------	--

STEGANOGRAFIJA I STEGANOANALIZA

2.1.1. Steganografija kroz istoriju

Džon Trithemius (1462-1516) bio je opat Nemačkog porekla. On je napisao „Steganografija: umetnost koja zahteva otkrivanje skrivenog pisanja misaonim aktivnostima čoveka³.“ Opisivao je steganografiju kao metod za komuniciranje sa dušom⁴. Objavljena kao trilogija na latinskom, prva dva dela njegovog rada su očigledno jedna od prvih knjiga koje opisuju kriptografske metode za sakrivanje poruka pisanjem. Treći deo trilogije je površna knjiga okultne astrologije. Treća knjiga sadrži tablice sa brojevima.

Dva istraživača Dr. Tomas Ernst i Dr Džim Rids⁵ su bili ubeđeni da treći tom sadrži sakriveni kod.

Dr. Ernst, u toku diplomskih studija na Univerzitetu u Pitsburgu, objavio je rad od 200 strana, ali je tek kada je 1996. godine objavljen članak na nemačkom jeziku, u nemačkom žurnalu *Daphnis*, privukao neznatnu pažnju.

Dr Rids, matematičar u AT&T⁶ laboratoriji nezavisno je počeo da istražuje treći tom. U toku istraživanja *Trithemius*-ovog rada, otkrio je rad Dr. Ernsta.

Ova dva istraživača su otkrili u relativno kratkom roku da treći tom sadrži skrivene poruke. Poruka je sadržana u tabeli koja je privlačila najmanju pažnju. Jedna poruka je bila sledeće sadržine „Brza braon lisica preskače lenjog psa.⁷“ Druga poruka je glasila „Nosilac ovog pisma je varalica i lopov. Čuvajte se od njega. On hoće nešto od vas.⁸“ Treća poruka je početak 23. psalma.

Steganografija svakako nije prvi primer skrivenog pisanja. Postoji mnogo primera iz istorije koji služe za ilustraciju želje da se sakrije poruka ili neki drugi tip inteligencije od drugih.

Kraljica Marija od Škotske⁹ je koristila kombinaciju kriptografije i steganografije da sakrije pisma. Ona je svoja pisma krila u rupi za zapušavanje bureta piva, koje je neometano ulazilo i izlazilo iz njenog zatvora.

Drugi vidovi steganografije nisu bili limitirani uobičajenim pisaćim materijalima. Jedan od njih podrazumeva velike crteže na zemlji načinjenih određenim redosledom ređanja kamenja ili posipanja zemlje u određenom obliku, ili tako što se uklanjala zemlja u određenom obliku ne bi li se formirala željena slika¹⁰. Primer je prikazan na slici 2.

Jedan od takvih primera su Naska linije u Peru¹¹. Na suvoj ravni je izgrebano više od 80 km linije između dva grada Naska i Palpe. Te jednostavne linije formiraju oblike majmuna, guštera, paukova itd. Ove linije se mogu slobodno videti, ali mnoge od njih su vidljive tek iz vazduha. Primer je prikazan na slici 1. Smatra se da su ove linije nastale između 200. godine pre Hrista i 700. godine posle Hrista.

³ Najpribližniji prevod do kog je moglo da se dođe, original glasi : “*Steganographia:hoe est ars per occultam scripturam animi sui voluntatem absentibus aperiendi certa.*”

⁴ Trithemius, Johannes [50]

⁵ Kolata, Gina [36]

⁶ **AT&T Inc.** je najveći provajder u Americi za lokalne i dalekoudaljene telefonske servise i DSL Internet pristupe.

⁷ Prevod odgovara originalnoj latinskoj poslovice.

⁸ Prevod odgovara originalnoj latinskoj poslovice.

⁹ The Science of Secrecy, Steganography [48]

¹⁰ Ovaj način crtanja po zemlji naziva se *Geoglyph*

¹¹ [Wikipedia \[29\]](#)



Slika 1.- Naska linije u Peruu



Slika 2.- Geoglyph u selu Cerro Sombrero, arheološko nalazište Arica, Chile

Herodot je u 5. veku pre rođenja Hrista brijao glave nosiocima poruka, pisao je ohrabrujuće poruke Aristagorasu iz Mileta, koje su podsticale na revolt protiv kralja Persije.

Nakon što glasniku poraste kosa, on biva otpremljen primaocu. Kada bi glasnik stigao na predodređeno odredište, glava bi mu ponovo bila obrijana i na taj način bi se došlo do skrivene poruke.

Još jedan od primera je pisanje poruka na svili, koja bi se nakon toga prenela na kuglicu i zatim bivala prekrivena voskom. Glasnik bi nakon toga progutao voštanu kuglicu. Način obnove skrivene poruke nije opisan u poznatim izvorima, ali se može logično rekonstruisati.

480. godine pre Hrista Grk po imenu Demaratus je poslao Spartancima poruku upozorenja o neizbežnoj invaziji Kserksa. Herodot opisuje metod koji je koristio Demarat¹²: „Kako je opasnost od otkrivanja bila velika, postojao je samo jedan način na koji je mogao da pošalje poruku preko: tako što je sa drvene table strugao vosak, zatim ispisivana na njemu poruka šta Kserks planira da uradi, a onda je poruka sakrivana ponovo voskom. Na ovaj način table, naizgled čiste, ne bi prouzrokovale probleme sa stražarima duž puta...“.

Podataka o drugim ranim radovima na steganografiji i kriptologiji mogu se pronaći na web strani koju je postavio Fabian Petitcolas¹³.

U novijoj istoriji, neke od steganografskih metoda korišćene su tokom Drugog svetskog rata¹⁴.

Mikrotačke razvijene od strane nacista su delovi mikrofilma, napravljene pod velikim uveličanjem, najčešće preko 200 puta. Ove tačke mogu sadržavati stranice informacija, slika itd. Nacisti su, takođe, upotrebljavali nevidljivo mastilo i bezšifarnu tehniku¹⁵. Bezšifarna tehnika (ili kodiranje) se koristi da se sakrije jedna poruka u drugu bez korišćenja komplikovanog algoritma. Jedan od najčešće citiranih primera je poruka poslata od nacističkih špijuna i glasi:

“President's embargo ruling should have immediate notice. Grave situation affecting international law. Statement foreshadows ruin of many neutrals. Yellow journals unifying national excitement immensely.”

“Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blocade issue affects pretext for embargo on by products, ejecting suets and vegetable oils.,,

¹² Singh Simon [47]

¹³ Petitcolas Fabien A. P. [41]

¹⁴ “Hidden in Plain Sight-Steganography”, Izdanje 2, Jun 1998 [29]

¹⁵ Bezšifarna tehnika je opisana na strani 16.

Nemačka ambasada u Vašingtonu, poslala je ovu poruku u telegramu svom glavnom štabu u Berlinu tokom I svetskog rata¹⁶. Čitajući prvo slovo svake reči u prvoj poruci ili svako drugo u svakoj reči u drugoj poruci dobićemo sledeći sakriveni tekst:

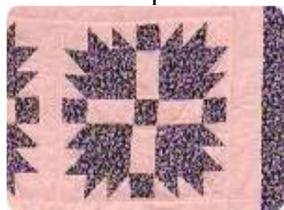
„Pershing sails from N.Y. June 1.“

Još jedan od primera steganografije uključuje upotrebu Kardano rešetke¹⁷. Ovaj uređaj, nazvan po izumitelju Girolami Kardanu, vrlo je jednostavan poput papira sa rupama usečenim u njemu. Ako želimo da dodemo do tajne poruke jednostavno se preko štampanog teksta postavlja rešetka.

U tehnikama srodnim Kardanovoj rešetki, klasične stenografske tehnike uključuju tekst napisan sitnim rupama izbušenim iglom i preko tog teksta se piše nov tekst sa penkalom.

Ovo je dokaz da je pre Civilnog rata u SAD postojao metod za dostavljanje tajnih poruka robovima kako bi im se pomoglo u bekstvu¹⁸. Koristeći razne šare u prekrivačima, koji su obično visili sa prozora da bi se sušili, poruke su bile prosleđivane robovima, podržavajući ih u njihovim naporima za slobodom.

Jedan od takvih primera šara je Medveda šapa.



Slika 3.- „Medveda šapa“, šara na jorganu¹⁹

Naučni pristup izučavanja steganografije praktično je započet 1983²⁰.

Do 11. septembra 2001. godine, steganografija se smatrala bezopasnom. Odjednom, posle više od dve hiljade godina postojanja postala je predmet opšteg interesovanja. Za njenu upotrebu zainteresovala se i Vlada najrazvijenije zemlje sveta SAD. Zbog mogućnosti opšte upotrebe, svojstva maskiranja, mogućnosti korišćenja u oblasti industrijske špijunaže, čini je interesantnom i za poslovni svet.

Steganografija je postala nesumnjivo sredstvo tajne razmene informacija između članova terorističkih grupa i organizacija. Analizirajući efekte terorističkih akcija, po metodama izvođenja i primenjenim sredstvima, nedvosmislen je zaključak da je, u smislu strategijskog iznenađenja, najveći doprinos dala steganografija kao sredstvo planiranja i operativnog delovanja. Teroristi Al Kaide organizovali su i izvršili napad na Svetski trgovinski centar i Pentagon komunicirajući putem nekoliko pornografskih Web sajtova. Plan terorističkog napada, u obliku šaljivih komentara, bio je „utisnut“ u slike koje su prenošene putem Interneta. Iako naizgled zastareo i naivan, steganografski metod prenosa poruka se pokazao krajnje efikasan. Bezbednosni sistem SAD je bio potpuno nemoćan. Teroristi su nadmudrili eksperte i američke bezbednosne agencije, bez obzira što je i napad na američku ambasadu u istočnoj Africi 1998. godine bio organizovan na isti način. U februaru 2001. godine, u američkom časopisu „USA Today“ pojavila su se dva članka u kojima su iznesene pretpostavke da bi Bin Laden i njegova teroristička organizacija Al Kaida mogli iskoristiti steganografiju za planiranje i izvršenje terorističkih napada preko sajta za sport i razonodu.²¹ Odmah posle terorističkih napada na Svetski trgovinski centar i Pentagon „Washington Post“

¹⁶ Kahn, 1996 [35]

¹⁷ Cardano Grille, „Classical Steganography“ [12]

¹⁸ Home and Garden Television, „Clues in the Quilts“ [30]

¹⁹ Home and Garden Television, „Clues in the Quilts“ [30]

²⁰ Reč je o „Problemnu zatvorenika“ [25]

²¹ Naslovi članaka su bili: (Terrorist instructions hidden online) i (Terror groups hide behind Web encryption).

u članku iz 19. septembra 2001. Godine, pod naslovom „U.S. agencije traže stručnjake za pomoć u pronalaženju šifrovanih poruka“, daje veliki publicitet u vezi načina i metoda tajne razmene informacija u toku priprema i izvođenja napada od strane članova Al Kaide.

Washington Post Staff Writers, sreda, 19. septembar 2001. godine, strana A14 – Vladine agencije kontaktiraju kompjuterske stručnjake za pomoć u razumevanju kako su Osama Bin Laden i njegovi saveznici koristili Internet za slanje šifrovanih elektronskih poruka u cilju koordinacije napada na Svetski trgovinski centar i Pentagon. Federalni agenti su pronašli dokaze da je Bin Ladenova grupa ubacivala tajna pisma u običnu elektronsku poštu i na Web stranim. Međutim, nastojanja da se poruke lociraju i dešifruju su u zastoju. Brojne i lake za preuzimanje softverske aplikacije su stalno raspoložive i omogućavaju korisnicima zaštitu prenosa informacija od radoznalih pogleda i osuđuju vladine pokušaje za stvaranje sistemskog načina za pronalaženje i proveru tih poruka. Osnovni alati za šifrovanje dopuštaju ljudima šifrovanje poruka tako da ih samo oni koji poseduju ključ mogu čitati. Sve veći broj, međutim, prevazilazi takav način i koristi mogućnost skrivanja poruka unutar grafika, muzičkih fajlova ili u zaglavlju *e-mail*-a.

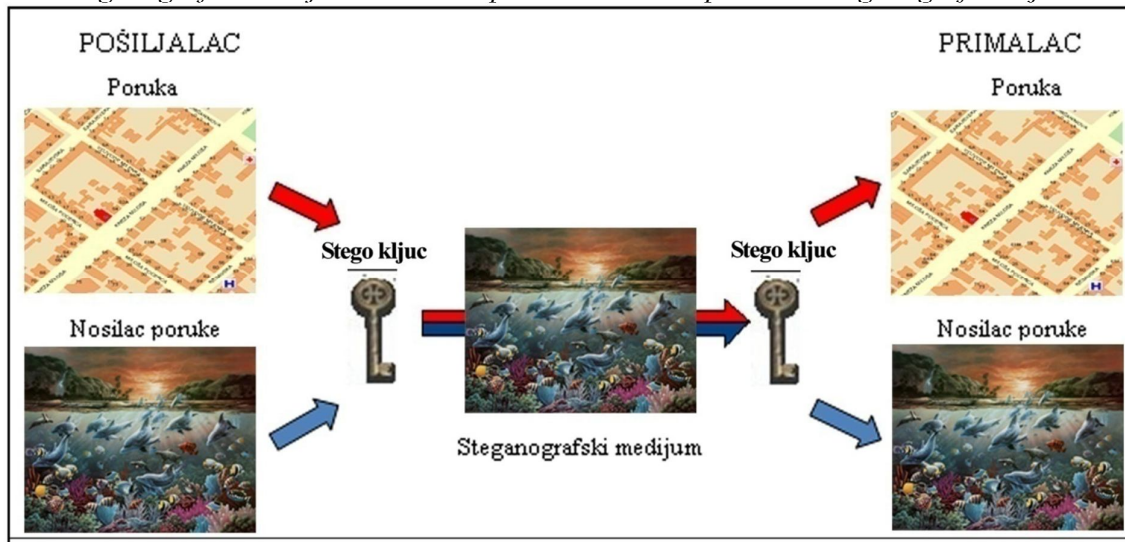
Tehnologija poznata kao steganografija, omogućava korisnicima da zaobiđu elektronska sredstva za prisluškivanje ubacivanjem poruka u naizgled bezazlene digitalne fajlove kao što su sinhronizovane pesme, pošta na *e-Bay* ili pornografske slike. Nil Džonson (*Neil Johnson*), pomoćnik direktora Centra za bezbednost informacionih sistema na Džordž Mason univerzitetu, koji se finansira od strane vlade, je rekao da je steganografija moćna zato što se poruke mogu sakriti bilo gde. Džonsonova najnovija istraživanja su orjentisana, sa izvesnim uspehom, na to kako pregledati sajtove, slike ili protok podataka da bi se ustanovilo da je primenjena steganografija. Mark Lovels (*Mark Loveles*), konsultant kompjuterske bezbednosti sa „*BindView Development Corp*“, rekao je da je tehnologija steganografije pristupačna širokim slojevima i ako se ona koristi pravilno, skoro je nemoguće otkriti autore poruke i primaoca, zbog načina na koji se fajlovi distribuiraju od korisnika do korisnika i upotrebljavaju razmenjeni servisi. U cilju odbrane od terorista, Senator Džad Greg je predložio da autori obavezno predaju državnim bezbednosnim agencijama ključeve za šifrovanje od programa kada ih izrade, što je stav kojem se protive mnoga tehnološka udruženja i koja ističu da bi se to koristilo za napad na privatnost kompjuterskih korisnika koji se pridržavaju zakona. Fil Cimerman, tvorac poznate tehnologije za šifrovanje, rekao je da veruje da rešenje hvatanja terorista leži u ljudskom fizičkom kretanju, a ne većim nadgledanjem tehnologija. Vlada vodi rat protiv tehnologija šifrovanja podataka na nekoliko frontova više od 30 godina. Tražila je od Kongresa strožije sudske propise kod izvoza takvih tehnologija. Baš sada, Nacionalna bezbednosna agencija (NSA) je razvila celo odeljenje za pokušaj da se „moć novih tehnologija iskoristi za naše ofanzivno i defanzivno informaciono ratovanje“. Na zatvorenoj kongresnoj raspravi prošle godine, jedan federalni zvaničnik je rekao da američka inteligencija svojim radom i otkrivanjem novih tehnologija ide na ruku terorističkim organizacijama.

Kao što znamo, terorističke grupe Bliskog istoka, kao što je Hezbolah, Hamas, i organizacija Osame Bin Ladena, koristile su kompjuterske fajlove, *e-mail*-ove i šifrovanje za funkcionisanje njihovih organizacija. To mišljenje je odjeknulo do *Ben Venzke*, „cyber-security“ konsultanta u Virdžiniji koji pomaže nekolicini vladinih agencija. „Grupe poput njih su vrlo inteligentne. Vrlo su mudri u načinu primene operativne bezbednosti i koriste bilo koje alate koji su im raspoloživi“, rekao je on.

2.1.2. Savremena steganografija

Savremeni pojam steganografije, odnosno steganografskog sistema (stegosistema)²² podrazumeva skup sredstava i metoda koji se koriste za formiranje **skrivenog kanala** prenosa informacija. Steganografski sistem mora da zadovolji određene principe: koristi se javni, opšte dostupni kanal prenosa informacija, u procesu steganografije nepoznanica je samo stego ključ i prednost u raspoznavanju tajne poruke je na strani učesnika u razmeni informacija. Opšti proces steganografije (slika1.) dat je relacijom:

Steganografski medijum = skrivena poruka + nosilac poruke + steganografski ključ



Slika 4.- Opšti proces steganografije - stegosistem²³

S obzirom na to da se u svojstvu podataka može koristiti bilo koja informacija : tekst, audio podaci ili slika, kao sveobuhvatni naziv odgovarajuće je koristiti termin **poruka** (engl. *message*) umesto informacija.

Nosilac poruke²⁴ (engl. *carrier, cover, cover medium*) je bilo koja informacija (poruka – slika, audio ili video fajl) namenjena da kao „nosilac“ prenese skrivenu poruku.

Poruka, ugrađena ili **tajna poruka**, (engl. *embedded message*) je poruka koja se implementira u nosioca poruke.

Stego ključ (engl. *steg-key*) je tajni ključ pomoću koga se tajna poruka implementira u nosioca poruke. U zavisnosti od broja nivoa zaštite, u stegosistemu može postojati jedan ili više stego ključeva. Po analogiji sa kriptografijom, u zavisnosti od vrste stego ključa, razlikujemo stego sisteme sa tajnim i javnim ključem.

Steganografski medijum (engl. *steganography medium, stego-medium*) je posrednik koji sadrži implementiranu poruku koja se tajno prenosi.

Steganografski kanal (stegokanal) je komunikacioni kanal preko kojeg se šalje stego nosilac poruke.

Primena kriptografije se najčešće bazira na sledećem principu: pošiljalac tajne poruke bira nasumično nosioca poruke (u zavisnosti od korišćenog softvera, nosilac poruke može biti slika, audio ili video fajl). U izabranog nosioca poruke implementira se tajna poruka uz pomoć stego ključa i na taj način se primaocu šalje steganografski medijum, gde primaoc na drugoj strani obrnutim postupkom dolazi do sadržaja tajne poruke.

²² Na konferenciji **Information Hiding: First Information Workshop** 1996 godine (Baltimor) predložena je upotreba jedinstvene terminologije i definisani su osnovni pojmovi steganografije.

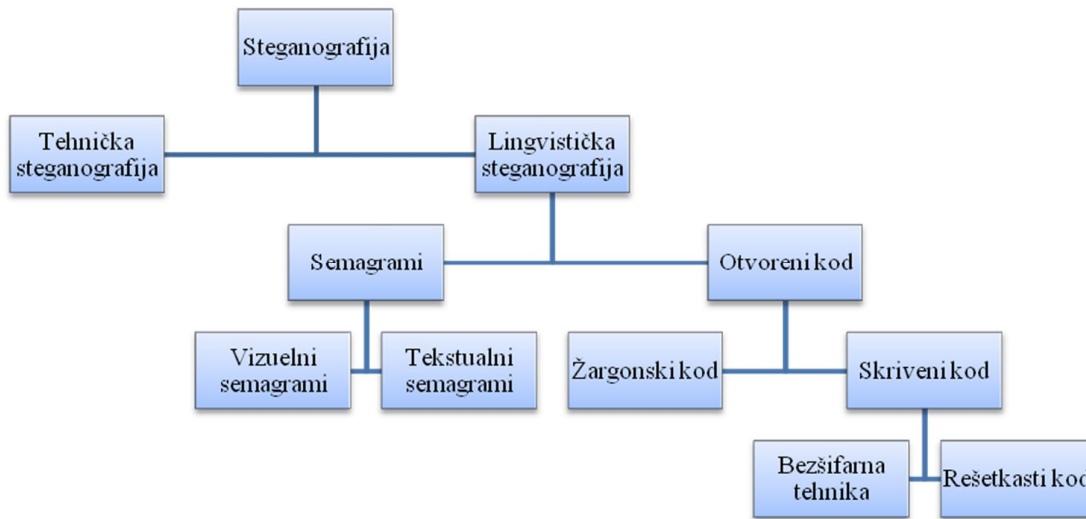
²³ Чековский, С., Овсянников, В., 2002 [19]

²⁴ Nosioca poruke često možemo susreti još pod nazivima kontejner, paket, prenosnik itd.

Da tajna poruka ne bi bila vidljiva posmatraču poruke koja se prenosi, bitno je da nosilac poruke sadrži dovoljno redundantnih bitova (ukoliko je u pitanju digitalna slika) koji mogu biti zamenjeni tajnom porukom. Važno je napomenuti da nisu svi digitalni formati pogodni za prenošenje tajnih poruka, jer se npr. promenom bitova u nekom izvršnom fajlu dovodi do toga da program ne radi ili javlja greške pri radu.

2.1.3. Klasifikacija steganografskih tehnika

Na slici 5. predstavljena je podela steganografskih tehnika.



Slika 5.- Klasifikacija steganografskih tehnika²⁵

Tehnička steganografija koristi naučne metode za sakrivanje poruka, kao što je upotreba nevidljivog mastila ili mikrotačaka i druge metode smanjenja veličine tajnih poruka.

Lingvistička steganografija krije poruke u nosioce na neki neuobičajen način i dalje ih kategoriše kao semagrame ili otvorene kodove.

Semagrami kriju informacije kroz simbole ili znakove. **Vizuelni semagrami** koriste naizgled bezopasne ili svakodnevne fizičke oblike za prenos poruka, kao što su postavljanje detalja na desktop ili web sajt. **Tekstualni semagrami** kriju poruke modifikujući izgled nosioca teksta, kao što je vešta promena tipa ili veličine slova, dodavanjem dodatnih praznih mesta, ulepšavanjem slova ili dodavanje ručno pisanog teksta.

Otvoren kod krije poruke u legitimne nosioce poruka na način koji nije očit nekom nesumnjivom posmatraču. Nosilac poruke se ponekad zove javno saopštenje, s obzirom na to da je skrivena poruka prikriveno saopštenje. Ova kategorija je podeljena na **žargonski kod** i **sakriveni kod**.

Žargonski kod, kao što mu ime kaže, koristi jezik koji je razumljiv grupi ljudi ali je beznačajan drugima. Žargonski kod uključuje simbole koji se koriste da ukažu na prisustvo i vrstu signala bežične mreže, podzemnu terminologiju, ili bezazlenu konverzaciju koja prenosi posebno značenje zato što su činjenice poznate samo govorniku. Podskup žargonskog koda je i znakovni kod u kome se izvesnim preuređenjem fraze menja značenje.

Sakriveni ili **tajni kod** krije poruku javno u nosećoj poruci tako da ona može biti otkrivena od bilo koga ko zna na koji način je ona sakrivena. **Rešetkasti kod** koristi šablon koji je korišćen za prikrivanje u nosiocu poruke. Reči koje se pojave pri otvaranju šablona je

²⁵ Bauer, 2002 i dorađena od strane Arnold-a 2003 [6][3]

sakrivena poruka. *Bezšifarna* tehnika krije poruku prema nekom preuređenom setu pravila, poput “čitaj svako petu reč” ili “traži svako treće slovo u svakoj reči”.

Da bi se sakrila poruka u digitalnom fajlu koristeći bezšifarnu tehniku nisu potrebni specijalni alati ili posebne veštine. Slika ili tekstualni blok može biti sakriven u drugoj slici u PowerPoint fajlu, na primer. Poruka može biti sakrivena u atributima Word fajla, u komentaru na Web stranici ili u nekom drugom formatu kojeg Web browser²⁶ ignoriše. Tekst može biti sakriven kao stilizovana linija u dokumentu tako što se tekstu dodeljuje boja pozadine, a zatim se on postavlja u drugi crtež koji je u prvom planu. Primalac može da povрати skriveni tekst tako što će mu promeniti boju²⁷. Ovo su sve svakako nisko-tehnički mehanizmi, ali su veoma efektni.

2.1.4. Kompjuterska steganografija

Kompjuterska steganografija je deo steganografije koja se bavi realizacijom stegosistema upotrebom kompjuterske tehnike²⁸. Savremene metode kompjuterske steganografije se razvijaju u dva pravca:

- I. Metodi zasnovani na korišćenju specijalnih svojstava kompjuterskih formata i
- II. Metodi zasnovani na statističkom preobilju informacija u audio i video digitalnim signalima.

2.1.4.1. Specijalna svojstva kompjuterskih formata

Ovaj metod²⁹ se manje koristi pri realizaciji metoda kompjuterske steganografije namenjenih zaštiti informacija, a više za realizaciju metoda informacionog napada, odnosno, za ubacivanje virusa, programa-agenata. Npr. virus *W32/Perrun* je vrlo prost virus obima 18 Kb, ubacuje se u fajlove sa .jpg ekstenzijom tako što se samo nadoda na njih formirajući dvokomponentni program.

2.1.4.2. Preobilje informacija u audio i video digitalnim signalima

Osnovni pravac razvoja metoda kompjuterske steganografije zasnovan je na ovoj metodi. Digitalna fotografija, digitalna muzika i digitalni video predstavljaju matricu brojeva koji kodiraju intenzitet (jačine svetlosti kod fotografije, intenzitet jačine zvuka kod muzike) u diskretnom trenutku u vremenu i prostoru. Kako biti sa najmanjim značenjem u sebi sadrže malo korisne informacije, njihova zamena sa tajnom porukom ne utiče značajno na kvalitet reprodukovanoog zvuka ili slike.

Kako zbog grešaka kvantizacije³⁰ digitalne signale već prati šum, kvalitet se neznatno pogoršava i ne registruje se čovekovim čulima. Metodi iz ove grupe mogu se podeliti na:

1. Metod zasnovan na neznatnoj modifikaciji slika (engl. *image domain*). Ovaj metod se ponekad naziva i *bit vise method* i on obično koristi modifikaciju po najmanje značajnim bitima (engl. – *LSB* odn. *least significant bits*).
2. Metod zasnovan na transformaciji slika (engl. *transform domain*). Ovo su metodi zasnovani na transformacijama slika koristeći trigonometrijske transformacije (engl. *DCT* - *Discrete Cosine Transformation* - diskretnu kosinusnu transformaciju), ili na slaganje

²⁶ Artz, 2001 [4]

²⁷ Seward, 2004 [44]

²⁸ Curran, K., 2003 [16]

²⁹ Format PE (*portable executable*) ima osobinu da je razbijen u više sekcija. U svakoj od sekcija ima slobodnog prostora u koji je moguće umetnuti neke druge podatke

³⁰ Kvantizacija je jedan od dva postupka koji se primenjuje na analogni signal kako bi se dobili digitalni signali.

različitih talasa (engl. *Wavelet transformation*)³¹. O kojim mogućnostima prenosa informacija je reč, najbolje se vidi na primerima.

Kolor fajl po LSB metodu³² omogućava da se u fajlu veličine 800 Kb smesti skrivena poruka i do 100 Kb. S druge strane, samo jedna sekunda digitalnog zvuka, po LSB metodu, omogućava prenos tajne poruke do 10 Kb³³. Tipična 8-bitna slika dimenzija 640 x 480 sa 256 nijansi boja omogućava skrivanje poruke od 300 Kb, odnosno 24-bitna slika 1024 x 768 do 2 Mb.

2.1.5. Steganografija u digitalnim formatima

2.1.5.1. Steganografija u video formatima

Kada se informacija krije unutar video fajla, program ili osoba kriju informaciju uglavnom koristeći DCT metod. DCT funkcioniše neznatnim menjanjem svake slike u videu, ali samo toliko da to ne bude vidljivo ljudskom oku.

Preciznije, DCT menja vrednost određenih delova slike, uglavnom ih zaokružujući. Na primer, ako deo slike ima vrednost 6.667 zaokružuje se najviše na 7.

Steganografija u video fajlovima je slična steganografiji u slikama, osim što je informacija sakrivena u svakom frejmu videa.

Kada je samo mali deo informacije sakriven unutar videa generalno nije uočljiv uopšte, u svakom slučaju, što je više informacija sakriveno postaće manje uočljive.

2.1.5.2. Steganografija u audio formatima

Kada se informacija krije u audio fajlu, uglavnom se koristi tehnika kodiranja na slabom bitu koja ima sličnosti sa LSB koji se generalno koristi u slikama.

Problem sa kodiranjem slabog bita je taj što je on uglavnom uočljiv ljudskom uhu, pa je to donekle rizična metoda za nekoga ko je koristi ako pokušava da maskira informaciju unutar audio fajla.

Metod proširenog spektra (engl. *Spread spectrum*) je drugi metod koji se koristi za sakrivanje informacija unutar audio fajla. Ovaj metod funkcioniše na taj način što se dodaju slučajni šumovi informacijama koje su sakrivene u nosiocu i raširene kroz spektar frekvencija.

Pored sakrivanja podataka metodom proširenog spektra koristi se i metod sakrivanja podataka uz pomoć eha (engl. *Echo data hiding*). Ovaj metod koristi eho u muzičkim fajlovima takvim redom da se kriju informacije koje taj fajl nosi. Informacija može biti sakrivena jednostavnim dodavanjem dodatnog zvuka izvesnom ehu u audio fajlu. Ono što čini ovaj metod sakrivanja informacije u audio fajl boljim od drugih je to što on u stvari poboljšava zvuk audio fajla u audio fajlu.

Audio kodiranje uključuje konvertovanje analognog signala u digitalni tok bita. Analogni zvuk-glas i muzika je predstavljena sinusnim talasom raličitih frekvenci. Ljudsko uho ne može da čuje nominalnu frekvenciju u rasponu od 20 do 20.000 Hz (*Hertz* – herc). Zvuk je analogan, što znači da je signal kontinualan. Skladištenje digitalnog zvuka zahteva da kontinuirani zvučni talas bude promenjen u set uzoraka koji mogu biti predstavljeni nizom nula i jedinica.

Pretvaranje analognog u digitalni zvuk je usavršeno uzorkovanjem analognog signala, mikrofonom ili nekim drugim uređajem i pretvaranjem tog uzorka u naponske nivoe. Naponski ili signalni nivoi su tada konvertovani u numeričke vrednosti koristeći šemu zvanu

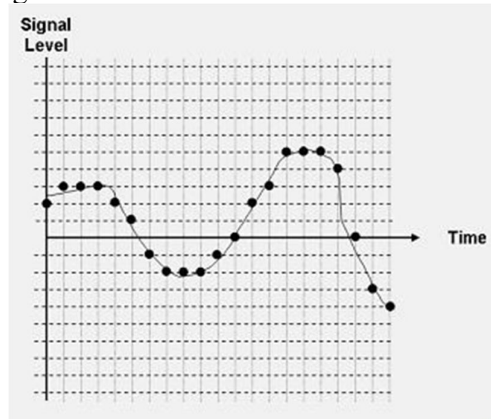
³¹ Curran K., [16]

³² Ovaj metod opisan je na strani 24.

³³ Чековский, С., Овсянников, В., 2002 (19)

pulsno kodna modulacija (engl. PCM - *pulse code modulation*³⁴). Uređaj koji izvršava ovo konvertovanje zove se koder-dekoder ili samo koder.

PCM omogućava samo približnost originalnom analognom signal, kao što je prikazano na slici 6. Ako je nivo analognog zvuka izmeren na 4.86 nivou, npr. biće konvertovan na vrednost 5 u PCM. Ova razlika se naziva kvantizaciona greška. Druga audio aplikacija definiše drugi broj u PCM nivou tako da je ova “greška” gotovo nemoguća za detekciju ljudskom uhu. Telefonska mreža konvertuje svaki glasni uzorak u osmobarbitnu vrednost, dok muzičke aplikacije koriste generalno šesnaestobarbitnu vrednost.



Slika 6.- Jednostavna pulsno kodna modulacija³⁵

Analogni signal treba da bude uzorkovan srazmerno iz dve najveće frekvencijske komponente signala, tako da original može biti korektno reprodukovano nezavisno od uzorka. U telefonskoj mreži, ljudski glas nosi frekvenciju okvirno 0-4000 Hz, iako je samo zapravo 400-3400 Hz korišćeno za prenos glasa, s toga, glas je pojednostavljen 8.000 puta u sekundi. Muzička audio aplikacija simulira pun spektar ljudskog uha i generalno koristi 44.1 kHz brzinu uzorkovanja³⁶.

Protok bita nekompresovane muzike može se lako izračunati frekvencijom uzorkovanja (44.1 kHz), rezolucijom ili kvantizacijom PCM-a (16 bita) i broja zvučnih kanala (dva). Ona iznosi 1.411.200 bita u sekundi. Ovo bi značilo da jedan minut audio fajla (nekompresovanog) zauzima 10.6 MB ($1,411,200 \times 60 / 8 = 10,584,000$ b).

Audio fajlovi se smanjuju korišćenjem raznih tehnika kompresovanja. Jedan očigledan metod je redukovanje broja kanala na jedan ili redukovanje brzine uzorkovanja, u nekim slučajevima na 11 kHz. Drugi kodeci koriste vlastite šeme kompresovanja.

Sva ova rešenja smanjuju kvalitet zvuka.

Tabela 2.- Neki od uobičajenih digitalnih audio formata (Fries and Fries 2000)

Audio format	Ekstenzija	Koder
AIFF (Mac)	.aif, .aiff	Modulacija pulsnog koda (ili drugi)
AU (Sun/Next)	.au	A-law odn. μ -law (ili drugi)
CD audio (CDDA)	n/a	Modulacija pulsnog koda
MP3	.mp3	MPEG Audio Layer III
Windows Media Audio	.wma	Microsoft-ovo vlasništvo
QuickTime	.qt	Vlasništvo Apple-a
RealAudio	.ra, .ram	Vlasništvo Real Networks-a
WAV	.wav	Modulacija pulsnog koda (ili drugi)

³⁴ Pulsno kodna modulacija je digitalno predstavljanje analognog signala, gde se najveći deo signala, ravnomerno, u stalnim intervalima, menja iz stalnih (konstantnih) signala u diskretne signale, i zatim se od niza diskretnih signala stvara niz simbola u digitalnom (obično binarnom) kodu.

³⁵ An Overview of Steganography for the Computer Forensics Examiner [30]

³⁶ Fries and Fries 2000 [27]

2.1.5.3. Steganografija u dokumentima

Korišćenje steganografije u dokumentima funkcioniše jednostavnim dodavanjem praznih mesta i tabova na krajevima linija u dokumentima.

Ovaj vid steganografije je veoma efikasan, zato što korišćenje praznih mesta i tabova nije uopšte vidljivo ljudskom oku, bar u najvećem broju tekstualnih editora.

Prazna mesta i tabovi nalaze se prirodno u dokumentima, pa ne postoji bilo koji mogući način da korišćenje ovog metoda steganografije bude nekome sumnjivo.

2.1.5.4. Steganografija u slikama

Kada krijemo informaciju u slikama, najčešće korišćen metod, je metod najmanje važnog bita (engl. *Least Significant Byte* – LSB). Za kompjuter slika predstavlja jednostavan fajl koji pokazuje različite boje i intenzitete svetlosti u različitim delovima slike.

Najbolji format slike za sakrivanje informacija je 24-bitna BMP slika. Razlog je taj što je ovo najveći tip fajla, a samim tim i najkvalitetniji. Kada je slika visokog kvaliteta i rezolucije mnogo je lakše sakriti i maskirati informaciju u njoj. U 24-bitnom slikovnom formatu, kao što je BMP, boja je predstavljena kao kombinacija crvene, zelene i plave boje. Svaku od ovih boja predstavlja 1 bajt. Kombinacija od po jednog bajta crvene, zelene i plave daje 3 bajta (24 bita) koji predstavljaju 1 piksel. Iako je 24-bitna slika najbolja za sakrivanje informacija, zbog njene veličine mnogi se opredeljuju za 8-bitni BMP ili sliku nekog drugog formata npr. GIF. Još jedan od razloga je taj što slanje velikih slika preko Interneta može izazvati sumnju.

Važno je zapamtiti da ako krijemo informaciju u slici, konvertovanjem slike u neki drugi format, najverovatnije će doći do gubitka informacija koje su bile pohranjene u njoj.

Na slici 7. predstavljena je RGB kocka, uobičajen način za predstavljanje boja koje se dobijaju iz tri osnovne boje, crvene, zelene i plave (engl. *red, green, blue* – RGB), i svaka je predstavljena na svojoj osi³⁷.

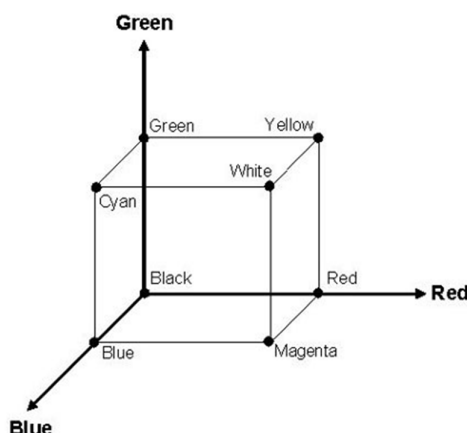
Mešavinom 100 % crvene, 100% plave i 100% zelene boje formira se crna boja koja je na slici predstavljena kao presek tri ose, odnosno kao nulta tačka.

Mešavinom 100 % crvene, 100% plave i odsustvom zelene boje formira se magenta.

Mešavinom 100% zelene i 100% plave i odsustvom crvene boje formira se cijan.

Mešavinom 100% zelene i 100% crvene i odsustvom plave boje formira se žuta boja.

Odsustvo sve tri boje predstavlja belu boju.

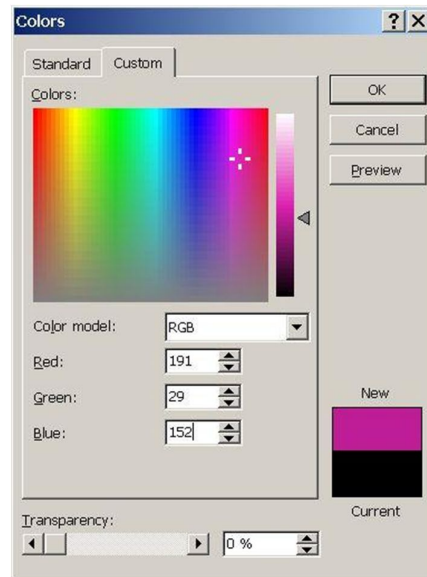


Slika 7.- RGB kocka

Slika 8. prikazuje nivo RGB inteziteta slučajno izabrane boje. Svaka RGB komponenta je specifična po jednom bajtu, tako da vrednost svake boje varira od 0-255. Ova

³⁷ moreCrayons 2003 [38]

određena nijansa je označena nivoom crvene na 191, zelene 298 i plave boje na 152. 24-bitna šema podržava 16.777.216 (2^{24}) jedinstvene boje³⁸.



Slika 8.- U prozoru za izbor boje prikazani su nivoi RGB boje za odabranu boju

Najveći broj aplikacija za digitalne slike danas podržava 24-bitne slike, gde je svaki element slike (piksel) kodiran u 24. bita, obuhvatajući tri RGB bajta kao što je prethodno opisano. Druge aplikacije kodiraju boje koristeći 8 bita/pikselu. Ove šeme takođe koriste 24-bitni slikovni format, s tim što su palete te koje određuju koje će boje biti korišćene u slici. Svaki piksel je kodiran sa 8 bita gde vrednost tačke u 24-bitna boje ulazi u paletu. Ovaj metod ograničava jedinstven broj boja u datoj slici na 256 (2^8).

Izbor kodiranja boje svakako utiče na veličinu slike. Slika dimenzija 640 x 480 piksela koristeći 8-bitni slikovni format zauzima otprilike 307 KB ($640 \times 480 = 307.200$ bajta), dok bi slika dimenzija 1400x1050 koristeći 24-bitni slikovni format zauzela 4.4 MB ($1400 \times 1050 \times 3 = 4.410.000$ bajta).

Paleta boja i 8-bitni slikovni format su obično korišćeni u GIF (*Graphics Interchange Format*) i BMP formatu. GIF i BMP se generalno uzimaju u obzir da bi se obezbedila idealna kompresija zato što obnovljena slika posle kodiranja i kompresije je identična u bit originalnoj slici³⁹.

JPEG (*Joint Photographic Experts Group*) format slike koristi diskretnu kosinusnu transformaciju, pre nego kodiranje piksel-po-piksel. U JPEG formatu, slika je podeljena na 8x8 blokova za svaku odvojenu komponentu boje. 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. Svaki 8x8 blok, ili podblok, je transformisan u 64 diskretnih kosinusnih transformacionih koeficijenta koji su približni osvetljenju (svetlosti, tami i kontrastu) i signalu boje tog dela slike. JPEG se generalno smatra lošim formatom za kompresovanje, jer slika obnovljena iz kompresije je blizu originalnoj slici, ali nije i identična.⁴⁰

Da bi stavili što veću količinu podataka u sliku, mi možemo pre ubacivanja podataka, da te iste podatke kompresujemo i tako smanjimo njihovu veličinu, a ujedno povećamo prostor za skladištenje podataka unutar slike.

³⁸ Curran, K. and Bailey, K, 2003 [17]

³⁹ Johnson and Jajodia, 1998A [33]

⁴⁰ Johnson and Jajodia, 1998A [33]

Postoje dve vrste kompresije. Obe vrste imaju isti cilj, ali ipak postoji jedna velika razlika.

- 1) Kompresija bez gubitaka (*Lossless* kompresija) smanjuje originalnu veličinu slike upotrebom različitih algoritama, a posle toga je moguće takvu sliku dekompresovati i vratiti u originalno stanje.
- 2) Kompresija sa gubicima (*Lossy* kompresija) takođe smanjuje originalnu veličinu slike, ali to radi na račun kvaliteta slike. Takvu sliku je nemoguće vratiti u originalno stanje jer su neki njeni delovi trajno uklonjeni. Pravi predstavnik *lossy* kompresije jeste JPEG. Za kompresiju podatka može se koristiti bilo koji algoritam.

Poboljšanje izgleda stegoslike

Može se desiti da se, i pored minimalnih promena boja, primeti mutnjikavost i šarenilo na slici, ili da se pojave „usamljene tačke“ na slici. Ovo se ipak može izbeći upotrebom različitih tehnika obrade slike, odnosno različitih filtera i efekata, ali pažljivo odabranih.

1. Maskiranje i filtriranje

Ovo je jedna od najzastupljenijih tehnika u steganografiji. Postoji više načina na koje se može primeniti. Ako se primeti u nekom delu slike mutnjikavost posle ubacivanja skrivenih podataka, onda se original slike može malo potamniti i nakon toga ubaciti podaci u nju. Uspešnost ove tehnike se zasniva na činjenici da ljudsko oko slabije raspoznaje razlike među bojama slabije sjajnosti. Ali ne treba preterivati ni u tom polju jer onda stegoslika neće više ličiti na sliku.

2. Dodavanje „šuma“

Jedan od veoma efektnih metoda jeste i dodavanje šuma. Cela tehnika se zasniva na dodavanju belih tačaka ili izbeljivanju nekih tamnijih. Sve ovo krajnjem korisniku stvara utisak da je slika skenirana i da je slabijeg kvaliteta, i takvu sliku retko ko uzima u detaljno razmatranje. Pri dodavanju šuma, važno je da se ne menjaju bitovi koji nose skriveni podatak, već samo oni bitovi koji se ne koriste za skrivanje podataka.

3. Korekcija boje piksela

Korekcija boje piksela je, dosad, najsavršenija tehnika. Funkcioniše tako što se skriveni podatak upisuje npr. u svaki drugi piksel, a pikseli koji ostanu slobodni, koriguju se prema bojama susednih piksela. Korekcija slobodnog piksela se vrši tako što se, pored njegove originalne boje, gledaju i one susedne (slika bolje izgleda ako se gleda nekoliko susednih), a potom se nađe srednja vrednost boje. Tako će slika izgledati skoro isto kao i original, odnosno približnije nego pre ugrađivanja podataka. Nedostatak ove tehnike jeste to što se, u stvari, koristi svaki drugi piksel za skrivanje podataka, što znači da ima duplo manje prostora za podatke. Velika prednost ovog načina poboljšanja izgleda slike je to što se šanse za otkrivanje tajnog sadržaja svode baš na minimum. Slika će još bolje izgledati ako se podaci sakrivaju u svakom trećem pikselu i tako dalje, ali, naravno, biće srazmerno manje mesta. Korekcija boje piksela može se nesmetano koristiti na slikama velikog formata u koje je potrebno staviti podatak relativno male dužine.

2.1.6. Ugrađivanje vodenih pečata u sliku

Digitalna prezentacija zaštićenih dokumenata poput filmova, pesama ili fotografija ima mnogo prednosti. Mogućnost stvaranja neograničenog broja savršenih kopija stvara probleme vlasnicima prava na te dokumente. U poslednje vreme sa širenjem popularnosti Interneta ovaj problem postaje sve izražajniiji. Jedini alat za zaštitu vlasničkih prava donedavno je bilo šifrovanje podataka. Šifrovanjem podataka mogu se zaštititi podaci samo za

vreme transporta do primaoca, a nakon što primalac dešifruje dokument, podaci postaju ponovno nezaštićeni.

Kao rešenje je stvoren koncept vodenih pečata. Vodeni pečati su delovi informacije umetnuti u originalni dokument, tako da promene na originalnom dokumentu budu teško uočljive čoveku, ali se mogu lako detektovati računarom.

Ubacivanje vodenih pečata u sliku može se obaviti u prostornom i u transformacijskom domenu. Pokazalo se da su sastavi koji koriste transformacijske domene otporniji na napade u odnosu na sastave u prostornom domenu.

2.1.6.1. Metodi za ubacivanje vodenog pečata u prostornom domenu

Jedan od prvih metoda ubacivanja vodenog pečata u sliku je bilo iskorišćavanje piksela koji ima najmanju vrednost bita. Ljudsko oko nije u stanju prepoznati razlike u slici nastale LSB promenom, pa se taj bit može iskoristiti za ubacivanje dodatne informacije. Ali, ubačeni pečat ovom metodom jednostavno se može uništi. Dovoljno je sliku zarotirati za 1 stepen, promeniti kontrast ili učiniti neku drugu transformaciju i pečat će biti nemoguće ponovno izdvojiti iz slike.

Bolji algoritam u prostornom domenu⁴¹ koristi binarnu masku i pikselima slike određenom binarnom maskom povećava intenzitet za neku vrednost (pretpostavlja se da se radi o crno-beloj slici). Vodeni pečat u ovom algoritmu je binarni uzorak iste veličine kao i slika u kojem je broj nula jednak broju jedinica. Ubacivanje pečata se vrši povećanjem intenziteta piksela slike označenog jedinicom u binarnoj maski za *faktor k*. Faktor k se određuje na temelju statističkih svojstava slike. Ekstrakcija pečata se vrši poređenjem srednje vrednosti intenziteta označenih i neoznačenih piksela i pri tome nije potrebna originalna slika. Povećanje čvrstine algoritma se postiže korišćenjem varijabilnog faktora k i korišćenjem pečata po blokovima veličine 2x2 ili 3x3.

U algoritmu koji predlažu *Voyatzis i grupa autora* vodeni pečat može biti i slika (logo) veličine $S1 \times S2$. Prostornom transformacijom nazvanom **totalni automorfizam** logo se iterativno transformiše u vodeni pečat veličine $M1 \times M2$, koji predstavlja haotični razmeštaj binarnih piksela logoa slike. Vodeni pečat se ubacuje u sliku kombinovanjem piksela iz vodenog pečata i dela originalne slike veličine $S1 \times S2$. Detekcija vodenog pečata se vrši izdvajanjem dela iz označene slike, odakle se procenjuje haotični vodeni pečat. Izvršavanjem totalnog automorfizma na procenjenom haotičnom vodenom pečatu dobija se *binarni logo*.

Kuter i grupa autora predlažu metod za kolor slike koja je otporna na JPEG kompresiju, ali i na geometrijske transformacije zahvaljujući sinhronizacionim referencama. Vodeni pečat se dodaje u plavu komponentu piksela prema formuli:

$$B_{ij}^* = B_{ij} + (2s - 1)L_{ij}q,$$

gde je ***B_{ij}*** vrednost plave komponente piksela, ***L_{ij}*** vrednost luminancije za taj piksel, ***B_{ij}**** je nova vrednost plave komponente piksela, ***s*** je bit vodenog pečata, a ***q*** je konstanta za jačinu pečata.

Za transformaciju je izabrana komponenta plave boje jer je u ljudskom oku manja gustina osećaja za plavu boju, odnosno promene u "plavom" delu spektra su slabije vidljive nego za druge boje. U detekciji pečata potrebna je procena originalnih vrednosti piksela. Procena se vrši na temelju linearne kombinacije između susednih piksela i modifikovanog piksela. Razlika između procenjene vrednosti i vrednosti modifikovanog piksela se upoređuje s konstantnom vrednošću (pragom) i na temelju toga se utvrđuje da li je u taj piksel umetnuta vrednost pečata "1" ili "0".

⁴¹ Ovaj domen se još naziva i domen slike

Metode za umetanje pečata u prostornom domenu su slabe u poređenju sa linearnim transformacijama: rotaciji, translaciji i skaliranju.

2.1.6.2. Metodi za ubacivanje pečata u transformacionom domenu

Čvršći sastavi vodenih pečata koriste transformacione domene. Postupak ubacivanja pečata započinje transformacijom originalne slike iz prostornog domena u odgovarajući transformacioni domen. Od transformacionog domena se zahteva da, što je moguće bolje, aproksimira svojstva ljudskog vizuelnog sistema, jer se tada može u sliku umetnuti više informacije uz manje vidljivih promena. Za transformaciju se najčešće upotrebljavaju: diskretna Fourierova transformacija (*DFT*), *DCT* ili transformacija u domenu talasa (engl. *wavelet*). Osim navedenih transformacija koriste se i preklapajuća ortogonalna transformacija - *LOT* (engl. *lapped orthogonal transform*), Frenelova transformacija, fraktalna transformacija, Fourier-Mellin transformacija i dr.

Nakon transformacije potrebno je odabrati podskup frekvencijskih koeficijenata koji će biti modifikovani. Obično taj podskup pripada pojasu srednjih frekvencija. Odabir koeficijenata niskih frekvencija se po pravilu izbegava, jer promene na tim koeficijentima su vidljive, a koeficijenti visokih frekvencija po pravilu su nezaštićeni od kompresija. Vodeni pečat se korišćenjem transformacionih domena proširi po celoj slici. Modifikovanje koeficijenata se većinom svodi na dodavanje određene vrednosti odabranim koeficijentima. Nakon umetanja vodenog pečata u sliku izvršava se inverzna transformacija u prostorni domen i slika je spremna za distribuciju.

2.1.7. Metodi prenošenja informacija u digitalnim formatima

Postoji mnogo načina na koje možemo poruku sakriti u digitalni medij. Istražitelji u digitalnoj forenzici su upoznati sa podacima koji su ostali u zanemarenim fajlovima ili nelokalizovanim mestima kao ostaci preostalih fajlova. Programi mogu biti pisani da pristupaju zanemarenim i neoznačenim mestima direktno. Male vrednosti podataka mogu takođe biti sakrivene u neiskorišćenim delovima u zaglavlju fajla⁴².

Informacije mogu biti sakrivene i na hard disku u tajnoj particiji. Sakrivena particija neće biti vidljiva pod normalnim okolnostima, iako konfiguracija diska i drugi alati možda dozvoljavaju potpuni pristup sakrivenoj particiji. Ova teorija je implementirana u steganografski *ext2fs* sistemski fajl za Linux. Sakriveni sistemski fajl je posebno interesantan zato što štiti korisnika od zamršenosti određenih informacija na njegovom hard disku. Ovo omogućava korisniku tvrdnju da on nikada nije posedovao određene informacije ili da tvrdi da se određeni događaji nikada nisu desili. Pod ovim sistemom korisnici mogu da sakriju brojne fajlove na disku, tajnost sadržaja fajlova je zagarantovana i ne remete se neskriveni fajlovi kada se ukloni steganografski fajl drajver⁴³.

Mrežni protokoli su takođe jedni od digitalnih nosioca. Tajni prenos kontrolnog protokola koji je uveo Kreg Rovland formira tajni komunikacioni kanal koristeći identifikaciono polje u paketu internet protokola (IP) ili niz brojnih polja u delovima protokola za kontrolu prenosa (TCP)⁴⁴.

Slika i audio fajl su najčešći nosioci medija na internetu zato što potencijalni nosioci fajlova već postoje, velika je mogućnost kreiranja neograničenog broja novih nosioca i lak je pristup steganografskom softveru koji će operisati nad ovim nosiocima. Iz tog razloga, pažnju treba posvetiti slikama i audio fajlovima.

⁴² Curran, K. i Bailey, K, 2003 [17]

⁴³ Anderson, R i sar., 1998 [1], Artz, 2001 [4]

⁴⁴ Johnson idr., 2001 [34]

2.1.7.1. LSB supstitucija

Kao što je već napomenuto, LSB je najčešće korišćen steganografski metod. Termin najmanje važan bit dolazi od numeričke važnosti bita u bajtu. Bit visokog reda ili najvažniji bit je onaj koji ima najveću aritmetičku vrednost ($2^7=128$), dok je bit niskog reda ili najmanje važan bit onaj koji ima najmanju aritmetičku vrednost ($2^0=1$). Najmanje značajni bitovi odabrane datoteke nosioca zamenjuju se bitovima tajne poruke.

Jednostavan primer LSB supstitucije je sakrivanje slova A u sliku koja će biti nosilac tajne poruke. ASCII ekvivalent slova A je u binarnom obliku 01000001. Za skrivanje su nam dovoljna 3 piksela.

Neka su ti pikseli:

(00100111,11101001,11001000)
(00100111,11001000,11101001)
(11001000,00100111,11101001).

Umetanje binarne vrednosti slova A u tri piksela rezultira sa:

(00100110,11101001,11001000)
(00100110,11001000,11101000)
(11001000,00100111,11101001).

Samo su podebljani bitovi (3 bita od 9 najmanje značajnih) promenili vrednost. U proseku se primenom ove metode promeni samo polovina najmanje značajnih bitova. Piksela koji se najviše promenio, a promenio se za dve nijanse, što je u odnosu na 16,7 miliona nijansi zanemarljivo za ljudsko oko.

LSB supstitucija se može koristiti da bi se prepisale propisane RGB boje ili indikator palete u GIF i BMP fajlovima, koeficijent u JPEG fajlovima i nivo pulsno kodne modulacije u audio fajlovima. Prepisivanjem najmanje važnog bita, numeričke vrednosti bita se menjaju veoma malo i najmanja je mogućnost da će biti detektovana od strane ljudskog oka ili sluha.

LSB substitucija je jednostavna tehnika u steganografiji, ali samo najnaivniji steganografski softver bi prosto prepisao svaki LSB sakrivenim podacima. Gotovo svi softveri koriste neku vrstu sredstva za slučajnu upotrebu pravog bita u nosiocu fajla koji je promenjen. Ovo je jedan od faktora koji detekciju steganografije čini veoma teškom.

Jedan od načina da se sakriju informacije u slici je da se promeni redosled boja u paleti ili da se koristi LSB kodiranje u paleti boja pre nego na slici. Ovaj metod je prilično slab. Mnogi grafički softveri ređaju paletu boja po učestanosti, svetlosti ili nekom drugom parametru i slučajno uređene palete se nalaze izvan statističke analize⁴⁵.

Noviji, kompleksniji metodi steganografije nastavljaju da isplovljavaju. **Steganografski metod proširenog spektra** je sličan proširenom spektru radio prenosa, koji je razvijen u Drugom svetskom ratu i koji se danas obično koristi u sistemima za razmenu podataka, gde je „energija“ signala raširena preko širokog spektra frekvencija, umesto fokusiranja na pojedinačnu frekvenciju, u naporu da se detekcija i ometanje signala što više otežaju. Steganografija proširenog spektra ima istu funkciju, a to je da se izbegne detekcija. Ovi metodi daju prednost zbog činjenice da se neznatne deformacije slike i zvuka sa najmanjom verovatnoćom mogu otkriti u visoko energetske delovima signala nosioca (najveći intenzitet u audio fajlovima ili intenzitet-jasnoća boja u slikama). Čak i kada se uporedo gleda, lakše je

⁴⁵ Fridrich, J. i Du, R, 2000 [25]

obmanuti ljudska čula kada su male promene napravljene u glasnoj muzici i/ili jasnim slikama⁴⁶.

2.1.8. Detekcija steganografije

Problem zatvorenika⁴⁷ je najčešći primer korišćen za opis steganografije. Problem uključuje dva zatvorenika, Alisa i Boba, koji su zaključani u odvojenim zatvorskim ćelijama i žele da prenesu neki tajni plan jedno drugom. Njima je dozvoljeno da razmenjuju poruke međusobno, ali Vilijam, stražar, može da čita sve poruke. Alis i Bob znaju da bi Vilijam, ukoliko otkrije tajni kanal, obustavio komunikaciju.

Vilijam može da utiče na aktivan ili pasivan način. U pasivnom stražarskom modelu, on ispituje svaku poruku i odlučuje da li da prosledi poruku ili ne, bazirajući se na svojoj mogućnosti da detektuje skrivenu poruku. U aktivnom stražarskom modelu, može da promeni samu poruku ukoliko on to želi. Konzervativan ili zlonameran stražar je mogao da promeni svaku poruku u pokušaju da poremeti skriveni kanal tako da bi Alis i Bob morali da koriste veoma robustan (otporan na proboj) steganografski metod.

Težina stražarevog zadatka najviše zavisi od kompleksnosti steganografskog algoritma i znanja koje poseduje.

U čistom steganografskom modelu, Vilijam ne zna ništa o steganografskom modelu koji koriste Alis i Bob. Ovo je slaba pretpostavka za Alisa i Boba, pošto je zaštita sa skrivanjem retko uspešna, posebno kada se primenjuje kriptografija. Ovo je čest model koji se javlja kada digitalni forenzičari pretražuju web sajt ili hard disk na potencijalno prisustvo steganografije.

Pri upotrebi tajnog steganografskog ključa pretpostavlja se da Vilijam zna steganografski algoritam, ali ne zna tajni steganografski/kriptografski ključ koji su koristili Alis i Bob. Ovo je u skladu sa pretpostavkom da korisnik kriptografije treba da napravi tajni ključ, prema Kirkofovom principu koji glasi: „Sigurnost kriptografske šeme je u upravljanju ključevima, ne u sigurnosti algoritma.”⁴⁸ Ovo je možda suviše zahtevna pretpostavka za praksu, ali da bi informacija bila kompletna trebalo bi uključiti i kontrolu pristupa nosiocu fajla.

2.1.8.1. Steganoanaliza

Steganoanaliza, steganaliza ili detekcija steganografije od treće strane, relativno je mlada istraživačka disciplina o kojoj su se prvi članci pojavili 1990-tih godina. Veština i naučnost steganoanalize ima za nameru otkrivanje ili procenu sakrivenih informacija zasnovano na posmatranju nekog prenosa podataka, bez pretpostavke koji steganografski algoritam je korišćen⁴⁹. Steganoanaliza, takođe, za cilj može imati izvlačenje skrivene poruke i da na taj način onemogući da primaocu poruke dođe do nje, kao i promenu tajne poruke kako bi se poslala dezinformacija primaocu. Detekcija steganografije i izvlačenje skrivene poruke je generalno dovoljno ako je svrha skupljanje dokaza povezanih sa istraživanim kriminalom, iako uništavanje i/ili zamena tajne poruke može takođe biti pravno legitimna tokom istrage aktivnosti kriminalne ili terorističke grupe.

U suštini **steganoanaliza** treba da reši tri osnovna zadatka i to:

- detekciju postojanja skrivene poruke,
- definisanje formata u kojem je ona "spakovana" i
- dekodiranje skrivene poruke.

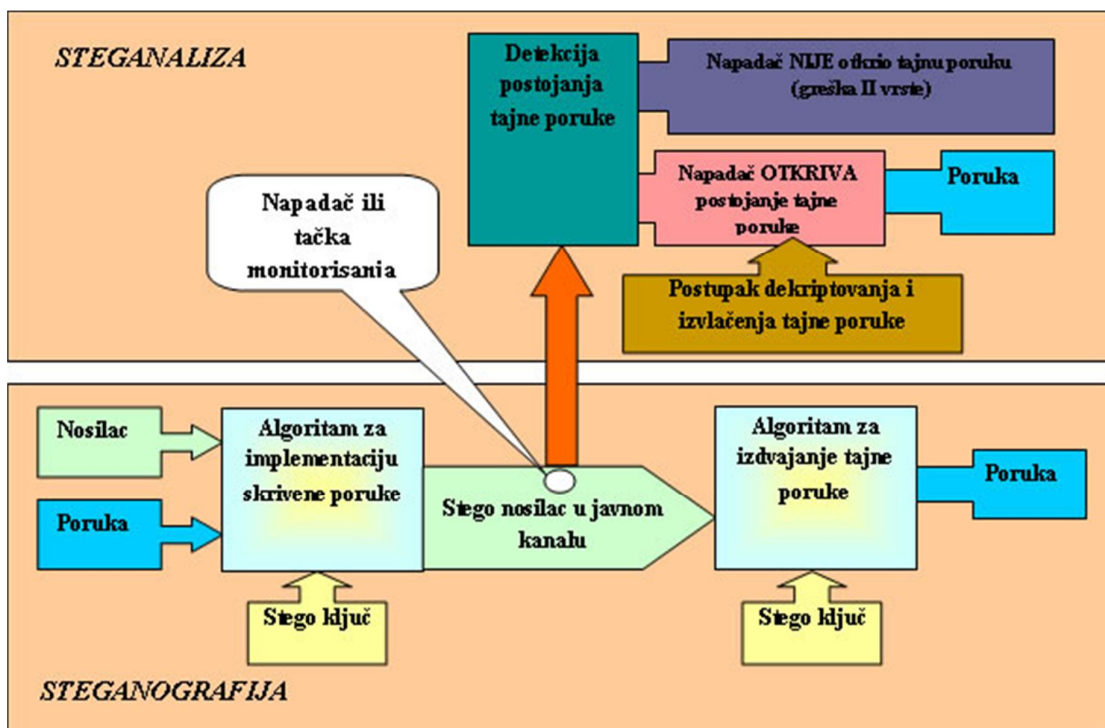
Odnos steganografije i steganalize prikazan je na slici 9.

⁴⁶ Wayner, 2002 [51]

⁴⁷ Simmons, 1983 [45]

⁴⁸ Kahn, 1996 [35]

⁴⁹ Chandramouli, 2002 [18]



Slika 9.- Odnos steganografije i steganoanalize

Za razliku od kriptanalize, gde je evidentno da dobijeni šifrat sadrži tajnu poruku, steganoanaliza uglavnom startuje sa nekoliko sumnjivih informacionih tokova, ali je neizvesno da li neki od njih sadrži skrivenu poruku. Steganoanaliza počinje smanjivanjem skupa sumnjivih informacionih tokova u podskup najverovatnije izmenjenih informacionih tokova. To se najčešće realizuje statističkom analizom korišćenjem napredne statističke tehnike.

Najjednostavniji metod detekcije modifikovanih fajlova je njihovo upoređivanje sa originalima. Suština detektovanja informacije je kretanje kroz grafičke prikaze na *Web* sajtovima. Analitičar može sačuvati poznate čiste kopije tih materijala i uporediti ih sa aktuelnim sadržajima na sajtu. Razlike, pod pretpostavkom da je nosilac isti, će sačinjavati skrivenu tajnu informaciju.

Generalno, upotreba visokog nivoa kompresije čini steganografiju teškom za otkrivanje, ali ipak ne nemogućom. Dok postupak kompresije obezbeđuje dobro mesto za skrivanje podataka, visoka kompresija ipak smanjuje količinu podataka raspoloživih za skrivanje tajne poruke.

Skrivanje informacija unutar jednog elektronskog nosioca podataka uzrokuje promene osobina nosioca koje mogu rezultirati nekim oblikom degradacije ili neuobičajenom karakteristikom.

Za detekciju postojanja skrivenih poruka, u steganoanalizi se koriste **metodi zasnovani na uočavanju promena**. Prema vrsti promena razlikuju se sledeći metodi:

- vizuelna detekcija (fajlovi sa ekstenzijom *jpeg*, *bmp*, *gif*),
- zvučna detekcija (fajlovi sa ekstenzijom *wav*, *mpeg*),
- statistička detekcija (promena u šablonu piksela ili *LSB*) ili analiza histograma i
- strukturna detekcija ili detekcija neobičnih struktura (pregled sadržaja fajla, njegove dužine, promena datuma i vremena, modifikacije sadržaja i provera sume-graničnog broja bita).

Vizuelna i zvučna detekcija ne pružaju neke ozbiljne mogućnosti steganoanalize. Mnogi jednostavni steganografski alati rade u domenima slika i biraju bitove poruke u nosiocu

nezavisno od sadržaja nosioca. Iako je lakše sakriti poruku u delovima svetlijih boja ili glasnije muzike, program možda neće pokušati da izdvoji te delove. Vizuelna inspekcija može biti dovoljna za odbacivanje sumnje sa steganografskog medijuma⁵⁰. Statistička i strukturna detekcija spadaju u ozbiljnije metode i za njih postoje instrumentalizovani alati i programi.

Vizualna detekcija se zasniva na analiziranju i upoređivanju originalnog nosioca sa stego slikom (stego nosiocem) i zapisivanju vidljivih promena, što je poznato kao "napad kada je poznat nosilac". Prilikom upoređivanja mnogobrojnih slika moguće je da se modeli pojave kao potpisi steganografskog alata. Ako slike nosioci nisu raspoložive za upoređivanje, dobijeni poznati potpisi su dovoljni da označe postojanje skrivene poruke i za identifikaciju alata korišćenog za utiskivanje poruke. Detekcija ovih potpisa može biti automatizovana unutar alata za detekciju steganografije. Stegodetekcija upoređuje paletu modela i potpisa i analizira fotografije koje se ističu od drugih fotografija u svojoj oblasti.

Drugi oblik vizuelne detekcije za prisustvo skrivenih informacija je dopunjavanje ili odsecanje slike. Sa nekim stego alatima, ako slika nije potrebne veličine, ona se dopunjava ili odseca. Drugi indikator je veliki porast ili smanjenje u broju jedinstvenih boja.

Statistička analiza zasniva se na statističkim testovima koji mogu otkriti da je slika modifikovana steganografijom, utvrđivanjem da statističke osobine slike odstupaju od pravila. Neki testovi su nezavisni od formata podataka i samo određuju entropiju suvišnih podataka. Kod analize se očekuje da slike sa skrivenim podacima imaju višu entropiju nego nemodifikovane slike. Na današnjem stepenu razvoja steganoanalize, statistička analiza daje najveće mogućnosti u detekciji steganografskih sadržaja. U ovoj oblasti veliki doprinos dali su *Niels Provos* i *Peter Honeyman* iz Centra za informacione tehnologije objedinjenog univerziteta u Mičigenu u svom radu "**DETEKCIJA STEGANOGRAFSKIH SADRŽAJA NA INTERNETU**". Ovaj rad kao osnovu u istraživanjima koriste mnogi naučni istraživači u oblasti steganoanalize.

Statistička analiza slika i audio fajlova može pokazati da li statističke osobine fajla bivaju deformisane u odnosu na očekivanu normu. Ova takozvana statistika prvog reda, varijacija, hi kvadrat test (X^2), meri vrednost suvišnih informacija i/ili deformaciju u medijumu. Iako ova merenja mogu doprineti prognozi poput one da li je sadržaj bio menjan ili izgleda sumnjivo, ona nisu konačna⁵¹.

Statistička steganoanaliza je teško izvodljiva zato što se neki steganografski algoritmi muče da bi očuvali nosioca fajla statistike prvog reda kako bi izbegli ovu vrstu detekcije. Šifrovanje tajne poruke takođe čini detekciju težom zato što šifrovani podaci imaju visok stepen slučajnosti, jedinice i nule se pojavljuju sa jednakim mogućnostima⁵².

Obnavljanje tajne poruke dodaje nov sloj kompleksnosti u poređenju sa jednostavnom detekcijom prisutnosti tajne poruke. Obnavljanje poruke zahteva poznavanje ili procenu dužine poruke i, ako je moguće, šifrovani ključ i poznavanje krypto algoritma.

Specifičnost algoritma nosioca fajla može analizu učiniti jasnijom. JPEG je privukao veliku pažnju istraživača zbog načina na koji različiti algoritmi deluju na ovaj tip fajla. JPEG je loš medijum kada se koristi jednostavno ubacivanje LSB zato što promena u fajlu olakšava detekciju skrivenih informacija. Postoji par algoritama koji kriju informacije u JPEG fajlovima i oni funkcionišu na drugačiji način.

Jsteg senkvencijalno ugrađuje skrivene podatke u najmanje važne bitove, JP Hide&Seek koriste slučajne procese za selekciju najmanje važnih bitova, F5 koristi matrično šifrovanje bazirano na Hamingovom kodu, dok OutGuess brani statistiku prvog reda.

⁵⁰ Wayner, 2002 [51]

⁵¹ Wayner, 2002 [51]

⁵² Farid, 2001 [24]

Napredni statistički testovi koriste statistiku višeg reda, linearnu analizu, Markovljeva slučajna polja, statistiku različitih talasa itd. Diskusije koje su vođene na ovu temu nisu dostupne javnosti iz bezbednosnih razloga, ali se rezultati istih mogu uočiti u pojedinim alatima za detekciju steganografije. Steganografski metodi za digitalne medije mogu se široko klasifikovati kao operateri u domenima slike ili transformacionim domenima. Alati u domenima slike kriju poruku u nosiocu manipulacijom bitovima, poput zamene najmanje važnog bita. Alati za transformacijske domene manipulišu steganografskim algoritmima, poput diskretne kosinusne transformacije koeficijenata u JPEG slikama.

Iz ovoga sledi da steganoanaliza široko prati način na koji steganografski algoritmi funkcionišu.

Steganografske tehnike menjaju statistiku nosioca i velike ili duge sakrivene poruke će više promeniti nosioca nego one manje. Statistička analiza je obično korišćena za detekciju sakrivenih poruka, posebno kada se analiza radi na slepo⁵³. Veliki broj ljudi radi u oblasti statističke analize.

Neobične strukture u stego slikama su sumnjive. Na primer, postoje neki uslužni programi za disk analize koje mogu filtrirati skrivene informacije u nekorišćenim particijama u načinu skladištenja. Filteri takođe mogu biti korišćeni za identifikaciju *TCP/IP* paketa koji sadrže skrivene ili nevažeće informacije u zaglavlju paketa. *TCP/IP* paketi u toku prenosa informacija kroz Internet imaju nekorišćen ili rezervni prostor u zaglavlju paketa. Zaglavlja paketa se retko čitaju od strane regularnih korisnika i tako čine idealno mesto za skrivanje podataka. Nedostatak korišćenja ove metode skrivanja podataka je da *firewalls* mogu biti konfigurisani za filtriranje paketa koji sadrže nepodesne podatke u rezervnom polju. Osim toga, skrivanje informacija u zaglavlju paketa je nepouzdan zato što je moguće da *TCP/IP* zaglavlja, i rezervni biti, u toku rutiranja budu nadopunjeni, što bi degradiralo steganografski prenos. LSB u slikama baziranim na paletama najčešće su razlog velikog broja dupliranih boja, gde identične, ili najbliže identične, boje se dva puta pojavljuju i ne slažu se jedino u najmanje važnom bitu. Steganografski programi koji kriju informaciju jedino manipulacijom reda boja u paleti prouzrokuju strukturalne promene. Strukturalne promene često kreiraju potpis steganografskog algoritma koji je korišćen⁵⁴.

Tehnike steganoanalize mogu biti klasifikovane na sličan način kao kriptanalitički metodi, u najvećoj meri bazirani na to koliko informacija znamo⁵⁵.

- ✓ Napad na steganografiju: steganografski medijum je jedina stavka dostupna za analizu
- ✓ Napad na poznatog nosioca: nosilac tajne poruke i steganografski medijum su stavke dostupne za analizu
- ✓ Napad na poznatu poruku: poznata je tajna poruka
- ✓ Napad na odabranu steganografiju: steganografski medijum i algoritam su poznati
- ✓ Napad na odabranu poruku: poznata poruka i steganografski algoritam su korišćeni za kreiranje steganografskog medija za dalju analizu i poređenje
- ✓ Napad na poznatu steganografiju: poznati su nosilac, steganografski medijum i steganografski algoritam

Mnoge savremene steganoanalitičke tehnike su bazirane na potpisu, sličnom antivirusima i sistemima za detekciju upada (IDS/IPS). Steganoanalitički sistemi bazirani na anomalijama tek izbijaju na površinu. Iako su raniji sistemi precizni i čvrsti, noviji će biti

⁵³ Jackson i sar., 2003 [31]

⁵⁴ Wayner, 2002 [51], Jackson i sar., 2003 [31]

⁵⁵ Curran i Bailey, 2003 [17], Johnson and Jajodia 1998 [33]

fleksibilniji, bolji i brže će moći da odgovore novim steganografskim tehnikama. Forma zvana „slepa steganografska detekcija“ raspoznaje razlike između čiste i steganografske slike koristeći statistiku baziranu na dekompoziciji različitih talasa ili ispitivanjem prostora, orijentacije i razmera kroz podskup većih slika.⁵⁶

Zajednica zakonskih snaga nema uvek taj luksuz da zna gde i kada je korišćena steganografija ili koji je algoritam korišćen. Opšti alati koji mogu detektovati i klasifikovati steganografiju su još uvek u razvoju, ali polako postaju dostupni u softverskim alatima.

Kripto svet je začaran krug – steganoanaliza pomaže u pronalaženju ugrađene steganografije ali, takođe, predstavlja nove steganografske algoritme za izbegavanje detekcije.

2.1.9. Tipovi napada na steganografske sisteme

Napadi i analize na skrivene informacije mogu imati nekoliko oblika: detekcija, izdvajanje ili uništavanje skrivene informacije. Pod pojmom "razbiti" steganografski sistem podrazumevaju se tri radnje: detekcija postojanja skrivene informacije, izvlačenje informacije iz nosioca i njeno dešifrovanje. Sistem je već postao nesiguran ako je napadač u stanju samo da dokaže postojanje tajne informacije. Polazna pretpostavka je da napadač poseduje neograničene računarske resurse i u stanju je da primeni raznovrsne algoritme napada. U slučaju da on ne može da potvrdi svoju hipotezu da je tajna poruka implementirana u nosioca, tada govorimo o teorijski sigurnom sistemu.

Napadi na steganografske sisteme u odnosu na krajnji cilj napadača, mogu se teoretski podeliti na tri vrste: pasivne, aktivne i namerne.

U **pasivne napade** spada ona grupa tehnika koje samo detektuju postojanje tajne poruke. Ovakav zadatak se formalno može predstaviti kao problem statističkog testiranja hipoteza. Napadač (prisluškiivač), mora definisati test funkciju koja kao rezultat daje vrednost koju koristi da klasifikuje nosioce koji su emitovani javnim kanalom. Postoje dve mogućnosti greške u statističkom testiranju hipoteza. Greška I-vrste nastaje kada se detektuje postojanje tajne poruke u nosiocu, a ona stvarno ne postoji. Greška II-vrste nastaje kada se ne detektuje postojanje tajne poruke, a ona stvarno postoji. U praksi steganografski sistemi se trude da maksimizuju verovatnoću da napadač napravi grešku II-vrste.

Prilikom projektovanja steganografskog sistema posebna pažnja se mora posvetiti aktivnim i namernim napadačima. Aktivni napadači predstavljaju one napadače koji su u stanju da modifikuju stego nosioca u toku prenosa. Opšta pretpostavka je da aktivni napadači ne smeju previše modifikovati stego paket jer će u tom slučaju perceptulane i semantičke osobine biti narušene, već mogu vršiti samo manje izmene odnosno prepravke.

Steganografski sistemi su često jako osetljivi na modifikacije stego paketa, kao što su digitalno procesuiranje, filtriranje, usrednjavanje, komprimovanje, prebacivanje iz formata u format. Čak i kompresije sa minimalnim gubicima mogu izazvati potpuni gubitak tajne informacije, jer one baš uklanjaju one neprimetne komponente signala u kojima se najčešće vrši utiskivanje tajne poruke.

Aktivni napadač, koji često nije u stanju ni da detektuje postojanje tajne poruke, može dodati slučajan signal u stego nosiocu i uništiti tajnu informaciju. Napadači mogu biti slučajni i namerni. Kao primer slučajnog napadača može se navesti slučajan šum koji se akumulira prilikom emitovanja signala nekim od spojnih puteva. Sve navedene tehnike mogu oštetiti ili onemogućiti tajnu komunikaciju. Zbog toga jedan od značajnih zahteva koje steganografski sistem mora da ispuni je robusnost. Sistem se naziva robusnim ako se utisnuta tajna informacija ne može oštetiti bez drastičnih promena stego nosioca.

Potrebno je naglasiti da postoji kompromis između sigurnosti, tj. tajnosti i robusnosti. Što je sistem robusniji na modifikaciju nosioca, to je on manje siguran. To se objašnjava na

⁵⁶ Jackson i sar., 2003 [31], Farid, 2001 [24]

taj način što robusnost zahteva da se vrši implementacija redundantne informacije, koja će dosta narušiti statističke karakteristike nosioca i time prouzrokovati smanjenje verovatnoće greške II vrste. Jednostavno rečeno, sigurnost zahteva da tajnu informaciju sakrijete u oblasti koje su perceptualno neprimetne, dok robusnost zahteva baš suprotno da tajnu informaciju sakrijete u oblasti koje su perceptualno primetne jer će tako biti teže oštetiti informaciju bez velike degradacije kvaliteta nosioca.

Mnogi sistemi se dizajniraju tako da budu robustni na određene karakteristične tipove napada, kao što je kompresija, dekompresija, filtriranje, dodavanje šuma. Idealan sistem bi trebao da bude robustan na sve vidove napada - što bi bilo jako teško napraviti.

Generalno postoje dva principa da se napravi robustan steganografski sistem. Kod prvog sistema vrši se predviđanje mogućih napada i zatim se projektuje takav postupak implementacije tajne poruke koji je robustan na tu vrstu modifikacija, tako da modifikacija ne uništi u potpunosti informaciju. Druga strategija je da se primene inverzne modifikacije, od onih koje su korišćene tokom napada, kako bi se rekonstruisala originalna tajna informacija.

U prisustvu ***namernih napadača*** robusnost nije dovoljna. Namerni napadači su svi oni napadači koji pokušavaju da falsifikuju poruku ili da startuju steganografski protokol lažno se predstavljajući kao komunikacioni partner. U slučajevima kada proces implementacije ne zavisi od neke tajne informacije koju poznaju samo pošiljalac i primalac, namerni napadač može falsifikovati poruku, s obzirom da primaoc nije u mogućnosti da verifikuje ispravnost identiteta pošiljaoca. Da bi se ovo predupredilo, algoritam za utiskivanje mora biti robustan i siguran.

Zbog toga se pred siguran steganografski sistem postavljaju četiri osnovna zahteva koje mora da ispuni i to:

1. Poruke se moraju implementirati u nosioce korišćenjem javnih algoritama i tajnih ključeva, a tajni ključ mora jedinstveno identifikovati pošiljaoca.
2. Jedino vlasnik ispravnog ključa može detektovati, izdvojiti i dokazati postojanje tajne poruke. Niko drugi ne bi trebalo da bude u stanju da pronađe ikakav statistički dokaz da tajna poruka postoji.
3. Ako napadač uspe da selektuje sadržaj jedne skrivene poruke, ne sme biti u stanju da detektuje ostale.
4. Kompjuterski je neizvodljivo detektovati tajnu poruku.

2.1.10. Steganografski programi

StegoMagic 1.0

StegoMagic može sakriti bilo koji fajl ili poruku u tekstualni fajl, wav fajl, 24-bitnu BMP sliku i BMP sliku sa 256 boja. Pri korišćenju ovog programa ne dolazi do promene veličine fajla nosioca izuzev kada je nosilac tekstualni fajl. Ne dolazi do primetnih izobličenja nosioca nakon sakrivanja željenog fajla, što znači da će nosilac izgledati tačno kao original i zbog toga je gotovo nemoguće otkriti skrivene podatke. Podaci se kodiraju DES algoritmom.

Podaci koji se kriju moraju biti približno veličine 1/8 nosioca ili manji. Izuzetak predstavljaju nosioci tekstualnog tipa. Moguća je zaštita podataka šifrom.

StegoMagic se može pokrenuti na svim Microsoftovim platformama.

MP3Stego

MP3Stego omogućava sakrivanje informacija u mp3 fajlovima tako što se kompresija vrši uz pomoć MPEG Audio Layer III formata. Podaci se kriju u mp3 fajlove u toku kompresionog procesa. Podaci se prvo kompresuju, šifruju i onda sakrivaju u mp3 fajl. Iako je MP3Stego pisan steganografskom aplikacijom, on može biti korišćen i u svrhe zaštite mp3 fajlova poput vodenog pečata. Svako može dekompresovati i kompresovati fajl i na taj način

uništiti skrivenu informaciju, jer to su jedini poznati napadi koji su poznati na ovaj tip fajla, ali u tom slučaju se veoma gubi na kvalitetu.

Ovaj program koristi mp3 dekodier *dist10* od ISO MPEG podgrupe za simulaciju softvera, standard ISO/IEC 11172-3:1993 koji definiše šifrovanje i digitalno skladištenje audio medija i 3DES algoritam.

GRL RealHidden Version 1.0

Ovaj program je veoma jednostavan za upotrebu. Potrebno je izabrati akciju odn. sakrivanje ili izvlačenje sakrivenog fajla iz nosioca. Nosilac može biti fajl gotovo svih formata JPG, BMP, GIF, MP3, WAV, EXE itd., ali se preporučuje provera nosioca nakon umetanja tajne poruke, jer može doći do greške pri otvaranju. Prema ranije navedenom u radu, najbolje je za nosioca izabrati neki od slikovnih formata, jer izvršni fajlovi često neće raditi ukoliko se menjaju bitovi u njemu.

Ovaj program je interesantan zato što u završnom koraku nudi mogućnost brisanja izvornog fajla i kompresovanje izlaznog i na taj način otežava detekciju sakrivenog sadržaja.

Wb4Stego

Kao fajlove nosioce ovaj program koristi .bmp fajlove, tekstualne fajlove, HTML i PDF fajlove. Kriptografija je primenjena pre šifrovanja i na taj način obezbeđena je visoka sigurnost. Iako neko ima saznanja da je sakrivena poruka u nosiocu, ne može je dešifrovati bez šifre. *wbStego4* nudi šifrovanje i razne algoritme koji su kompatibilni sa ranijim verzijama ovog programa, *wbStego 2.x* i *3.x*, kao i četiri algoritma za jaku kriptografiju: Blowfish, Twofish, CAST128, Rijndael (AES). Ovim se omogućava zaštita šifrom koja može imati i do 2 biliona karaktera, u ranijim verzijama do 256 karaktera. Ako se iskoristi jak algoritam za šifrovanje, ključ se generiše iz šifre korišćenjem heš algoritma SHA-1. Što je šifra duža i što više različitih karaktera i brojeva sadrži veća je sigurnost

2.1.11. Alati za detekciju steganografije

Gargoyle

Gargoyle je program razvijen od strane *WetStone Technologies* 2004. godine, ranije *StegoDetect*, i može se koristiti za detekciju prisustva steganografskih sadržaja. Gargoyle primenjuje zaštićen skup podataka svih fajlova iz poznatih rasprostranjenih steganografskih softvera, upoređujući ih sa pomešanim fajlovima predmeta koji se istražuje. Gargoyle skup podataka može biti korišćen i za detekciju prisustva kriptografije, hitnih poruka, ključa za zapisivanje u operativni registar, trojanskog konja, krekovanih lozinki i drugih zlonamernih softvera.

EnCase

Ovaj program omogućava pretraživanje, lociranje i sortiranje prema zadatim parametrima svih slika koje postoje na računarima, diskovima, magnetnim medijumima ili web sajtovima, uključujući steganografske fajlove, izbrisane fajlove, zanemarene fajlove i nealocirane prostore. Posebno je popularan u sudskim i inspeksijskim organima zbog toga što omogućava upravljanje velikom količinom raznih evidencija i dokaza u računarima i prikaz na osnovu zadatih parametara.

Stegdetect

Stegdetect je program razvijen od strane Niela Provos-a. Ovo je popularni automatizovani alat za detekciju steganografskog sadržaja u slikama. Niel Provos je autor i steganografskog programa *OutGuess*. Stegdetect je program za detekciju podataka skrivenih u JPEG slikama zasnovan na određenim steganografski baziranim aplikacijama. Omogućava

detekciju JSteg, JPHide (unix i windows), Invisible Secrets, OutGuess 01.3b, F5 (analiza zaglavlja), AppendX and Camouflage. OutGuess 0.2 nije detektovan statističkom analizom.

Iako još uvek nedostupan, Institut za bezbednost tehnologija na Dartmut koledžu, je razvio softver sposoban da detektuje sakrivene podatke u slikama koristeći statistički model koji je nezavisan od formata slike ili steganografske tehnike. Ovaj program je testiran na 1800 slika i četiri različita steganografska algoritma i bio je u mogućnosti da detektuje prisutnost sakrivenih poruke sa 65% preciznosti i procentom lažne uzbune manjom od 0.001.

DIGITALNI VODENI PEČAT

2.1.12. Digitalni vodeni pečat kroz istoriju

Termin „Vodeni pečat“ najverovatnije potiče od nemačkog termina „*wassermarke*“⁵⁷ i prvi put se pojavljuje krajem 18. veka. S obzirom na to da vodeni pečat nema uticaja na stvaranje pečata, ovo ime mu je najverovatnije dato zato što pečati liče na efekte vode na papiru.

Vodeni pečat postoji od pre 700 godina u vidu vodenog pečata koji se ručno nanosio na papir. Izvor najstarijeg vodenog pečata na papiru je grad Fabrian u Italiji i datira iz 1292 godine. On je imao glavnu ulogu u evoluciji industrije papira. Krajem 13. veka oko 40 papirnih industrijskih fabrika su delile tržište u Fabrianu i proizvodile papir različitih formata, kvaliteta i cena. Kako je konkurencija rasla postalo je teško identifikovati papir različitih proizvođača. Uvođenje vodenog pečata bio je savršen metod za eliminisanje bilo kakve nedoumice. Pečati su pravljeni dodavanjem šare od tanke žice u papirni kalup. Papir bi bio neznatno deblji u delu gde je umetnuta žica i stoga transparentniji. Nakon ovog izuma, vodeni pečat se ubrzo proširio u Italiji, a zatim i po celoj Evropi i iako je s početka korišćen za ukazivanje na brend papira ili proizvođača, kasnije služi za nagoveštavanje formata, jačine i kvaliteta. Do danas tehnike papirnog vodenog pečata su široko korišćene u celom svetu za obeležavanje autentičnosti novca. 1779. *Gentleman's Magazine* je preneo da je čovek po imenu Džon Metison (engl. John Mathison):

„ ... otkrio metod za falsifikovanje vodenog pečata bankovnog papira, koji je zamišljen kao princip za zaštitu od prevara. On ovo otkriće nudi kao mogućnost za otkrivanje, i učenje, sveta na koji način može otkriti prevaru, uz izvinjenje, koje, međutim, nije bilo upućeno banci.“

Džon Metison je sutradan obešen.

David Kahan u svojoj knjizi nudi interesantne istorijske beleške⁵⁸. Jedna relevantna priča opisuje poruku sakrivenu u knjizi *Hypnerotomachia Poliphili* koja je anonimno objavljena 1499. Prva slova svakog poglavlja daju rečenicu „Poliam Frater Franciscus Columna Permarvit“. Prevodi su različiti, za najmerodavniji se uzima „Otac Frančesko Kolumna koji voli Polia“.

1954. Emil Hembruk patentirao je vodeni pečat za muzička dela. Identifikacioni kod insertovan je u muziku naizmeničnim dodavanjem malih useka centriranih na 1 kHz. Ovaj metod zaštite objavljen je 1961. godine u *U.S. Patent*⁵⁹. 1984. godine posumnjalo se da se ovaj metod koristi za slanje reklamnih poruka u podsvest slušaoca.

Koncept papirnog vodenog pečata je primenjen i na digitalni vodeni pečat (u daljem tekstu DVP) u kompjuterskoj eri.

Teško je definisati kada je prvi put diskutovano o DVP-u.

⁵⁷ Simpson J. i Weiner E., 2000. [46]

⁵⁸ David Kahn, 1967. [21]

⁵⁹ Emil Frank Hembrooke, 1967. [23]

1979. Szepanski je opisao mašinski-detektibilnu šaru koja bi mogla da bude smeštena u dokumente u anti-falsifikacione svrhe.

1988. Holt i saradnici opisali su metod za ugrađivanje identifikacionog koda u audio signale.

1988. Kamacu i Tominaga su prvi put upotreбили izraz DVP.

1993. Tirkel i sar.⁶⁰ predstavljaju dve tehnike za sakrivanje podataka u slikama. Oba metoda su bili bazirani na modifikaciji najmanje važnih bitova (*engl. last significant bit – LSB*) u vrednostima piksela.

1995. interesovanje za DVP je počelo ubrzano da se razvija. U dijagramu 1. prikazan je histogram broja listova izdatih na ovu temu.⁶¹

1996. je izdata prva knjiga sa temom „Radionica za sakrivanje informacija“, u kojoj je glavna tema bila DVP. Napisao ju je R. Anderson.

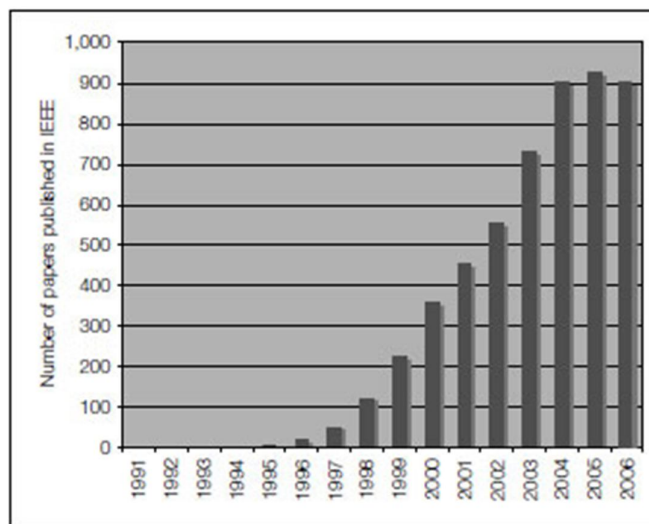
1999. SPIE⁶² je na konferenciji posvetio posebnu pažnju bezbednosti i ugrađivanju vodenih pečata u multimedijalne sadržaje.

1999. radna grupa za zaštitu kopiranja - CPTWG (*engl. Copy Protection Technical Working Group*) testira primenu vodenog pečata za zaštitu video formata na DVD diskovima. Inicijativa za zaštitu digitalne muzike - SDMI (*engl. Secure Digital Music Initiative*) je napravila vodeni pečat koji je služio kao centralna komponenta za zaštitu muzike.

Dva projekta sponzorisa je Evropska unija: VIVA i Talisman. Oba projekta služila su za monitoring radio emitovanja.

Međunarodna organizacija za standarde – ISO (*engl. International Organization for Standardization*) zainteresovala se za primenu tehnologije DVP-a u MPEG standardu.

2006. Filips elektronik odnosi još jednu pobjedu. Njihov tim razvija vodeni pečat za video sadržaje, CineFence, koji je dizajniran da skuplja standarde za digitalne bioskope DCI⁶³. Kopije ili piratski filmovi koji se prave nelegalnim putem, preko digitalnog projektora mogu se pratiti do bioskopa u kom su se prikazivali sa tačnim datumom i vremenom.⁶⁴



Dijagram 1. – Godišnji broj listova izdatih na temu steganografije i DVP na osnovu IEEE

⁶⁰Tirkel i sar, 1993. [49]

⁶¹ Carol Carr and Patricia E. O'Neill, c 1995 [10]

⁶² SPIE -Society of Photographic Instrumentation Engineers – Neprofitno internacionalno udruženje za raymenu, sakupljanje i širenje znanja u oblasti optike, fotonike i izumnog inženjeringa

⁶³ DCI- Digital Cinema Initiatives

⁶⁴ <http://www.drmwatch.com/drmtech/article.php/3587141>

2.1.13. Značaj DVP-a

Iznenadno zanimanje za PVD počelo je kada se došlo do saznanja da je njegova upotreba u zaštiti prava intelektualne svojine mnogostruka. Internet je postao društveno prihvatljiv uvođenjem web pretraživača od strane Mark Andersena 1993⁶⁵ i tada je postalo jasno da ljudi žele da skidaju digitalne sadržaje sa Interneta. On predstavlja odličan sistem za distribuciju digitalnih medija jer je jeftin, ne postoji nepotrebno skladištenje, gomilanje zaliha, a isporuka je gotovo trenutna.

Zbog ovakvog stanja, vlasnici sadržaja, posebno muzičkog i video, uvideli su rizik zbog moguće piraterije.

Rizik od piraterije je pogoršan obiljem visokokapacitivnih digitalnih uređaja za snimanje. Dok je jedini način za nasnimavanje pesme ili filma prosečnom kupcu bila dostupna analogna traka, piratske kopije bile su uglavnom lošijeg kvaliteta u odnosu na original. Međutim, sa uređajima sa digitalnim snimanjem, pesme ili filmovi mogu biti snimljeni sa malo ili čak bez degradacije u kvalitetu. Koristeći digitalne uređaje i Internet kao mesto distribucije, piraterima se omogućava distribucija materijala zaštićenih autorskim pravima, bez odgovarajuće kompenzacije koja bi trebala da bude isplaćena vlasnicima. Stoga, vlasnici sadržaja su u stalnoj potrazi za tehnologijama koje obećavaju zaštitu njihovih prava.

Prva tehnologija koja je ponudila zaštitu prava je kriptografija. Nedostatak kriptografije je bio taj što ako bi pirateri naručili proizvod, sa njim bi dobili i ključ za dešifrovanje, što bi im dalje omogućilo neometanu distribuciju na internetu ili digitalnom mediju. Zbog toga se javila potreba za tehnologijom koja može štititi sadržaj i nakon dešifrovanja. Vodeni pečat je imao potencijal da upotpuni ovaj nedostatak zato što on smešta informaciju unutar sadržaja i ne uklanja se prilikom normalne upotrebe.

Dešifrovanje, ponovno šifrovanje, konvertovanje iz digitalnog u analogni format i promena formata fajla su samo neki od postupaka koje DVP može da preživi.

DVP je uzet u obzir za mnoge prevencije od kopiranja i zaštite aplikacija kopirajtom. U prevenciji kopiranja DVP se može koristiti za informisanje softvera ili hardvera da je određen sadržaj zaštićen autorskim pravima. U zaštiti aplikacija autorskim pravima DVP može biti korišćen za identifikaciju nosioca autorskih prava i na taj način se može osigurati odgovarajuća naplata.

Iako su prevencija kopiranja i zaštita autorskih prava bila osnovna u istraživanjima u oblasti DVP-a, postoje još mnoge oblasti u kojima se on može primeniti: u monitoringu emitovanja, praćenju transakcija, autentifikaciji sadržaja, kontroli kopiranja, monitoringu pronalazaka i ideja...

2.1.14. Primena i osobine DVP-a

DVP je veština neprimetne izmene nekog rada odn. ugrađivanja poruke o tom istom radu. On je karakteristika koja identifikuje sliku, audio fajl, film ili bilo koji drugi digitalni format. On je usko vezan sa delom informatike koja se bavi sakrivanjem informacija i steganografijom. Ova tri polja imaju odlično preklapanje. Sakrivanje informacija zahteva da bilo ko informaciju učini nevidljivom ili da zadrži tajnost postojanja poruke. Steganografija podrazumeva skriveno prenošenje informacija kroz raličite digitalne formate.

Primer steganografije je Herodotova priča koja govori o robu kog je poslao njegov vladar Histieus u Milet sa tajnom porukom koja mu je bila tetovirana na koži lobanje. Nakon tetoviranja sačekalo bi se da robu poraste kosa i nakon toga bi bio otpreman u Milet gde bi mu, da bi došli do skrivene poruke, ponovi brijali glavu. U ovom slučaju rob je služio samo kao medijum za prenos tajne poruke. Razlika između steganografije i DVP-a se može veoma dobro prikazati korišćenjem ovog primera.

⁶⁵ Abbate J., *Inventing the Web* [2]

Pretpostavimo da na robovoj glavi piše „Ovaj rob pripada Histeusu“. U ovom slučaju poruka obezbeđuje informaciju o robu što nas dovodi do definicije DVP-a. Ako bi bilo ko drugi pokušao da tvrdi da je rob njegovo vlasništvo, Histeus bi brijanjem glave robu dokazao svoje vlasništvo nad njim.

Ovim primerom pokazano je kako se DVP može koristiti za zaštitu autorskih prava. DVP se razlikuje od ostalih tehnika zbog svojih karakteristika:

1. Vodeni pečat se ne vidi.
2. Vodeni pečat je neodvojiv od zaštićenog rada načinom na koji je ugrađen.
3. Vodeni pečat prolazi kroz iste transformacije kao rad koji se štiti.

Cilj DVP-a je da proizvede podatke (sliku, audio i video) koji neće pretrpeti nikakvu ili minimalnu degradaciju kvaliteta, odn. biće gotovo identični originalnoj verziji pre ugrađivanja DVP-a.

DVP se može primeniti na mnoge načine. Generalno, ako želimo da on nosi podatke o Radu⁶⁶ metapodaci mogu biti unutar njega. Naravno, podaci o Radu se mogu smestiti u zaglavlje digitalnog fajla, mogu se kodirati vidljivim barkodom ili se umetnuti u audio klip kao glasovno upozorenje o polaganju autorskih prava. Na slici br. 10 dat je prikaz procesa ugrađivanja vodenog pečata.

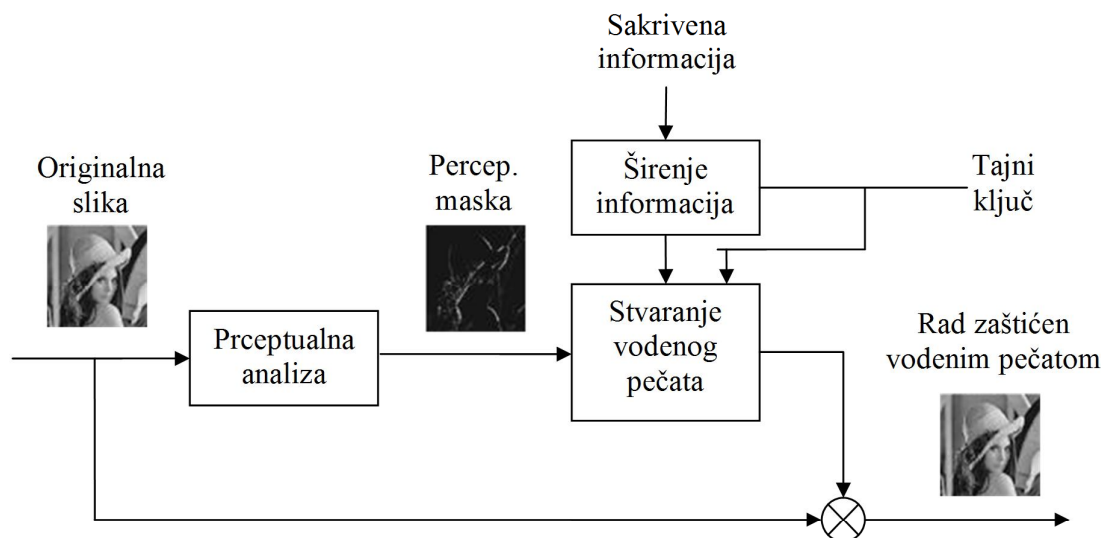
Da bismo uporedili razliku između DVP i drugih tehnika iskoristićemo već navedene karakteristike DVP⁶⁷:

1. DVP je nevidljiv za razliku od bar koda.
2. Neodvojiv je od Rada u koji je ugrađen za razliku od podataka dodatih u zaglavlje nekog dokumenta i iz tog razloga neće nestati nakon formatiranja.
3. On trpi transformacije kroz koje prolazi Rad za razliku od podataka koji su dodati u zaglavlje nekog dokumenta.

Performanse dodeljene sistemu DVP-a mogu biti promenjene na osnovu malih setova osobina. Npr. robusnost, ili otpornost, opisuje koliko dobro DVP podnosi uobičajeno delovanje signalnih procesa, sigurnost pokazuje koliko je DVP nevidljiv itd. Značaj ovih osobina zavisi od namene sistema, npr. ako je svrha detekcija DVP-a u kopiranom Radu koji je poslat preko analognog signala, DVP mora da bude otporan na degradaciju koja bi mogla da bude uzrokovana tim kanalom, ali ako osnovano očekujemo da Rad neće biti modifikovan između memorisanja i detekcije onda je otpornost irelevantna.

⁶⁶ Termin „Rad“ je u saglasnosti sa jezikom koji je korišćen u zakonu o kopirajtu u Sjedinjenim državama (United States Code, Naslov 17) i označava određenu kopiju nekog elektronskog signala (audio, video ili slikovnog).

⁶⁷ Strana 35.



Slika 10.- Ugrađivanje vodenog pečata

2.1.15. Primena DVP-a

Za svaki od osam primera identifikovaće se karakteristični problemi koji DVP čine odgovarajućim rešenjem.

2.1.15.1. Monitoring emitovanja

1997. izbio je skandal na japanskim TV stanicama koje se bave reklamiranjem. Najmanje dve stanice imale su rutinski prebukiran programski plan. Klijenti su im plaćali za preko hiljadu reklama koje nikada nisu objavljene.⁶⁸ Ova praksa je sprovedena neotkrivena preko 20 godina, delom zato što nije postojao sistem za monitoring realnog sprovođenja reklama.

Postoji više tipova organizacija i pojedinaca koji su zainteresovani za monitoring emitovanja:

- Klijenti koji žele da osiguraju vreme koje su platili u reklamnom bloku
- Izvođači s druge strane teže ka tome da osiguraju da su dobili zavidan broj firmi koje se reklamiraju kod njih

Metodi za praćenje emitovanja mogu se podeliti na: manuelne (slabotehničke) i automatizovane.

Manuelni metod za praćenje emitovanja je postavljanje ljudi koji će beležiti šta su videli ili čuli. Ovaj metod je skup i moguće su česte greške.

Tehnike za automatski monitoring su podeljene u 2 kategorije:

1. Pasivni monitoring sistem pokušava da direktno prepozna sadržaj koji je emitovan, tako da simulira ljudska zapažanja, ali na mnogo jeftiniji i sigurniji način.
2. Aktivni monitoring sistem se oslanja na povezane informacije koje se emituju uporedo sa sadržajem.

Do problema dolazi kada se upoređuju dobijeni signali sa bazom podataka postojećih pesama, filmova i sl. Ako izdvojimo neki frejm iz video zapisa i tražimo ga u bazi dolazi do problema iz razloga što jedan frejm može sadržati milione bita informacija, što je veoma nepraktično, jer tolike sekvence nisu dobre za pretragu u bazi. Stoga, sistem mora da obradi

⁶⁸ David Kilburn, 1997. [21]

primljene signale u manje potpise koji su dovoljno bogati informacijama za raspoznavanje između svih postojećih Radova u bazi.

Pored toga, emitovanje generalno degradira signale, što rezultuje višestruku osetljivost Rada u različitom vremenu i to može dovesti do različitih potpisa. Ovo znači da monitoring sistem ne može da traži istovetno poklapanje emitovanog signala sa onim koji je pohranjen u bazi. Umesto toga, on mora da prikaže najbližeg suseda u velikoj bazi, što znači da je veoma teško dizajnirati pasivni monitoring sistem koji je 100% pouzdan.

Kada bi se i rešio problem pretraživanja u bazi, skladištenja u nju i organizovanje baze bilo bi veoma skupo, jer bi takva baza bila veoma velika. Takođe, sistem bi trebao da nadzire nekoliko geografskih lokacija simultano. U Sjedinjenim državama postoji 120 televizijskih prodavnica. Stoga, svako mesto mora da ima pristup centralizovanoj bazi određenog Rada.

S obzirom da pasivni monitoring ne zahteva saradnju onih koji se reklamiraju, on dozvoljava monitoring servisu da sastavi spisak konkurentskih tržišta. Tako bi npr. Pepsi mogao da sazna koliko Coca-cola troši na reklamiranje u Atlanti. Ali zbog procentualne greške do koje može doći, nijedna kompanija ne koristi pasivni monitoring u ove svrhe.⁶⁹

Ostven i saradnici⁷⁰ su podneli izveštaj sa veoma interesantnim rezultatima vezanim za otisak prsta za audio format. Njihov rad je komercijalizovan od strane Filips korporacije i licenciran brojnim kompanijama kao što su Nilsenov sistem za emitovanje podataka, Musicwave, Optimus, Amena itd.

Aktivni monitoring je tehnički lakši za implementaciju od pasivnog. Identifikacija informacija je otvorena za pouzdano dešifrovanje i nije potrebna baza podataka za interpretiranje njenog značenja. Jedan od načina za implementaciju aktivnog sistema monitoringa je da se smeste identifikatori informacija u odvojene delove emitovanog signala.

Kao primer može se uzeti analogna televizija koja dozvoljava digitalnoj informaciji da bude dešifrovana u vertikalnom potisnom intervalu – VBI (*engl. Vertical blanking interval*). Ovaj deo signala, poslat između frejmova, nema efekta na sliku. **Nedostatak** je taj što ubačeni signali u VBI mogu biti problematični. U Sjedinjenim državama, nije uvek jasno ko ima pravo na upravljanje sadržajem u VBI. Oba satelitska i kablovska operatora tvrde da je njihovo. Američki zakon zahteva da distributeri dostave uži uvod njihovim klijentima i oni nisu u pravnoj obavezi da pruže više informacija o tome koje informacije koje mogu biti ubačene u VBI od strane provajdera sadržaja. Identifikacioni kod ubačen u VBI od strane oglašivača ili mreže neće biti zasigurno prenet. Pridodate informacije verovatno neće preživeti promene formata, kao što su konverzija iz analognog u digitalni format, bez modifikacije postojećeg hardvera. Ranije ovo nije bio značajan problem, ali se povećao sa prelaskom velikog broja televizijskih emitovanja sa analognog na digitalni prenos.

DVP je očigledno alternativni metod kodiranja identifikacionih podataka za aktivan monitoring. On ima prednost zbog toga što ne koristi pojedine segmente emitovanog signala već koristi postojeće sopstvene informacije i zbog toga je potpuno kompatibilan sa instaliranom osnovom opreme za emitovanje, uključujući i analogni i digitalni signal.

Primarni nedostatak je taj što je proces umetanja mnogo komplikovaniji nego smeštanje podataka u VBI ili u zaglavlje fajla. Takođe postoji zabrinutost, posebno u delu kreiranja sadržaja, da DVP može degradirati vizuelni ili audio kvalitet Rada. I pored toga postoje mnogobrojne kompanije koje obezbeđuju monitoring emitovanja baziran na vodenom pečatu. Teletrax nudi servis koji je baziran na video vodenom pečatu od Filipsa.

⁶⁹ Mogućnost greške je 5%, što predstavlja veliki procenat.

⁷⁰ Ostveen i sar., 2002 [39]

2.1.15.2. Identifikacija vlasnika

Tačna forma kopirajnt napomene je veoma važna.

Za **vizuelni Rad**, napomene moraju da izgledaju:

- „Copyright *datum vlasnik*;“
- „© *datum vlasnik*;“
- „Copr. *datum vlasnik*.“

Važno je napomenuti da korišćenje „(C)“ umesto „©“ ne služi istoj zakonskoj svrsi.

Za **zvučne zapise**, kopirajnt napomena je „® *datum vlasnik*“ i mora biti postavljena na površini fizičkog medija, nalepnici ili na pakovanju, kao i da se „daje razumno objašnjenje za polaganje prava na kopirajnt“.

Napomene za kopirajnt za **tekstualne forme** imaju nekoliko ograničenja, poput tehnologije za identifikovanje vlasnika Rada. Kao prvo, lako ih je ukloniti iz dokumenta kada se on kopira, čak i bez namere ili nelegalne radnje. Npr. profesor želi da iskopira stranice neke knjige i nenamerno propusti stranu koja sadrži na sebi znak kopirajnta, ili ukoliko neko iseče delove slike, posebno deo koji nosi podatak da je slika zaštićena, i postavi je na Internet, oni koji sliku budi skidali sa Interneta neće ni biti svesni da rade nelegalnu aktivnost. Još gora situacija je u audio izdanjima, gde je napomena o pravu na intelektualnu svojinu (*copyright*) smeštena na fizički medijum (disk, traku, zapis itd.) ili na pakovanju. Nijedna od ovih napomena naravno neće biti kopirana zajedno sa audio sadržajem. Neki audio sadržaji mogu postojati samo u elektronskoj formi, npr. na veb sajtu, gde fizički medijum ili pakovanje ne postoje.

Zato što vođeni pečat može biti nevidljiv i neodvojiv od Rada koji ga sadrži, on je prikladan za tekst za identifikaciju vlasništva. Ako korisnik Rada poseduje detektor vođenog pečata, on bi trebao da bude u mogućnost da identifikuje vlasnika tog Rada, čak iako je rad možda modifikovan na način koji bi trebao da ukloni tekstualnu napomenu o autorskim pravima.

Digimarc-ov vođeni pečat za slike je dizajniran sa određenom namenom. On uspešno rasprostranjuje distribuciju svog detektora vođenog pečata vezivajući se za Adobe-ov popularni program za obradu slika Photoshop. Kada *Digimarc*-ov detektor prepozna vođeni pečat on kontaktira centralnu bazu podataka preko Interneta i koristi vođeni pečat kao ključ da pronađe kontakt informacije vlasnika slike.

Legalna primena ovog sistema još uvek nije testirana u pravosuđu.

2.1.15.3. Dokazivanje vlasništva

DVP se, pored identifikacije vlasnika autorskih prava, može koristiti i za dokazivanje vlasništva.

Kao primer može se uzeti sledeća situacija: osoba X kreira sliku i postavi je na internet sajt, s tim što ju je pre toga obeležila „© 2009 X“. Osoba Y skida sliku sa interneta i uz pomoć programa za obradu zameni napomenu o autorskim pravima sa „© 2009 Y“ i tvrdi da je slika njegovo vlasništvo.

Ukoliko je osoba X pre postavljanja slike na internet registrovala sliku u Agenciji za zaštitu autorskih prava⁷¹ tako što im je poslala kopiju slike, koju su oni zajedno sa podacima o autoru smestili u centralno skladište, to bi moglo da predstavlja rešenje nastale situacije. S obzirom na visinu novčanog iznosa za registraciju u agenciji, većina se ne opredeljuje za ovaj način zaštite.

Takođe, ona je, da bi dokazala svoje autorsko vlasništvo, mogla da napravi foto negative u ranim fazama izrade slike, ali ako osoba Y zaista želi da dobije slučaj uz malo truda može napraviti sopstvene negative i priloži ih kao dokaz.

⁷¹ <http://www.autorskaagencija.com/>

U slučaju korišćenja samo DVP-a dokazivanje vlasništva nije moguće. Problem je taj što bilo ko može da detektuje postojanje DVP-a može i da ga ukloni.

Da bi se ovaj problem rešio potrebno je da onemogućiti upotrebu detektora. Kada osoba Y nema detektor, uklanjanje pečata može da bude ekstremno teško. Tako da kada bi osobe X i Y izašle pred sudiju, osoba X bi prikazala svoju kopiju originala slike. Njen original i sporna kopija bi nakon pregleda detektorom za DVP svakako detektovali postojanje vodenog pečata.

U slučaju da vodeni pečat osobe X ne može da se ukloni nakon detekcije, osoba Y je u mogućnosti da naruši verodostojnost. Kako naznačavaju Kraver i saradnici⁷² osoba Y može koristeći sopstveni sistem vodenog pečata da vodeni pečat napravi da izgleda kao da je pečat njegov i to na istom mestu na kom se nalazio pečat osobe X. Ovoj postupak bi trećoj strani onemogućio da sudi da li je slika vlasništvo osobe X ili Y.

Rešenje ove vrste problema je u pravljenju neznatne promene u izjavi osobe X. Umesto da pokušava da direktno dokaže vlasništvo ugrađivanjem „X je vlasnik slike“ u vidu vodenog pečata, treba da pokuša da dokaže da je jedna slika izvedena iz druge. Više o načinu na koji se to postiže biće u odeljku Sigurnost DVP-a. Ovim sistemom se postiže dokazivanje koja je slika original, odn. koja je prva nastala. Ovo je sigurniji i ubedljiviji način za dokazivanje od pravljenja foto negativa, jer osoba Y takođe može napraviti negative, ali ne i napraviti lažni original koji bi prošao ovu vrstu testa.

2.1.15.4. Praćenje transakcija (otisak prsta)

U ovoj oblasti primene DVP-a, vodeni pečat beleži jednu ili više transakcija koje su zauzele mesto u istoriji kopiranja Radova.

Najčešće se u literaturi o praćenju transakcija, osoba odgovorna za zloupotrebu nekog Rada naziva *izdajnikom*, dok se osoba koja dobije isti rad od izdajnika naziva *piraterom*. Kako ova razlika nije značajna kada se razmatraju druge primene DVP-a, nadalje će se koristiti termin *suparnik* kako bi se opisao neko ko pokušava da ukloni, onemogućiti ili falsifikuje vodeni pečat.

Praćenje transakcija se mnogo češće naziva **otisak prsta**, iz razloga što svaka kopija Rada može jedinstveno da se identifikuje, što je analogno ljudskom otisku prsta koji jedinstveno identifikuje osobu.

Postoji par tehnologija za praćenje transakcija koje ne potpadaju pod definicijom vodenog pečata. Jedna uobičajena alternativa za vodeni pečat je korišćenje vidljivog pečata. Visoko osetljivi poslovni dokumenti, poput biznis plana, ponekad sadrže u pozadini velike sive brojeve, sa različitim brojevima na svakoj kopiji. Ovi pečati se često nazivaju vodeni pečati zato što imaju fizičku sličnost sa papirnim vodenim pečatom, ali ne poseduju jednu od odlika koje su veoma bitne za vodeni pečat, a to je nevidljivost.

Jedan od primera upotrebe vodenog pečata za praćenje transakcija je slučaj DiVX korporacije. DiVX je prodao veći broj DVD plejera koji su imali implementiran platite-da biste-gledali poslovni model. Implementirali su jednu vrstu sigurnosne tehnologije kako bi predupredili pirateriju svojih diskova, a jedna od tih tehnologija je bio vodeni pečat dizajniran da prati transakcije. Svaki plejer koji je mogao da čita DiVX bi smestio jedinstveni vodeni pečat u svaki video koji bi bio pušten preko njega. Tako da, ako neko taj isti video kopira i prodaje ga na crnom tržištu, DiVX korporacija može nabaviti jednu od kopija i identifikuje suparnika tako što bi dekodirao vodeni pečat. DiVX vodeni pečat nije korišćen za praćenje suparnika pre nego što je DiVX korporacija prestala sa radom.

2004. Technicolor, divizija Tompsona, koristio je video tehnologiju vodenog pečata licenciranu od strane Filipisa za dodeljivanje vodenog pečata za svakog od 5.803 članova koji glasaju za najbolji film, najboljeg glumca itd. u okviru dodele Oskara. Svakom članu se

⁷² Craver S. i sar., 1996 [15]

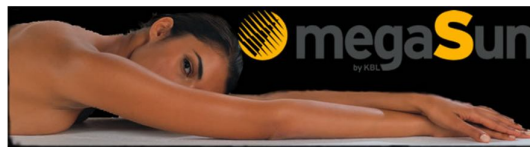
dostavlja kopija svih filmova u DVD ili VHS formatu. Nakon distribucije svih filmova, na internetu su se pojavile piratske verzije filmova: „Poslednji samuraj“, „Nešto mora da se da“, „Velika riba“ i „Mistična reka“. Analiziranjem ovih piratskih kopija otkriveno je da je originalni materijal bio materijal koji je poslat glumici Karmin Karidi⁷³. Njena izjava je bila da je kopiju poslala prijatelju Raselu Sragu i da nije znala da on namerava da napravi nelegalne kopije. Bez obzira na sve, ova sedamdesetogodišnja glumica je izbačena iz Akademije. Columbia pictures i Warner Bros su naknadno tužili Karmin. Warner Bros je dobio najvišu zakonsku odštetu od 150 000 dolara po naslovu u građanskoj tužbi.

2.1.15.5. Autentifikacija sadržaja

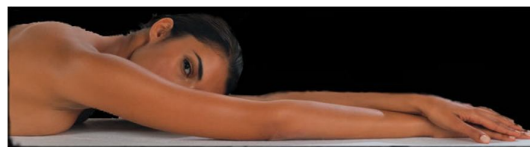
Sa porastom digitalnih Radova postalo je lakše falsifikovati ih i teže detektovati.

Na slikama 11 i 12 prikazana je izmena slike korišćenjem programa za obradu slika. Slika 11 je original, dok je slika 12 modifikovana verzija. Ukoliko bi slika 11 bila kritični dokaz u slučaju izvršenog kompjuterskog kriminala, u toku policijske istrage bi ova forma falsifikovanja mogla da izazove ozbiljan problem.

Isti se problem javlja i sa audio i video sadržajem.



Slika 11.- Slika sa logom



Slika 12.- Slika bez logoa

Problem izvorne poruke dobro je proučen u kriptografiji. Jedan od kriptografskih pristupa ovom problemu je kreiranje **digitalnog potpisa**, koji je u biti šifrovan pregled poruke. Za šifrovanje je korišćen asimetričan ključ, tako da se za dešifrovanje traži drugačiji ključ od onog koji je korišćen za šifrovanje. Samo autorizovan izvor poruke zna ključ potreban za dešifrovanje. Zbog toga, napadač koji pokušava da promeni poruku ne može da kreira drugi ključ. Ako neko naknadno uporedi promenjenu poruku sa originalnim potpisom, taj će naći da se ključevi ne podudaraju, a samim tim i da je poruka promenjena.

Fridman⁷⁴ predlaže kreiranje „sigurnosne kamere“ tako što bi se obračunavali potpisi u samoj kameri. Samo bi kamera imala ključ potreban za kreiranje potpisa. Ovi potpisi su metapodaci koji moraju biti preneseni zajedno sa Radom koji overavamo. Zbog toga je veoma lako izgubiti potpis u normalnoj upotrebi. Uzmimo u obzir slikovni autentifikacioni sistem koji metapodatke smešta u zaglavlje JPEG formata. Ako se slika konvertuje u drugi fajl format koji nema mesta za potpis u svom zaglavlju, potpis će biti izgubljen. Kada je potpis izgubljen, Rad nije autentičan.

Preporučljivije rešenje je ubacivanje potpisa direktno u rad posredstvom vodenog pečata.⁷⁵ Epson je ponudio takav sistem kao opcioni na mnogim svojim digitalnim kamerama. Ubačen potpis na takav način naziva se **autentični pečat**. Autentični pečat koji je dizajniran tako da postaje nevažeći nakon što se izvrši i najmanja promena Rada zove se **slab vodeni pečat**.

⁷³ Carmin Caridi- glumica koja je najistaknutiju ulogu imala u filmu Kum 3.

⁷⁴ Friedman G. L., 1993 [26]

⁷⁵ Macq B. M. i Quisquater J-J., 1995 [37]

Korišćenjem autentičnog pečata eliminiše se problem osiguranja da potpis ostane u Radu. Potrebna je opreznost da postupak postavljanja vodenog pečata ne promeni Rad toliko da se čini nevažećim kada se uporedi sa potpisom. Ovo se može usavršiti odvajanjem rada na dva dela: jedan u kom je obračunat potpis i drugi u kom je ubačen potpis.

Nekoliko autora predlaže obračunavanje potpisa od bitova višeg reda jedne slike i ubačenog potpisa u bitovima manjeg reda.⁷⁶

Ako Rad koji sadrži autentični pečat prođe kroz izmene, pečat će proći kroz njih zajedno sa Radom. Ako npr. Rad podelimo na više blokova i u svaki blok ubacimo autentični pečat, bićemo u mogućnosti da utvrdimo koji delovi su autentični, a koji su izmenjeni.

Primena autentičnog pečata moguća je i u policijskoj istrazi nekog kriminala. Recimo da policija dobije video nadzor sa izmenjenim sadržajem. Ako je snimak overen tradicionalnim potpisom, svi istražitelji će znati da je video lažan i da mu se ne može verovati. Ako je korišćen vodeni pečat dizajniran da propusti lokalnu autentifikaciju, onda istražitelji mogu otkriti da je svaki video frejm verodostojan, osim onog na kom je npr. registarska tablica na kolima. Ovo bi bio jak dokaz da je nečiji identitet u ovom zločinu uklonjen iz video snimka.

Drugi tip informacije mogao bi se izvesti ispitivanjem promenjenog autentičnog pečata, odn. ispitivanjem da li je pretrpeo kompresiju sa gubicima koja je primenjena na Rad. Kvantizacija primenjena od većine algoritama za kompresiju sa gubicima mogu ostaviti statističke promene na digitalnom vodenom pečatu koje bi mogle biti uočene ispitivanjem.

Nasuprot ovome, možda je istražiteljima nebitno da li je Rad bio kompresovan ili ne, već uzimaju u obzir da li su na Radu učinjene neke znatne promene.⁷⁷

Ovo vodi do oblasti **polu-slabih vodenih pečata** i potpisa, koji mogu da prežive veoma male transformacije, kao što su kompresija sa gubicima, ali su uništivi pri većim promenama.

2.1.15.6. Kontrola kopiranja

Većina primena koje su obrađene do sada imaju efekat samo nakon što neko uradi nešto pogrešno. Kontrola emitovanja pomaže za hvatanje nepoštenih emitera nakon što oni ne ispoštuju planiran blok reklama, praćenje transakcija identifikuje suparnike nakon što oni distribuiraju nelegalne kopije itd. Ove tehnologije služe za zastrašivanje kako se ne bi sprovodile zloupotrebe.

Kontrola kopiranja služi kao prevencija za sprečavanje ljudi da prave nelegalne kopije zaštićenog sadržaja.

Prva i najjača odbrana od ilegalnog kopiranja je šifrovanje. Šifrovanjem Rada jedinstvenim ključem, on postaje neupotrebljiv bilo kome ko nema taj ključ. Ključ bi se tada prosledio legitimnim korisnicima na način koji bi njima bio težak za distribuciju ili kopiranje.

Mnoge satelitske televizijske stanice su šifrovane. Ključevi za dešifrovanje su prosledeni svakom klijentu, koji je platio, u vidu smart kartice.

Postoje tri načina na koja bi suparnici mogli da savladaju šifrovan sistem:

1. Dešifrovanjem podataka bez posedovanja ključa, što je ujedno i najteži način
2. Nabavkom validnog ključa, što je nešto lakši način
3. Da legalno kupe ključ i kopiraju sadržaj nakon dešifrovanja

S obzirom na to da je vodeni pečat ubačen u sam sadržaj Rada, on je prisutan u svakom prikazivanju sadržaja i s toga može da obezbedi bolji metod za implementiranje kontrole kopiranja⁷⁸. Ako bi u sklopu svakog uređaja za snimanje bio detektor vodenog

⁷⁶ James M. Barton, 1997 [32]

⁷⁷ Za primer se mogu uzeti razlike između slika 12 i 13.

⁷⁸ Bloom i saradnici, 1999 [7]

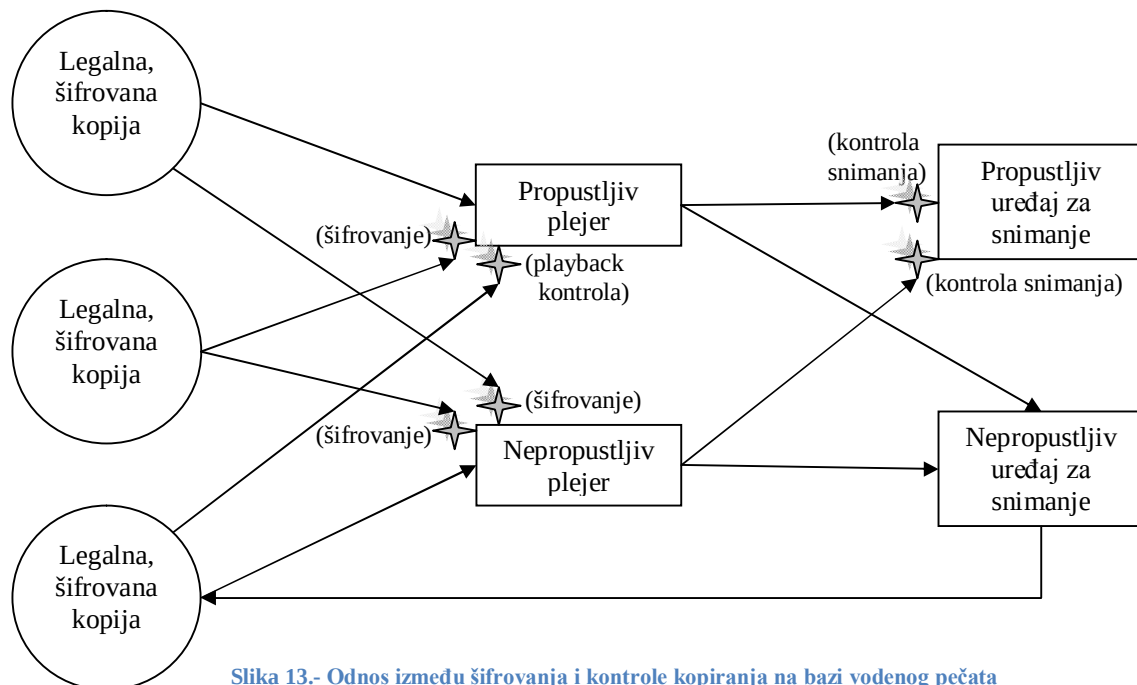
pečata, uređaji bi mogli da budu napravljeni tako da spreče snimanje kada god se detektuje nikada-ne-kopiraj vodeni pečat. Ova funkcija se ponekad naziva i *kontrola snimanja*. Takav sistem se primenjuje na video DVD-jeve od strane Radne grupe za tehničku zaštitu kopiranja – CPTWG (*engl. Copy Protection Technical Working Group*) i za zaštitu audio zapisa od strane Inicijative za sigurnost digitalne muzike - SDMI (*engl. Secure Digital Music Initiative*).

Problem koji se javlja u ovom slučaju jeste taj kako obezbediti da svi uređaji za snimanje sadrže detektor vodenog pečata. Problem nije samo do proizvođača zbog visoke cene implementacije, već i do potrošača, jer bi oni radije da poseduju uređaj koji ima mogućnost da pravi ilegalne kopije.

Direktno rešenje ovog problema jeste da se zakonski obavežu proizvođači da implementiraju detektore u svoje uređaje. Ovakav zakon ne postoji, ali i da postoji pravna bitka bi se vodila u svakoj zemlji pre nego što bi vodeni pečat mogao da obezbedi svetski poznatu zaštitu. Iz ovog razloga, ni CPTWG ni SDMI se ne oslanjaju na ovaj zakon. Umesto toga, oni postavljaju uslov da se detektor vodenog pečata ugrađuju u patente licencirane za tehnologije koje proizvođači žele da uključe u svoje uređaje. Tako da ako bi proizvođači DVD plejera ugradili detektor za vodeni pečat, pri puštanju nekog zapisa moglo bi se proveriti da li je Rad propisno šifrovan ili potražiti poseban potpis i ukoliko on ne postoji plejer bi se jednostavno ugasio. Ova ideja je poznata kao *playback kontrola*.

Na slici 13. prikazana je interakcija šifrovanja, kontrole snimanja i *playback* kontrole u svetu legalnih propustljivih i nepropustljivih uređaja. Linije prikazuju potencijalnu putanju sadržaja i one su određene šifrovanjem, kontrolom snimanja ili *playback* kontrolom.

Legalna, šifrovana kopija Rada, kao što je DVD kupljen u video radnji, može biti pušten na propustljivom plejeru, ali ne i na nepropustljivom, zato što ga on ne može dešifrovati. Izlaz iz propustljivog plejera ne može biti snimljen na propustljivom uređaju za snimanje, zato što bi on detektovao vodeni pečat i ugasio se, ali takav sadržaj može biti snimljen nepropustljivom uređaju za snimanje, rezultujući nešifrovanu, ilegalnu kopiju Rada. Ova kopija može biti puštena na nepropustljivom plejeru, ali ne i na propustljivom, jer bi on detektovao vodeni pečat i sprečio puštanje sadržaja.



Slika 13.- Odnos između šifrovanja i kontrole kopiranja na bazi vodenog pečata

2.1.15.7. Kontrola uređaja

1953. godine Tomberlin⁷⁹ opisuje sistem za redukovanje cene za distribuiranje muzičkih cevi do kancelarija, prodavnica i ostalih objekata. Standardno, muzika je distribuirana zemljanim linijama (iznajmljenim telefonskim linijama), koje su bile jako skupe. MusicScan, ovlašćeni vlasnik patenta, imao je nameru da redukuje cenu zamenjivanjem iznajmljenog distributivnog sistema sa sistemom za bežično emitovanje. Ovo je takođe bilo preskupo za radio prenos. Umesto toga, MusicScan-ovi objekti bi dobijali muziku od komercijalnih radio stanica koji emituju reklame isto koliko i muziku. Tomberlinova ideja bila je da se objedini signal vodenog pečata u radio prenos koji nagoveštava kada radio prenos treba da bude ignorisan. Naravno, ignorisan deo bi bio reklamni blok. Ovo je usavršeno sa dva kontrolna signala koji nagoveštavaju početak i kraj segmenata emitovanja koji bi trebali da budu blokirani.

1981. razmatrana je primena vodenog pečata za kontrolu od strane Reja Dolbija⁸⁰. Tada, broj FM radio stanica na kojima se emitovala muzika uz korišćenje tehnike za redukovanje šuma zvala se *Dolby FM*. Za potpuno iskorišćavanje Dolby FM-a, radio je zahtevao odgovarajući dekodirer. Slušaoci su morali da prelistavaju radio stanice kako bi odredili koja emituje Dolby FM i nakon toga bi mogli da ručno uključe ili isključe svoj radio dekodirer. Dolby je predložio da radio sam uključuje svoj dekodirer reagovanjem na nečujan ton emitovanja u okviru audio frekvencionog spektra. Takav ton predstavlja jednostavan vodeni pečat.

1989. Broton i Lomester⁸¹ patentirali su tehniku koja omogućava akcionoj igrački da menja televizijske programe. U ovoj tehnici, jednostavni vodeni pečat podešava horizontalne linije za skeniranje u okviru svakog frejma videa. Ovaj modularni signal je detektovan od strane uređaja koji je osetljiv na svetlo i postavljen blizu televizora. Broton i Lomster su takođe spominjali da se promenom intenziteta linija za skeniranje dobija povećanje detekcije radio frekvencionog signala i da on isto tako može da formira osnovu alternativnog detektora.

U najskorije vreme vodeni pečat za kontrolu uređaja primenjen je u Digimarc-ovom mobilnom sistemu gde se jedinstveni identifikator ugrađuje u odštampane i distribuirane slike kao što su slike u reklamnim magazinima, raznim pakovanjima, kartama itd. Nakon što je slika ponovo slikana kamerom mobilnog telefona, vodeni pečat je pročitao softverom u telefonu i ključ se koristi za direktno slanje web pretraživačem (*browserom*) na udružen web sajt.

2.1.15.8. Unapređivanje zaostalog

Ponekad razvijeni sistem želimo da nadogradimo kako bismo obezbedili bolju funkcionalnost. Ova poboljšanja mogu biti nekompatibilna sa postojećim sistemom. Npr. danas većina teži prelasku sa analogne na digitalnu televiziju, što je skup i dugotrajan proces. Tokom prelaska, mora se uvesti potpuno nova digitalna oprema i klijenti moraju kupiti digitalne televizijske prijemnike. U međuvremenu, zaostao analogni sistem mora nastaviti sa funkcionisanjem sve dok veći broj klijenata ne pređe na digitalnu tehnologiju.

Idealno bi bilo da unapredimo sistem tako da nov sistem bude kompatibilan sa zaostalim. DVP je jedan od načina koji bi to omogućio. Primer je Tektronix-ov digitalni koder vodenog pečata za sinhronizaciju audio i video signala. Problem nastaje kada su video i audio kanali televizijskog signala procesirani odvojeno. Digitalni signal unosi razna kašnjenja u audio i video kanalima što može dovesti do visoko dezorjentisanih fenomena poznatih kao sinhronizovana usta, u kojima se jasno vidi da se usta otvaraju pre ili posle govora.

⁷⁹ William M. Tomberlin i sar., 1953 [52]

⁸⁰ Ray Dolby, 1981 [42]

⁸¹ Broughton R. S. and Laumeister W. C., 1989 [9]

Nakon što se svi signalni procesi kompletiraju, stvarni audio signal je sravnjen sa ugrađenim audio signalom takvim redom da ako u bilo kom trenutku dođe do kašnjenja, da se ono izbriše pre emitovanja.

2.1.16. Osobine sistema DVP-a

Sistemi vodenog pečata mogu biti okarakterisani mnogim osobinama. U radu će biti razmatrano 10 najbitnijih osobina sistema koje zavise od oblasti primene vodenog pečata.

Osobine tipično vezane za proces ugrađivanja vodenog pečata su:

- delotvornost ugrađivanja
- verodostojnost
- korisnost tereta

Osobine koje su vezane za detekciju su:

- detekcija na slepo ili poznato
- lažno pozitivni odgovori
- otpornost

Sigurnost i korišćenje tajnog ključa su usko povezani sa korišćenjem ključeva kao celinom bilo koje sigurnosne osobine svojstvene šemi vodenog pečata.

Promene poruka moguće su bilo šifrovanjem, bilo promenom samog vodenog pečata ili prikazivanjem poruke sa višestrukim vodenim pečatom.

Ovo poglavlje će biti zaključeno troškovima ugrađivanja i detekcije vodenog pečata.

O svakoj osobini će biti rečeno toliko da ona bude jasnija korisnicima, dok će u poglavlju 2.4. detaljnije biti razmatrane dve osobine: otpornost i sigurnost.

2.1.16.1. Delotvornost ugrađivanja

Rad zaštićen vodenim pečatom definisan je ranije kao Rad koji, kada se ispituje detektorom, rezultuje pozitivno. Prema ovoj definiciji Rada zaštićenog vodenim pečatom, delotvornost sistema vodenog pečata predstavlja mogućnost detekcije odmah nakon ugrađivanja.

Iako je poželjno da je delotvornost 100%, ovaj cilj se često ostvaruje veoma visokim troškovima. U zavisnosti od aplikacije, možemo žrtvovati delotvornost za bolje performanse uzimajući u obzir druge karakteristike.

U nekim slučajevima delotvornost sistema vodenog pečata može biti određena analitički⁸². Takođe može biti procenjena empirički jednostavnim ugrađivanjem vodenog pečata u veliki set testova slika. Procenat izlaznih slika koje rezultuju pozitivnu detekciju će biti približan verovatnoći delotvornosti.

2.1.16.2. Verodostojnost

Generalno, verodostojnost sistema vodenog pečata se odnosi na primetnu sličnost između originala i verzije Rada koji je zaštićen vodenim pečatom. Drugačija definicija verodostojnosti je prikladnija ako se govori o Radu koji biva degradiran u toku prenosa pre nego što ga osoba vidi. Verodostojnost sistema vodenog pečata predstavlja perceptualnu sličnost između Rada koje jeste i koji nije zaštićen vodenim pečatom u trenutku u kom je on prezentovan potrošaču.

U nekim primenama, možemo prihvatiti srednje primetan vodeni pečat u zamenu za veću otpornost ili niže troškove.

⁸² Primena kod lažnih negativnih odgovora.

2.1.16.3. Korisni podaci (data payload)

Korisni podaci se odnose na broj bita vodenog pečata šifrovanih u okviru jedinice vremena ili u okviru Rada. Za fotografije korisni podaci se odnose na broj ugrađenih bitova u okviru slike, za audio snimke broj ugrađenih bitova u sekundi koji su preneseni, za video ili broj bita u frejmu ili broj bita u sekundi.

Vodeni pečat šifrovan sa N bitova se naziva *N -bitni vodeni pečat*. Takav sistem se može koristiti za ubacivanje bilo koje od 2^N različite poruke.

Različite primene DVP-a zahtevaju različite korisne podatke:

- Kontrola kopiranja zahteva samo 4-8 bita dobijenih informacija u određenom periodu.
- Monitoring emitovanja zahteva najmanje 24 bita informacija za identifikaciju svih reklama itd.

Mnoge aplikacije zahtevaju detektor kako bi obezbedile dve funkcije. On mora odrediti da li postoji vodeni pečat i ako postoji, identifikuje koja od 2^N poruke je šifrovana. Takav detektor bi prema tome morao da ima 2^N+1 moguće izlazne vrednosti: 2^N poruke plus „nije prisutan vodeni pečat“.

U literaturi mnogi predloženi sistemi su sa samo jednim mogućim vodenim pečatom i detektorom koji odlučuje da li jeste ili nije prisutan vodeni pečat, i koji se nazivaju *jednobitni vodeni pečati* zato što postoje 2^1 moguća izlaza: vodeni pečat je prisutan i vodeni pečat je odsutan. Ovo je protivrečno prethodno opisanom sistemu. Logičnije je da se ovaj sistem naziva *nula-bitni vodeni pečat* zato što on ima $2^0+1=2$ moguće izlazne vrednosti.

2.1.16.4. Detekcija na slepo ili poznato

U pojedinim primenama, originalni, Rad koji nije obeležen vodenim pečatom, je dostupan tokom detekcije. U drugim, detekcija mora biti obavljena bez pristupa originalnom Radu.

Ona koja zahteva pristup originalu naziva se *detekcija na poznato*. Ovaj termin takođe se odnosi na detektore koji zahtevaju samo neku informaciju izvedenu od originalnog Rada, pre nego ceo Rad. Detektori koji ne zahtevaju nijednu informaciju koja se odnosi na original nazivaju se *detektori na slepo*.

Sistemi koji koriste detekciju na poznato u literaturi se često nazivaju *privatni sistemi vodenih pečata*, dok se detektori na slepo nazivaju *javni*.

2.1.16.5. Lažno pozitivni odgovori (ocene)

Lažno pozitivni odgovor predstavlja detekciju vodenog pečata u Radu koji ga ne sadrži. Kada se govori o lažno pozitivnim odgovorima, u obzir se uzima koliki ih je broj i kolika je verovatnoća da će se oni pojaviti nakon aktiviranja detektora.

Postoje dva različita načina za definisanje verovatnoće.

U prvoj definiciji, lažno pozitivna verovatnoća predstavlja verovatnoću da će u kombinaciji: fiksni Rad i slučajno odabran vodeni pečat, detektor prijaviti da se vodeni pečat nalazi u tom određenom Radu.

U drugoj definiciji, lažno pozitivna verovatnoća je verovatnoća da će u kombinaciji: slučajno odabrani Rad i fiksni pečat, detektor prijaviti taj određeni pečat u Radu.

Najčešće se u praksi koristi druga definicija. U slučaju praćenja transakcija prva definicija je veoma važna, jer u njoj detekcija slučajnog pečata u određenom Radu može voditi do lažne optužbe za krađu.

Ako Rad nezaštićen vodenim pečatom konstantno generiše lažne pozitivne odgovore, može doći do velikih problema. Iz ovog razloga lažne pozitivne odgovore treba svesti na minimum.

2.1.16.6. Otpornost

Otpornost se odnosi na mogućnost detektovanja vodenog pečata nakon opštih signalnih procesnih operacija. Primer primene signalnih procesnih operacija na slikama uključuje prostorno filtriranje, kompresiju, štampanje i skeniranje sa gubicima i geometrijske deformacije.

Ne zahtevaju sve primene vodenog pečata otpornost na sve moguće signalne procesne operacije, češće je potrebno samo da ih vodeni pečat preživi u periodu između ugrađivanja i detekcije.

U nekim slučajevima otpornost može biti potpuno nebitna ili čak nepoželjna. Jedna bitna grana istraživanja vodenih pečata fokusira se na slabosti vodenih pečata. Slab vodeni pečat je onaj koji je dizajniran tako da nije otporan. Primer takvog pečata je vodeni pečat koji služi u svrhu autentifikacije. Bilo koji signalni proces primenjen na sliku trebalo bi da prouzrokuje gubitak vodenog pečata.

U drugim slučajevima, postoje primene u kojima vodeni pečat mora da bude otporan na svaku pojmljivu deformaciju kako ne bi bila uništena zaštita Rada. Ovaj slučaj je primenljiv kada je signalni proces između ugrađivanja i detekcije nepredvidiv, ili kada vodeni pečat mora biti siguran protiv neprijateljskog napada.

2.1.16.7. Sigurnost

Sigurnost vodenog pečata predstavlja mogućnost odbrane od neprijateljskog napada. Ova vrsta napada predstavlja bilo koji proces s namerom da se promeni svrha vodenog pečata. Tipovi napada mogu se svrstati u tri kategorije:

- Neovlašćeno uklanjanje
- Neovlašćeno ugrađivanje
- Neovlašćena detekcija

Neovlašćeno uklanjanje i ugrađivanje vodenog pečata spadaju u grupu *aktivnih napada* zato što je napad vršen na zaštićen Rad, dok neovlašćena detekcija spada u grupu *pasivnih napada* iz razloga što ova vrsta napada ne utiče na Rad.

Neovlašćenim uklanjanjem pečata onemogućava se detekcija DVP-a u Radu. Obično se razlikuju dve forme neovlašćenog uklanjanja pečata: napad eliminacijom i napad maskiranjem. *Napad eliminacijom vodenog pečata* podrazumeva da se ne može uopšte razmatrati da li napadnut Rad sadrži vodeni pečat ili ne, odn. ukoliko se ukloni pečat, ni najveštijim detektorom se ne može detektovati da je nekada postojao. *Napad maskiranjem vodenog pečata* znači da se može razmatrati da li napadnut Rad sadrži pečat ili ne, ali DVP može biti detektovan isključivo najveštijim detektorom.

Neovlašćeno ugrađivanje pečata takođe predstavlja vrstu falsifikovanja i podrazumeva nelegitimni postupak ugrađivanja vodenog pečata u Rad koji ne bi trebao da ga sadrži.

Neovlašćena detekcija, ili pasivni napad, može biti prekinuta u sva tri nivoa u kojima se ona odvija. Prvi nivo neovlašćene detekcije započinje kada suparnik detektuje i dešifruje ugrađenu poruku. Ovaj nivo predstavlja najotvoreniju i najobimniju formu neovlašćenog čitanja. Sledeća, manje opasna forma napada odvija se kada suparnik može da detektuje vodeni pečat i da razlikuje poruke, ali ne zna šta one znače. S obzirom na to da se vodeni pečat odnosi na Rad u koji je ugrađen, suparnik može otkriti značenje pečata upoređujući ga sa zaštićenim Radom. Poslednja forma napada predstavlja sposobnost suparnika da odredi prisustvo vodenog pečata, ali ne može da dešifruje poruku niti da napravi razliku između ugrađenih poruka. Treća forma se pre odnosi na steganografiju nego na DVP.

2.1.16.8. Šifre i ključevi digitalnog vodenog pečata

Mnogi sistemi vodenog pečata su dizajnirani tako da koriste ključeve na analogni način. U takvom sistemu, metod kojim se poruka ugrađuje u vodeni pečat zavisi od ključa, a da bi se ta poruka detektovala mora biti korišćen ključ za upoređivanje.

Pre uvođenja ključeva, sigurnost većine kriptografskih algoritama odnosila se na držanje tih algoritama u tajnosti. To je vodilo do dva problema:

- 1) Ako je sigurnost algoritma kompromitovana, morao se razvijati potpuno nov algoritam
- 2) Zbog potrebe za sigurnošću nije bilo moguće obelodaniti algoritam radi daljih istraživanja i unapređivanja.

Ove probleme je u većini rešilo uvođenje ključeva.

U moderne kriptografske algoritme, bezbednost je izvedena osiguravanjem ključa, a ne celog algoritma. S toga, šifrovanje i dešifrovanje algoritama može biti javno objavljeno i razvijano korišćenjem jednog ključa, dok se u stvarnoj upotrebi može koristiti drugi ključ. Ako je ključ kompromitovan nepotrebno je menjati ceo algoritam, samo treba odabrati nov tajni ključ. Iz ovoga sledi da dobro dizajnirana šifra treba slediti sledeće standarde:

- Znanje o šifrovanju i dešifrovanju algoritma ne treba da kompromituje sigurnost sistema.
- Sigurnost treba da bude zasnovana na ključevima.
- Ključeve treba izabrati iz velikog broja ključeva (obimnost ključeva, *engl.- keyspace*) tako da bi traženje pravog bilo nepraktično među velikim brojem drugih ključeva.

Nepoželjno je iste standarde primeniti i na algoritme vodenog pečata. Nažalost, *keyspace* između kriptografije i ugrađivanja vodenog pečata je različita. U kriptografiji svi n biti šifre moraju biti određeni i slični ključevi⁸³ nisu opremljeni korisnim informacijama. U ugrađivanju vodenih pečata suparnik često treba samo da nađe ključ koji je blizak i značajno promeni veličinu obima ključa. Pored toga sigurnosni zahtevi za ugrađivanje vodenog pečata su takođe drugačiji u odnosu na šifre. S toga, kriptografski metodi se ne mogu jednostavno nadograditi kako bi se primenili na vodene pečate. Kriptografija se brine jedino o sprečavanju neovlašćeng čitanja i pisanja poruka, što znači da se ona može koristiti u ugrađivanju vodenog pečata kako bi se sprečila određena forma pasivnog napada i prevare, ali ne daje rezultate u sprečavanju uklanjanja vodenog pečata. Ovaj problem ja sličan problemu ometanja signala u vojnim komunikacijama. Kako bi sprečila ometanja, vojska je razvila komunikaciju proširenog spektra koja je takođe zasnovana na tajnosti, slično kao ključ u kriptografiji.

Algoritmi vodenog pečata mogu biti dizajnirani tako da koriste tajni ključ na način sličan načinu na koji funkcioniše prošireni spektar.

Idealno bi bilo da je detekcija vodenog pečata u Radu nemoguća bez poznavanja ključa, čak i onda kada je poznat algoritam. Ograničavanje znanja o ključu samo na poverljivu grupu otežalo bi, ako ne i onemogućilo, suparniku da ukloni vodeni pečat bez prouzrokovanja značajne deformacije u verodostojnosti zaštićenog Rada.

Zbog toga što korišćenje ključeva u toku ugrađivanja i detekcije obezbeđuje različite tipove sigurnosnih formi u odnosu na one koje se koriste u kriptografiji, poželjno je koristiti obe forme ključeva u sistemu vodenih pečata. Prvo se šifrue poruka jednim ključem i zatim se ona ugrađuje korišćenjem drugog ključa. Da bi se ta dva tipa ključa držala odvojena koriste se termini *šifrovani ključ* (ili *kripto ključ*) i *vodenopečatni ključ* (*engl.-watermark key*).

2.1.16.9. Promene i višestrukost vodenog pečata

Kada se poruka ugradi u zaštićen Rad, pošiljalac može biti zabrinut zbog promene poruke. Iako je u pojedinim slučajevima promena poruke nepoželjna u drugim je ona neophodna.

⁸³ Ključevi koji se razlikuju u nekoliko bitova

U kontroli kopiranja, emiteri sadržaja mogu naznačiti na sadržaju *kopirati jednom* i zatim nakon kopiranja kopiju treba obeležiti sa *ne kopirati više*⁸⁴. Promena snimljenog videa može biti usavršena na više načina.

Najočigledniji način jeste jednostavna promena naznake *kopirati jednom* na ugrađenom vodenom pečatu u naznaku *ne kopirati više*. Ako je vodeni pečat dizajniran tako da dozvoli jednostavnu promenu, postoji rizik da će ilegalna promena postati svakidašnja, npr. ako se upotrebi uređaj ili program koji će promeniti video sa *kopiraj jednom* u *kopiraj slobodno*.

Alternativa je menjanje postojećeg vodenog pečata ubacivanjem drugog. Prisustvo oba pečata se može koristiti za naznačavanje oznake *ne kopirati više*. Inicijalna oznaka *ne kopirati više* može biti naznačena sa dva vodena pečata: primarnim i sekundarnim. Sekundarni može biti relativno slab u odnosu na primarni i njegovim uklanjanjem oznaka bi bila *ne kopirati više*. Ova dva metoda se u prvom trenutku čine isti, ali oni imaju veoma različita lažno pozitivna ponašanja. Njihova implementacija takođe povećava tehničke izazove, kao što je potreba za ugrađivanjem vodenog pečata u kompresovani medij bez promene protoka bita.⁸⁵

Još jedna potreba za višestrukošću vodenih pečata javlja se u oblasti transakcije vodenog pečata u Radu. Distribucija sadržaja uključuje brojne posrednike pre nego što on stigne u posed krajnjem korisniku. Snimljena oznaka u Radu može prvo iskoristiti vodeni pečat za identifikaciju same sebe kao vlasnika autorskih prava. Rad nakon toga može biti poslat brojnim muzičkim sajtovima. Svaka kopija Rada može imati jedinstveni vodeni pečat ugrađen u sebe kako bi se identifikovao svaki distributer. Konačno, svaki web sajt može ugrađivati jedinstveni vodeni pečat u svaki Rad koji prodaje za jedinstvenu identifikaciju svakog kupca.

2.1.16.10. Trošak

Ekonomičnost razvijanja ugrađivača vodenih pečata i detektora može biti veoma komplikovana i zavisi od poslovnog modela kom je namenjen.

Sa tehnološke tačke gledanja, dva osnovna zadatka su brzina i broj ugrađivanja i detekcija koje se moraju izvršiti. Drugo sporno pitanje je da li su detektori i ugrađivači implementirani kao hardver za posebnu upotrebu ili kao softverska aplikacija.

U monitoringu emitovanja ugrađivač i detektor moraju raditi u realnom vremenu iz razloga što ugrađivači ne smeju usporavati izvođenje rasporeda, a detektori moraju održavati emitovanje u realnom vremenu. S druge strane, detektor za dokazivanje vlasništva biće vredan čak i u slučaju da mu treba nekoliko dana da pronađe vodeni pečat. Takav detektor će biti korišćen samo u toku rasprave o vlasništvu prava. Zaključak o tome da li je vodeni pečat prisutan ili ne, trebao bi da bude izuzetno važan da bi korisnik bio voljan da ga sačeka.

Različite primene zahtevaju različit broj ugrađivača i detektora. Monitoring emitovanja zahteva ponekad i nekoliko stotina detektora na različitim geografskim mestima. Kontrola kopiranja može trebati mali broj ugrađivača, ali milione detektora ugrađenih u video i audio uređajima. S druge strane, u aplikacijama za praćenje transakcija implementiranih od strane DiVX, gde je u svakom plejeru ugrađen drugačiji vodeni pečat, potrebni bi bili milioni ugrađivača i samo mali broj detektora. Generalno, najveći broj uređaja treba da bude za datu primenu što jeftiniji.

2.1.17. Sigurnost i otpornost DVP-a

Mnoge primene vodenog pečata zahtevaju da vodeni pečat bude detektovan u Radu koji je, možda, promenjen nakon ugrađivanja. Vodeni pečati dizajnirani da prežive zakonsku i svakodnevnu upotrebu sadržaja poznati su kao *otporni pečati*.

⁸⁴ Engl.- *copy-once* i *copy-no-more*

⁸⁵ Hartung F. i Girod B., 1998. [28]

U ovom poglavlju biće predočene razlike između otpornosti i sigurnosti vodenog pečata koje se u literaturi inače ne prave često, već se umesto sigurnosti koristi reč otpornost. Dok su otporni vodeni pečati dizajnirani da prežive normalne procese, sigurni vodeni pečati su dizajnirani da se odupru bilo kom pokušaju suparnika da promeni njegovu namensku funkciju. S obzirom na to da se u većini slučajeva funkcionalna primena vodenog pečata ne može izvršiti ako je njegov prikaz nedektibilan, otpornost je neophodna osobina ako vodeni pečat treba da bude siguran. Drugim rečima, ako vodeni pečat može da bude uklonjen primenom normalnog procesa on se ne može smatrati sigurnim. Otpornost nije dovoljna za sigurnost, zato što sigurni vodeni pečat takođe mora biti sposoban da preživi neispitane procese koji su posebno dizajnirani da ga uklone. Dizajner sigurnog vodenog pečata mora da uzme u obzir radijus svih mogućih napada i na taj način ograniči oblast mogućeg delovanja.

2.1.17.1. Otpornost DVP-a

Postoji nekoliko strategija da bi se DVP učinio detektibilnim nakon što se zaštićeni Rad deformiše. Neke od njih teže da naprave vodeni pečat otpornim na sve moguće degradacije i teže ka tome da sačuvaju zaštićeni Rad. Druge strategije se odnose na manipulaciju određenih tipova deformacija. U praksi sistemi vodenih pečata će koristiti višestruke strategije za upravljanje različitim tipovima deformisanja.

Prvih pet izloženih strategija obezbeđuju vodenom pečatu da ostane nepromenjen, ili slabo promenjen, normalnim procesima. Strategije se odnose na traženje transformacionog domena u kom su pojedini delovi ostali neoštećeni procesom.

Poslednje dve strategije opisuju metode bazirane na preinačenju efekata deformacija. U njima, vodenom pečatu je dozvoljeno da bude promenjen usled deformacije, ali će se promeniti suprotstaviti ili detektor ili ugrađivač.

Dodatno ugrađivanje

Često kada je Rad deformisan nije se na sve koeficijente u njegovom prikazu delovalo podjednako. Ako za primer uzmemo sliku sečenu duž desne ivice, u pregledu piksela slike, samo krajnji desni pikseli su pogođeni, dok su ostali netaknuti. Ako je Rad uvijen propusno opsežnim filterom i prikazan u prostornom ili privremenom domenu, filtriranje će najverovatnije promeniti sve uzorke. U Furijerovom domenu filter će imati efekta samo na frekvencije van propusnog opsega.

Strategija za preživljavanje raznovrsnih deformisanja je ugrađivanje dodatnih vodenih pečata preko nekoliko koeficijenata. Ako neki od koeficijenata budu oštećeni, vodeni pečat u drugim koeficijentima bi trebao da ostane detektibilan. Primer ovog pristupa je prostorno popločavanje korišćeno u E_BLK_BLIND/D_BLK_CC sistemu⁸⁶. Ovo popločavanje obezbeđuje otpornost na deformacionu izmenu prostora kao što je isecanje.

Vodeni pečat koji je ugrađen dodatnim popločavanjem može biti detektovan na brojne načine. Jedan od metoda je kombinovanje podataka iz svake ploče u Radu i dešifrovanje rezultata. Ovo je metod koji je korišćen u D_BLK_CC detektoru, koji dodaje ploče zajedno i testira ih za vodeni pečat u njihovoj oblasti. Drugi metod je testiranje vodenog pečata u svakoj ploči posebno, obaveštavajući da je pečat prisutan ukoliko je detektovan u nekoliko delova lokacije. Ovaj pristup je prisutan u nekoliko predloženih sistema kao što je sistem Basa i saradnika.⁸⁷ Još jedan od metoda je testiranje vodenog pečata u svakoj ploči i zatim kombinovanje rezultujuće detektovane vrednosti.

⁸⁶ Engl.- *Block-Based, Blind Embedding, and Correlation Coefficient Detection*. E označava ime ugrađivača (engl. *Embedder*), dok D označava detektor. Ovaj sistem ilustruje podelu ugrađivanja vodenog pečata u prostor posrednika i prostor signalizacije korišćenjem funkcije izvlačenja. Takođe uvodi korišćenje korelacionog koeficijenta kao meru detekcije.

⁸⁷ Bas P. i sar. 2000. [5]

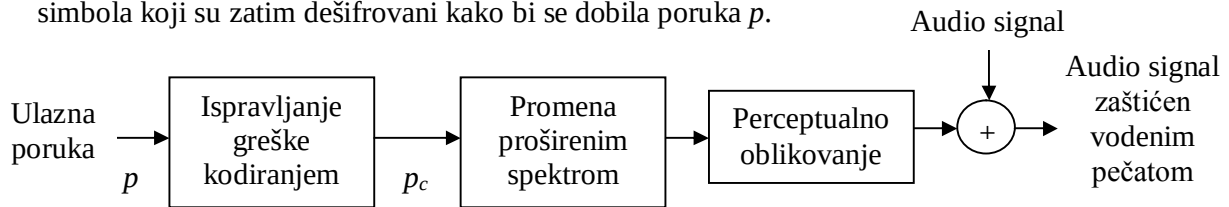
Iako najočigledniji primer dodatnog ugrađivanja uključuje popločavanje, postoje i drugi pristupi. Može se reći da je vodeni pečat ugrađen dodatno, u nekom domenu, ukoliko može biti detektovan u nekoliko podskupova koeficijenata.

Ideja dodatnog ugrađivanja može napraviti korak dalje ugrađivanjem poruke u Rad više puta šifrovanjem ključa, gde je svako šifrovanje dizajnirano da preživi različite deformacije. Zbog toga što Rad teško prolazi sve deformacije na koje je DVP osetljiv, ovo bi osiguralo da bar jedan pečat preživi.

Kodiranje proširenim spektrom

Kada se primenjuje u frekvencijskom domenu, ideja dodatnog ugrađivanja vodi do dobro poznate paradigme kodiranja proširenog spektra. U komunikacionom sistemu proširenog spektra, poruka je šifrovana nizom simbola. Oni su preneseni privremenim redosledom i svaki je predstavljen signalom i kao takvi poznati su pod nazivom *odlomci*. Odlomci su pseudo-slučajni delovi od 1s i 0s. U frekvencionom domenu oni su široko rasprostranjeni u okviru frekvencije. S toga, ako je signal ometan nekim procesom koji deformiše samo deo frekvencije, kao što je propusno opsežni filter ili dodavanje pojasno ograničene buke, ovi odlomci će i dalje moći da se identifikuju.

Na slici 14. prikazan je jednostavan prošireni spektar u audio sistemu zaštićenim vodenim pečatom. U ugrađivaču započinje se sa porukom p koja je greškom šifrovana i obeležena p_c . Neka p_c bude prikazana simbolom izvučenim iz 128 ASCII karaktera. Svaki simbol poruke se zatim pretvara u 512.-bitni pseudoslučajni deo ili odlomak. Rezultujući odlomak je perceptualno oblikovan i nakon toga se dodaje zaštićeni audio Rad. Kod prijemnika (*receiver*) se primenjuje obrnut proces. Prvo, oblikovanje je približno preinačeno. Svaki odlomak je identifikovan upoređivanjem sa 128 odlomaka u alfabetu (ASCII karakteri) i zatim je izabran onaj sa najboljim poklapanjem. Ovo proizvodi deo pogrešno šifrovanih simbola koji su zatim dešifrovani kako bi se dobila poruka p .



Slika 14.- Jednostavni primer audio vatermarkinga metodom proširenog spektra

Komunikacija proširenim spektrom ima dve bitne karakteristike vezane za *watermarking*.⁸⁸ Prva karakteristika je da je signalna energija ugrađena u bilo koju frekvenciju veoma mala. Ovi veoma niski srazmerni signalni šumovi prisutni u bilo kojoj pojedinačnoj frekvenciji detektovanog izlaznog signala još uvek mogu imati visoki srazmerni signalni šum bilo da on širi ili koncentriše energiju prisutnu u velikom broju frekvencija. Drugo, činjenica je da vodeni pečat raspršen preko velikog broja frekvencija takođe obezbeđuje otpornost na mnoge signalne deformacije.

Ugrađivanje u perceptualno značajne koeficijente

U praksi nije uvek preporučljivo ugrađivati vodeni pečat u sve koeficijente Rada. Neki koeficijenti su osetljivi na deformacije, tako da će oni malo verovatno biti od koristi.

Koks i saradnici⁸⁹ pružaju odgovor na to kako odlučiti koji koeficijent je pouzdan a koji ne. Koeficijent koji je perceptualno značajan je verovatno pouzdan, s obzirom na to da je onaj koji je perceptualno beznačajan verovatno i nepouzdan.

⁸⁸ Engl. *Watermarking*- zaštita Rada vodenim pečatom

⁸⁹ Cox J. i sar., 1997. [13]

Idealno perceptualno značajan koeficijent je onaj koji se nikada ne menja osim ako je Rad primetno deformisan. Generalno, sve normalne kompresije, prenosi i ostale izložene tehnologije, primenjene na Rad, dizajnirane su da zaštite osobine primetno važnih bitova.

Vodeni pečat ne mora obavezno da preživi proces koji oštećuje primetno značajne bitove. Prema definiciji, oštećenje prvih koeficijenata degradira perceptualni kvalitet Rada. Ako je rezultujući Rad oštećen tako da je njegova vrednost izgubljena, informacije ugrađene u njega možda neće biti korisne.

Glavni problem sa ugrađivanjem u perceptualno značajne koeficijente je taj što je on direktno suprotstavljen cilju kreiranja nevidljivog vodenog pečata. Da bismo napravili nevidljivi vodeni pečat, možda hoćemo da većinu njegove energije stavimo u perceptualno nebitne koeficijente. S toga, cilj verodostojnosti je često osnovano suprotstavljen cilju otpornosti.

Rešenje ovog problema takođe predlaže Koks i on predlaže da se vodeni pečat raširi preko velikog broja perceptualno značajnih koeficijenata u frekvencijskom domenu. Zbog toga što kodiranje raširenog spektra dozvoljava veoma malu energiju za korišćenje u svakoj frekvenciji, promena svakog koeficijenta može biti dovoljno mala da bude nevidljiva.

Alternativno rešenje je ugrađivanje u koeficijente koji imaju srednji nivo perceptualnog značaja. Njihova perceptualna značajnost nije ni dovoljno visoka da ne možemo da ugradimo vodeni pečat u njih ni toliko niska da je malo verovatno da će preživeti normalne procese.

Ugrađivanje u koeficijente poznate otpornosti

Kada ugrađujemo u perceptualno značajne koeficijente, pokušavamo da napravimo vodeni pečat koji će preživeti sve poznate procese koji održavaju vrednost Rada. U mnogim primenama nas ne interesuju svi mogući procesi, već poseban set procesa koji se mogu javiti između ugrađivanja i detekcije. U takvim slučajevima, možemo se susresti sa ovim procesima direktno.

Prvo, vodeni pečat bi trebao da bude opisan u domenu koji će najverovatnije biti otporan na proces koji nas interesuje. Kada izaberemo prikaz u kom ćemo opisati vodeni pečat, možemo da identifikujemo koeficijente koji će preživeti očekivanu deformaciju. Za neke deformacije, ovo se može uraditi analitičkim, dok se za druge to radi empiričkim testom. Testovi su jasni i uključuju poređenje sadržaja direktno nakon ugrađivanja i direktno pre detekcije. Poređenjem odgovarajućih koeficijenata, moguće je odrediti kako kanal između ugrađivača i detektora utiče na svaki koeficijent. Takav eksperiment treba da bude izvršen na raznovrsnom sadržaju i često su potrebni brojni pokušaji da bi se izgradio zadovoljavajući model sa dovoljnom statističkom sigurnošću.

Preporučljivo je da se vodeni pečat ugrađuje u različite setove koeficijenata za svaki Rad. Jedna od tehnika za izbor koeficijenata za pojedinačne radove jeste merenje relativne otpornosti za svaki koeficijent pre ugrađivanja u vodeni pečat. Ovo se može obaviti primenom nekoliko simultanih deformisanja na Rad i merenjem efekata koji oni proizvode na prikaz tog Rada u izabranom domenu. Tada se vodeni pečat ugrađuje u koeficijente koji su pronađeni kao najotporniji, koji mogu biti različiti set koeficijenata za svaki Rad. Spisak korišćenih koeficijenata prosleđuje se detektoru zajedno sa, potencijalno deformisanim, Radom. Iz ovoga sledi da takav sistem zahteva informisan detektor.

Preinačenje deformacije u detektoru

Razlika između ovog i prethodnog pristupa jeste ta što se u ovom pristupu teži ka tome da se, tokom procesa detekcije, promeni bilo koji proces koji je bio primenjen od trenutka kada je vodeni pečat ugrađen.

Mnogi procesi mogu biti tačno ili približno preinačeni. Ako detektor može da odredi da je neki od procesa primenjen na Rad u periodu između ugradnje i detekcije, on može da preokrene proces primenjen na Rad da bi dobio približno neprocesuiranu verziju.

U zavisnosti od algoritma vodenog pečata, moguće bi bilo da detektor dodeli deformaciju datom vodenom pečatu, pre nego da primeni inverznu deformaciju na Radu.

Težak korak u promeni deformacije u detektoru jeste određivanje koju deformaciju preinačiti. U najgorem slučaju, detektor može primeniti iscrpno pretraživanje, testirajući vodeni pečat nakon preinačenja na svaki od velikog broja procesa. Npr. detektor vodenog pečata u slici može pokušavati da detektuje sliku nakon rotiranja između 0 i 359 stepeni povećavajući stepen za 1.

Za neke tipove procesa, moguće je redukovati pretragu i mogućnost lažnih pozitiva. Ako jedan algoritam može identifikovati jedan ili mali broj deformacija koje su primenjene, detektor treba da testira vodene pečate nakon preinačenja samo tih deformacija. Takav algoritam mora da bude posebno definisan za svaku klasu deformacija.

Problem identifikovanja deformacija je generalno lakši u informisanim detektorima nego u slepim, zato što informisani detektor ima mogućnost upoređivanja primljenog Rada sa originalom. Kada se primeni ispravno preinačenje na Rad, on bi trebao da se poklapa sa originalom, sa izuzetkom njegovog vodenog pečata. Za mnoge tipove procesa, brz algoritam nastoji da pronađe parametre koji vode do najboljih poklapanja između dva Rada.

Unapred preinačena deformacija u ugrađivaču

U nekim okolnostima može postojati mali set dobro definisanih deformacija koje vodeni pečat mora da preživi. Da bi se izborili sa tim deformacijama, možemo ugraditi posebne vodene pečate u originalnom formatu. Ovi vodeni pečati su preobličeni tako da će oni nakon konverzije odgovarajućem načinu prikazivanja⁹⁰ biti detektovani. Osnovna ideja je ugrađivanje više od jednog vodenog pečata u sadržaj. Prvi vodeni pečat nije preoblikovan i biće detektovan od strane detektora vodenog pečata kada nije primenjena nijedna forma konverzije. Drugi vodeni pečat je preoblikovan za format *letterbox*, dok je treći preoblikovan za *panscan*⁹¹. U zavisnosti od načina prikazivanja, jedan od tri vodena pečata će biti detektovan.

Višestruki vodeni pečati mogu biti postavljeni u sadržaj ugrađivanjem jednog preko drugog ili vremenskim multipleksiranjem. U prethodnom slučaju, jedan frejm video sekvence može sadržati prvi vodeni pečat, drugi frejm sledeći itd. Multipleksiranje može biti grubo sa prvim ugrađenim vodenim pečatom u prvih 10 sekundi videa, sledećim u sledećih 10 itd. Nedostatak ovakvog pristupa je taj što za dati format, odgovarajući vodeni pečat je detektibilan $1/N$ u vremenu, gde N predstavlja broj predeformisanih vodenih pečata.

Naizmenična preklapanja višestrukih vodenih pečata rešava ovaj problem. Svaki vodeni pečat mora da bude ugrađen sa $1/N$ snagom, ako je ograničenje održivost verodostojnosti.

Najjednostavnija procedura za ugrađivanje predeformisanog vodenog pečata sastoji se iz tri koraka:

- I. Primeniti očekivanu deformaciju na Rad koji će biti zaštićen vodenim pečatom⁹².
- II. Ugraditi vodeni pečat u deformisan Rad. U ovom trenutku, ugrađivač vodenog pečata je nesvestan deformacije. On jednostavno ugrađuje vodeni pečat na isti način kao i u nedeformisan sadržaj.
- III. Primeniti obrnutu deformaciju na deformisan zaštićen Rad.

⁹⁰ Vodeni pečat se odnosi na vodene pečate za DVD format. Način prikazivanja se odnosi na proporcionalnost prikazivanja (4:3, 16:9)

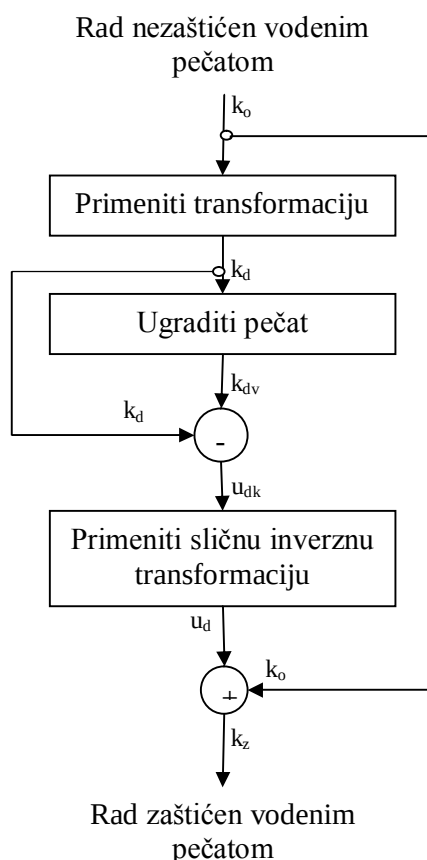
⁹¹ *Letterbox* i *panscan* su formati prikazivanja slike u 4:3 standardu, s tom razlikom da prikaz u *letterbox* formatu dodaje gornju i donju crnu liniju pri prikazivanju, dok *panscan* seče prikaz slike s leve i desne strane.

⁹² Očekivana deformacija je konverzija u *letterbox* ili *panscan* format.

Ova procedura je primenjiva na bilo koji algoritam za ugrađivanje vodenog pečata.

Nažalost, prethodno opisana procedura može uvesti neprihvatljivi gubitak verodostojnosti kada se primenjuje sa deformacijom koja nije perfektно invertibilna. I u *letterbox* i u *panscan* konverziji, neke informacije se izgube i stoga inverzno deformisanje u poslednjem koraku mora da uvede neku deformaciju u kvalitetu slike. Iz ovog razloga, bolje je primeniti malo komplikovaniju proceduru, koja radi na određenim tipovima deformacije.

- I. Napraviti kopiju Rada koji će biti zaštićen vodenim pečatom, primeniti očekivanu deformaciju na njega i time obezbediti deformisanu kopiju Rada, $\mathbf{k}_d$.
 - II. Kreirati zaštićenu verziju deformisane kopije vodenim pečatom, $\mathbf{k}_{dv}$.
 - III. Pronaći uzorak koji je dodat deformisanoj kopiji, $\mathbf{k}_d$, u drugom koraku: $\mathbf{u}_{dk} = \mathbf{k}_{dv} - \mathbf{k}_d$.
 - IV. Izvršiti inverznu deformaciju na dodati uzorak, $\mathbf{u}_{dk}$, da bi se dobio odgovarajući uzorak, $\mathbf{u}_d$, za originalnu sliku. Npr. ako je transformacija bila izjednačavanje sa *letterbox* formatom, $\mathbf{u}_d$ bi se dobila vertikalnim širenjem $\mathbf{u}_{dk}$.
 - V. Na kraju, dodati $\mathbf{u}_d$ originalnom zaštićenom Radu, $\mathbf{k}_o$, da bi se dobio zaštićeni Rad, $\mathbf{k}_z$.
- Ovi koraci su predstavljeni na slici broj 15.



Slika 15.- Proces ugrađivanja za umetanje predeformisanog vodenog pečata

Kada se deformacija kasnije primeneni na Rad zaštićen vodenim pečatom, k_z , rezultat će biti približno jednak deformisanom, vodenim pečatom zaštićenom, Radu, k_{dv} , kreiranom u drugom koraku. Vodeni pečat će biti detektovan od strane iste procedure dizajnirane da detektuje normalan vodeni pečat.

U retkim okolnostima u kojima možemo da identifikujemo mali broj specifičnih deformacija koje vodeni pečat mora da preživi, predeformisanje vodenih pečata u ugrađivaču može imati nekoliko koristi:

- Može biti primenjivan na bilo koji sistem za zaštitu vodenim pečatom za gotovo bilo koji deformaciju, sve dok je deformacija invertibilna
- Nema dodatnih troškova za detektor, što je važno jer svi troškovi moraju biti minimalizovani.
- Može se primeniti nakon što je detektor razvijen, što je važno ako se uvedu nove deformacije u normalnom upravljanju sadržajima.

2.1.17.2. Sigurnost DVP-a

U poglavlju o sigurnosti DVP-a biće opisani tipovi i nivoi sigurnosti koji su potrebni u određenim primenama vodenog pečata. U ovom poglavlju biće predstavljeni sigurnosni zahtevi koji treba da budu ispunjeni pri korišćenju vodenog pečata, dok će u drugom delu poglavlja biti ukratko izloženi načini za sprečavanje određenih kategorija napada i nabrojani poznati napadi na sigurnost sistema vodenih pečata.

Ograničavanje operacija nad vodenim pečatom

U svakoj primeni vodenih pečata, pojedine osobe imaju mogućnost da ih ugrađuju, detektuju i/ili uklanjaju, dok drugi moraju imati zabranu za sprovođenje neke od nabrojanih ili čak svih akcija. Sigurni vodeni pečati zahtevaju ove zabrane. Uzmimo na primer sledeća tri scenarija u kojima učestvuju dve osobe: Alis i Bob.⁹³

- I. Alis je oglašavač koja je ugradila vodeni pečat u svaku svoju radio reklamu pre distribucije na 600 radio stanica. Ona zatim vrši monitoring tih stanica sa detektorom, obeležavajući svoje reklame, zatim ih kasnije preklapa sa svih 600 dostavnica i identifikuje pojedine lažne troškove. Bob upravlja jednom od tih 600 radio stanica i hteo bi da emituje jednu svoju reklamu umesto Alisine. Ipak, on hoće da naplati Alis taj reklamni prostor i zbog toga tajno ubacuje Alisin vodeni pečat u svoju reklamu i pušta je. Alis detektuje taj vodeni pečat i veruje da je njena reklama korektno emitovana.
- II. Alis poseduje *watermarking* servis koji, za minimalnu naknadu, dodaje vlasnikov identifikacioni vodeni pečat u slike koje će biti puštene na Internet. Alis je takođe opremljena skupim servisom izveštavanja kako bi informisala svoje klijente o svim njihovim pronađenim slikama koje su zaštićene vodenim pečatom na Internetu. Njeni klijenti koriste ove informacije za identifikovanje bilo koje neovlašćene distribucije njihovih slika. Bob gradi sopstvenog crva koji detektuje vodene pečate ugrađene od strane Alis i nudi ih jeftinije.
- III. Alis poseduje filmski studio i ugrađuje vodene pečate za kontrolu kopiranja u svoje filmove pre nego što ih distribuira. Ona veruje da su svi njeni digitalni snimci zaštićeni i da je kopiranje nemoguće zato što će detektor odbiti da kopira njene filmove. Bob je video pirater koji poseduje uređaj dizajniran da ukloni vodeni pečat sa Alisinih filmova. Koristeći ovaj uređaj, on može da napravi nelegalne kopije Alisinih filmova.

U svakom od ovih scenarija Bob izvodi prevaru sa namerom da zloupotrebi Alisine vodene pečate kako bi izvodio operacije koje mu nisu dozvoljene.

U I scenariju on izvršava neovlašćenu operaciju ugrađivanja, odn. napad falsifikovanjem, ugrađivanjem vodenog pečata koji bi samo Alis trebala da može da ugradi.

U II scenariju on izvršava neovlašćenu detekciju, odn. pasivan napad, detektovanjem vodenog pečata koji bi samo Alis trebala da može da detektuje.

U III scenariju on izvršava neovlašćeno uklanjanje vodenog pečata koji ne bi trebalo da može da ukloni.

Svaka od ove tri kategorije napada postavlja sopstvene tehnološke izazove dizajnerima sigurnih vodenih pečata.

⁹³ Ova imena se najčešće, pored Kerol i Eva, koriste kao standardna u opisivanju kriptografskih problema.

Značaj sprečavanja svakog od ovih napada zavisi od primene. Korisno je analizirati sigurnosne zahteve svake primene pojedinačno određujući kome je dozvoljeno da obavi koju operaciju. Date primene su podeljene u različite grupe i dodeljen im je set dozvola. Rezultujuća operativna tabela, tabela br.3, određuje sigurnosne osobine za sistem zaštićen vodenim pečatom.

Ova tabela pokazuje dozvole za brojne različite grupe u svakom od tri različita scenarija. Značajno je da za mnoge ulaze nije bitno da li određena grupa može da izvrši pojedine operacije, zato što to ne bi direktno uticalo na sistem. Može se ispostaviti da je teško ili nemoguće odbiti grupu dozvola za jednu operaciju dok im se dozvoljava da izvršavaju drugu grupu operacija. Npr. pitanje je da li sistem može biti dizajniran da dozvoljava pojedincima da ugrađuju pečat, a da im uskrati mogućnost uklanjanja istog. Ako je nemoguće, morali bismo da onemogućimo javnosti mogućnost da ugrađuje vodeni pečat u *copy-control* primeni, promenom „-“ u tabeli na „N“.

Tabela 3.- Operativna tabela za tri prikazana watermarking scenarija

	Ugrađivanje	Detekcija	Uklanjanje
Monitoring emitovanja			
Oglašavač	Da	Da	-
Emiter	Ne	Ne	-
Javnost	Ne	Ne	-
Web izveštavanje			
Servis beleženja	Da	Da	-
Servis izveštavanja	-	Da	-
Javnost	Ne	Ne	Ne
Kontrola kopiranja			
Izvođač sadržaja	Da	Da	-
Javnost	-	Da	Ne

Oznaka “Da” u tabelama br.3 i br.4 označava da određena operacija mora biti omogućena, oznaka “Ne” znači da ta operacija mora biti sprečena, dok oznaka “-” ukazuje na to da će sistem raditi bez obzira na to da li je operacija dozvoljena.

Javni i privatni vodeni pečati

Posebni slučajevi kombinovanja dozvola prikazana je u tabeli 4. U oba slučaja, podela je izvršena na *poverljive pojedince* koji su uglavnom osobe za čiju je dobit dizajniran pečat i *javnost* za koju se sumnja da je potencijalni suparnik. Termin poverljivi pojedinci odnosi se na privatni *watermarking* i on ne dozvoljava javnosti da pristupa vodenom pečatu na bilo koji način. S druge strane, javni *watermarking* javnosti dozvoljava da detektuje vodeni pečat i ništa više. Javni i privatni *watermarking* se odnose na sigurnosne zahteve u odnosu na primenu vodenog pečata.

Tabela 4.- Operativna tabela za dve kategorije primene watermarkinga: privatni i javni

	Ugrađivanje	Detekcija	Uklanjanje
Privatni watermarking			
Poverljivi pojedinci	Da	Da	-
Javnost	Ne	Ne	Ne
Javni watermarking			
Poverljivi pojedinci	Da	Da	-
Javnost	Ne	Da	Ne

Slična terminologija se koristi za opisivanje algoritama vodenih pečata. *Privatni vodeni pečat*, ili privatni *watermarking* sistemi, odnose se na tehnologije za prvi set sigurnosnih zahteva u tabeli 4. Slično tome, *javni vodeni pečat*, ili javni *watermarking* sistemi, se odnose na drugi set. Korišćenje termina „javni“ i „privatni“ je dvosmisleno, zato što većina tehnologije može koristiti bilo koji tip primene.

Sistem koji koristi informisane detektore često se naziva privatnim, pod pretpostavkom da javnost nema pristup originalnom Radu koji je potreban za detekciju. Može postojati javna *watermarking* aplikacija u kojoj javnost ima pristup originalnom Radu.

Sistem može koristiti detekciju na slepo, bez korišćenja ključeva, koja se obično naziva javnom, pod pretpostavkom da javnost zna detekcioni algoritam. Ako je algoritam držan tajno, on se i dalje može koristiti za privatnu *watermarking* primenu. Sigurnost ovakvog sistema bi teško mogla da se potvrdi pre razvitka.

Sistem koji koristi detekciju na slepo, ali koristi ključeve, jednako je pogodan za obe vrste primena. Važna razlika između javnog i privatnog sistema je samo u tome kako su ključevi distribuirani.

Kategorije napada

U tabelama 3 i 4 date su naznake kome je dozvoljeno da obavlja koji postupak. U okviru ove tri kategorije delovanja prikazanih u kolonama postoje mnoge varijacije. Često je moguće da suparnik obavlja deo nedozvoljenih postupaka, iako ne može da obavi neki od postupaka u potpunosti. U zavisnosti od primene, takvi delimični napadi mogu imati ozbiljne posledice. Zbog toga je neophodno praviti razliku između svakog od tri tipa naznačenih kategorija neovlašćenih delovanja u specifičnije tipove napada.

Neovlašćeno ugrađivanje

Najsloženiji tip neovlašćenog ugrađivanja iziskuje da suparnik stvori i ugradi originalnu poruku, odnosno mora da napravi poruku koja će identifikovati Rad kao njegov i napravi alat za ugradnju.

Manje složen tip javlja se kada suparnik nastoji da promeni legitimnu poruku, a da prethodno ne stvori novu, i ugradi je u Rad.

Neovlašćena detekcija

U pojedinim primenama vodenog pečata u kojima bi mogućnost detektovanja trebala da bude onemogućena, s početka se brinemo o sprečavanju ljudi da dekodiraju značenje vodenog pečata.

U drugim slučajevima suparnik se može zadovoljiti jednostavnim saznanjem da li vodeni pečat postoji ili ne, bez interesovanja za značenje dešifrovane poruke. Ovaj problem se pre može svrstati u steganografiju nego u zaštitu vodenim pečatom. Razumljivo je da se primena vodenog pečata može naći u sistemu koji može biti kompromitovan od strane suparnika koji samo identifikuje da li je pečat prisutan u određenom Radu. U poglavlju 2.3.6.4. predloženi su napadi analizom osetljivosti i napad na uspon nagiba gde je mogućnost detektovanja prisustva vodenog pečata veliki izazov suparniku koji pokušava da ukloni pečat. S toga, razumljivo je da ako vodeni pečat treba da bude otporan na neovlašćeno uklanjanje mora da bude otporan i na neovlašćenu detekciju. Sigurnost protiv dešifrovanja, bez sigurnosti protiv detekcije, nije dovoljna.

Treći slučaj neovlašćene detekcije, koja se nalazi između potpunog dešifrovanja i potpune detekcije, događa se kada suparnik može praviti razliku između pečata koji šifrira različite poruke, čak i kada nije upoznat sa značenjem te poruke. Suparnik može da za data dva Rada zaštićena vodenim pečatom kaže da li dotični vodeni pečati šifriraju iste ili različite poruke. Ovaj tip napada predstavlja problem ako suparnik može da odredi značenje poruke na

drugačiji način od dešifrovanja iste. Npr. u drugom scenariju Bob hoće da ukrade Alisine klijente pronalaženjem njihovih identifikacija na Internetu.

Ona može da pokuša da se zaštiti korišćenjem tajnog koda za udruživanje vodenih pečata za svoje klijente i na taj način spreči Boba da dešifruje vodene pečate kako bi identifikovao vlasnike Radova. Ako Bob može pouzdano da odredi da li dva Rada sadrže isti vodeni pečat, on može da ukrade Alisin posao. On jednostavno može da zatraži od bilo kog potencijalnog klijenta da mu prosledi jedan primerak Alisinog Rada koji je zaštićen vodenim pečatom. Kada sazna da i drugi Rad na Internetu sadrži isti vodeni pečat, znaće da oni pripadaju istom klijentu. U ovom slučaju nema potrebe da Bob zna kako je Alis šifrovala identifikaciju za svakog klijenta u vodenom pečatu.

Neovlašćeno uklanjanje

Vodeni pečat se smatra uklonjenim iz Rada ukoliko je njegovo postojanje nedetektibilno. Najekstremniji slučaj takvog uklanjanja bi vratilo Rad u njegovu originalnu, nezaštićenu, formu. U svim primenama vodenog pečata koje zahtevaju sigurnost protiv neovlašćenog uklanjanja, neophodno je sprečiti suparnika da povрати Rad.

Suparnik će u većini slučajeva pokušati da promeni zaštićen Rad tako da povрати original i uz to ne pokrene detektor vodenog pečata. Da bi se pokazalo suparniku da je vodeni pečat siguran od uklanjanja potrebno je pokazati mu da se originalni Rad ne može povratiti.

Suparnik može koristiti ograničenje kojim će zahtevati da deformacija uvedena napadom proizvede minimalne perceptualne promene. Ovo je slično korišćenju ograničenja verodostojnosti, ali perceptualni model korišćen od strane suparnika nije potrebno da bude korišćen za ugrađivanje. Suparniku su zahtevi za verodostojnosti uglavnom strožiji od onih za ugrađivanje. U ovom slučaju verodostojnost je merena između Rada zaštićenog vodenim pečatom i napadnutog Rada.

U okviru Rada koji će zadovoljiti suparnika, razlika je često napravljena između onog u kom je vodeni pečat zaista uklonjen i onog u kom je vodeni pečat još uvek prisutan, ali može biti detektovan samo veštijim detektorom od onog koji je bio korišćen. Ova vrsta napada se odnosi na uklanjanje vodenog pečata.

Napad maskiranjem vodenog pečata može se sprovesti napadom na slikovni *watermarking* sistem u kom detektor ne može da detektuje ugrađeni vodeni pečat u slici koja je blago rotirana. Suparnik može da ukloni vodeni pečat iz bilo koje slike primenjujući blagu rotaciju. Veštiji detektor će uz korišćenje neke vrste registracije pretraživanja moći da invertuje rotaciju i ipak detektuje vodeni pečat.

Ova vrsta napada je u suprotnosti u odnosu na napad eliminacijom u kojoj suparnik pokušava da proceni deo ugrađenog vodenog pečata i oduzme ga. Rezultat takvog napada može biti najbliža originalnom Radu.

Razlika između napada maskiranjem i eliminacijom je jasna. Oba napada, napad rotacijom i napad procenjivanjem i odstranjivanjem, pomeraju tačke granica regije za detektovanje (u Radu zaštićenom vodenim pečatom) na tačke izvan nje (u nezaštićenom Radu). Zamenom detektora sa onim detektorom koji izvodi geometrijsku pretragu minimalnim menjanjem regije detekcije uključujemo u pretragu i Rad napadnut rotacijom. Prikaz je dat na slici broj 16.

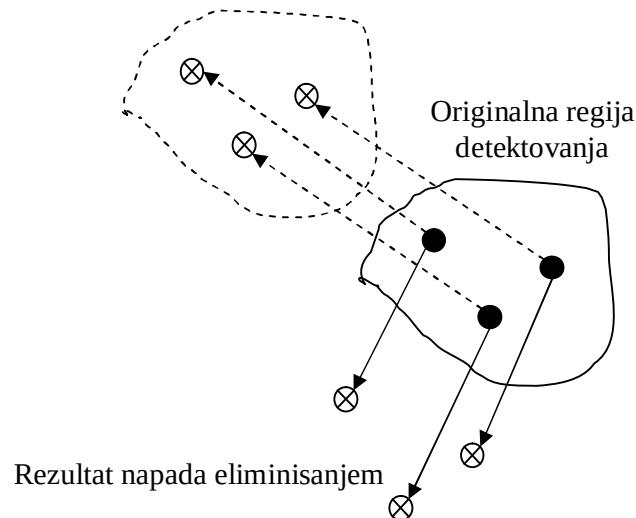
Ako je moguće odbiti napad rotacijom kreiranjem veštijeg detektora, zašto se ne bi svaki napad odbio na ovaj način?

Napad koji vraća istovetni originalni Rad, ne može biti odbijen modifikovanjem detektora. Možemo identifikovati druge napade koji takođe ne mogu biti ubrojeni u ovaj način, ispitivanjem gde napadnut Rad leži u media prostoru⁹⁴ u odnosu na distribuciju

⁹⁴ Visoko dimenzionisan prostor u kom svaka tačka odgovara jednom Radu.

sadržaja zaštićenog vodenim pečatom. U slučaju napada rotacijom, napadnut Rad još uvek poseduje neobične osobine koje mu je proces ugrađivanja dodelio. Oni će se malo verovatno javiti u distribuciji nezaštićenog Rada. Ako promenimo regiju detekcije da bismo uključili oblast oko napadnutog Rada, nećemo znatno podići lažno pozitivnu mogućnost.

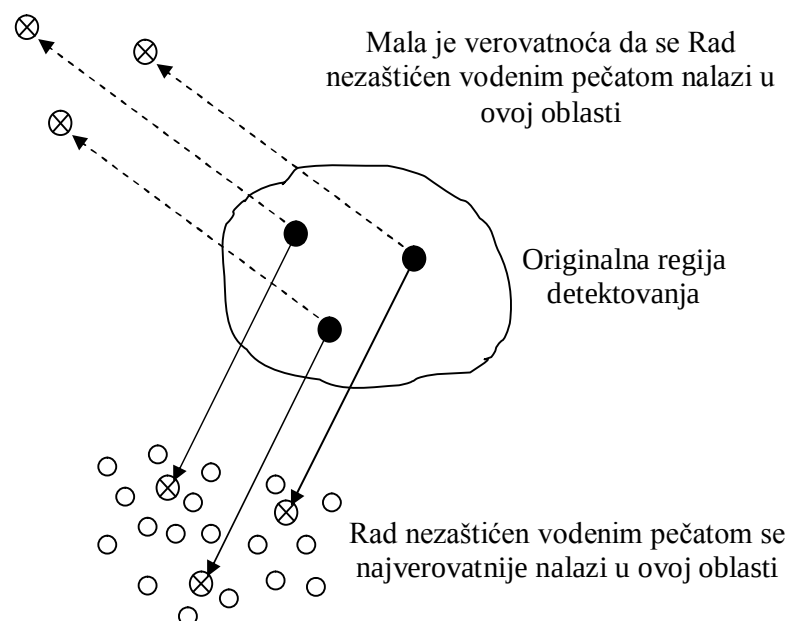
Rezultat napada maskiranjem



Slika 16.- Ilustracija napada eliminisanjem i maskiranjem

S druge strane, ako promenimo regiju detekcije da bismo uključili oblast oko napadnutog Rada, napadom procenjivanja i odstranjivanja, neprihvatljivo ćemo povećati lažno pozitivne odgovore.

Možemo definisati napad eliminisanjem kao napad koji pomera zaštićen Rad u regiju media prostora gde se verovatno nalazi nezaštićen Rad i napad maskiranjem kao napad koji pomera zaštićen Rad u regiju u kojoj se malo verovatno nalazi nezaštićen Rad. Razlika između ova dva napada prikazana je na slici broj 17.



Slika 17.- Prikaz značajne razlike između napada eliminisanjem i maskiranjem

Razlika između napada eliminacijom i maskiranjem može biti važna u primenama u kojima je izvodljiva promena detektora nakon što je napad otkriven. U primenama u kojima je moguća nadgradnja detektora, napad maskiranjem je manje posledičan u odnosu na napad eliminacijom.

Napad na sistem

Treba imati u vidu da nisu svi napadi na sistem vodenih pečata napadi na same pečate. Suparnik se često može sukobiti sa sistemom bez izvršenja bilo koje od prethodno navedenih neovlašćenih akcija. Napad koji iskorišćava slabosti načina na koji je korišćen vodeni pečat, pre nego slabosti samog vodenog pečata, naziva se napadom na sistem.

Jednostavan primer napada na sistem jeste primena kontrole kopiranja gde se u svaki uređaj za snimanje priključuje kompjuterski čip za detektovanje vodenog pečata. Suparnik može otvoriti uređaj i jednostavno izvaditi čip i tako omogućiti snimanje nelegalnih kopija. U takvom napadu, sigurnost samog vodenog pečata je nevažna. S obzirom da se u ovom radu obrađuju tehnologije zaštite vodenim pečatom i da je napad na sistem van ove teme, bitno je spomenuti i njega i uzeti ga u obzir kada se dizajnira sistem koji koristi vodene pečate, jer će napadač uvek napadati najslabiju kariku u sigurnosnom lancu.

2.1.17.3. Pretpostavke o suparniku

S obzirom na prikupljene tipove zahteva izraženim u tabelama 3 i 4, neophodno je napraviti neke pretpostavke o sposobnostima suparnika.

Ako napadaču nije ništa poznato

Najjednostavnija pretpostavka je da suparnik ne zna ništa o algoritmu i da ne poseduje posebne alate kao što je detektor. Pod ovim okolnostima, suparnik mora da se osloni na generalno znanje o slabostima algoritama vodenih pečata. Pretpostavimo da suparnik misli da je Rad možda zaštićen vodenim pečatom i hoće da ukloni taj vodeni pečat. On može pokušati da primeni različite deformacije koje zna, kao što su filtriranje za redukovanje šuma, ekstremna kompresija ili male geometrijske ili privremene deformacije. U pretpostavci je uzet primer osnovnog pristupa *Stirmark-ovog* programa koji često uspeva da napravi vodeni pečat nedektibilnim.

Ako napadač poseduje više od jednog Rada zaštićenog vodenim pečatom

U pojedinim slučajevima je moguće da suparnik dođe do višestruko zaštićenih radova vodenim pečatima i u takvoj situaciji može da iskoristi situaciju da ukloni vodeni pečat, čak iako ne zna algoritam. Napad koji se odnosi na posedovanje nekoliko zaštićenih Radova naziva se *napad u dosluhu* (engl. *Collusion attack*).

Postoje dva tipa ovog napada.

U prvom, suparnik poseduje nekoliko različitih Radova koji sadrže isti vodeni pečat i proučava ih da bi saznao kako algoritam funkcioniše. Ako svi radovi poseduju iste povezane delove, upoređivanjem bi dobio nešto blizu delova koje Rad poseduje. Približnim delom bi se vodeni pečat mogao odbiti iz Rada. Varijacija na prvi tip je kada se vodeni pečati ugrađuju dodatnim popločavanjem.⁹⁵ Ako su isti delovi vodenog pečata dodavani u nekoliko delova Rada, suparnik može da vidi te delove kao posebne Radove i izvrši napad u dosluhu kako bi ih identifikovao.

Drugi tip napada u dosluhu obuhvata suparnika koji poseduje nekoliko kopija istog Rada sa različitim vodenim pečatima u njima. U ovom slučaju, suparnik će možda biti u mogućnosti da dobije približnu kopiju originalnog Rada kombinujući odvojene kopije.

⁹⁵ Postupak opisan na str. 49.

Najjednostavnije kombinovanje jeste naći prosek kopija i na taj način pomešati različite vodene pečate i redukovati njihove amplitude.

Beneh i Šav⁹⁶ predložili su rešenje problema dizajniranjem šifre koja je pouzdana protiv drugog tipa napada sa dosluhom⁹⁷. Pretpostavimo da je Rad distribuiran ka n osoba, sa različito šifrovanom reči ugrađenom u svakoj kopiji. Šifri je „rečeno“ da bude sigurna za c osoba i da kada broj osoba koji poseduje zaštićen Rad dostigne c , da je tada velika mogućnost da dobijeni Rad sadrži dovoljno informacija da identifikuje bar jednu osobu koja učestvuje u napadu u dosluhu sa drugom. Ovo se može izvesti ako su šifre za sve osobe identične. Kada se uporede njihove dotične kopije, one neće moći da nauče ništa o tome kako da naškode delovima vodenog pečata i stoga možemo pretpostaviti da će oni ostati neoštećeni usled napada. Ako ovi neoštećeni delovi šifre nose dovoljno informacija, možemo identifikovati najmanje jednu osobu. Sledeći Bonehov i Šavov primer, nekoliko istraživača su prostudirali dizajn c-sigurnosne šifre i razvili alternativne formulacije.

U skorije vreme, Kajr i saradnici⁹⁸ su formalizovali slučaj gde napadač poseduje kopije zaštićenog Rada. Tačnije, oni su razmatrali slučajeve napada:

- Samo na vodeni pečat u kom suparnik ima pristup brojnim Radovima zaštićenim vodenim pečatom.
- Na poznatu poruku u kom suparnik ima pristup brojnim Radovima zaštićenim vodenim pečatom i njihovim pridruženim porukama
- Na poznati originalni Rad u kom suparnik ima pristup brojnim Radovima zaštićenim vodenim pečatom i njihovim pridruženim originalnim Radovima. U ovom slučaju, cilj suparnika je da dobije informaciju o tajnom ključu, kako bi napao drugi Rad zaštićen vodenim pečatom za koji je originalni Rad nedostupan.

Ako napadač zna algoritam

Za sistem koji zahteva visok nivo sigurnosti, sumnja da suparnik ne zna ništa o algoritmu vodenog pečata se smatra nesigurnom po sistem. Često je teško održati algoritam potpuno tajnim. Ako algoritam treba da se održi tajnim, samo mali broj istražitelja ga može ispitivati.

Iz ovih razloga, advokati kriptografske zajednice pretpostavljaju da suparnik zna sve o algoritmu osim jednog ili više tajnih ključeva. Ovo je poznato kao *Kirkhova pretpostavka*.

Suparnik koji ima potpuno znanje o algoritmu vodenog pečata može pronaći i iskoristiti slabosti u strategiji detektovanja. Pa tako, ako je u mogućnosti da identifikuje specifičnu deformaciju koju detektor ne može da popravi, nakon toga može uspešno primeniti napad maskiranjem.

Poznavanje algoritma vodenog pečata može pomoći suparniku da odredi tajnu koji opisuje određeni vodeni pečat. Jednom kada otkrije tajnu, suparnik je u mogućnosti da izvrši neovlašćeno ugrađivanje, detektovanje ili uklanjanje vodenog pečata.

Ako napadač poseduje detektor

Ako aplikacije određuju da suparnik mora imati dozvolu da izvede neku akciju, moramo sumnjati da on poseduje alat potreban za izvođenje istih. Slučaj koji je najčešće analiziran jeste onaj u kom je suparniku dozvoljeno da detektuje vodeni pečat, ali ne i da ga ukloni, i u ovakvom slučaju moramo pretpostaviti da suparnik poseduje detektor.

Čak i kada suparnik ne zna ništa o algoritmu, pristup detektoru mu daje ogromnu pomoć u napadu na vodeni pečat. Može se razmisliti o detektorima poput „crne kutije“ ili „orakl“, kod kojih suparnik može podneti promenjen Rad i na taj način saznati da li je u regiji

⁹⁶ Boneh D. i Shaw J., 1995. [8]

⁹⁷ Engl. *Collusion-secure codes*

⁹⁸ Cayre F., Fontaine C., i Furon T., 2005. [11]

detekcije. Ponavljanjem promena na Radu i testiranjem posle svake promene, može se saznati kako algoritam detektovanja, većim delom, funkcioniše.

Još teži sigurnosni problem javlja se kada suparnik poseduje detektor i saznanje na koji način on funkcioniše. U suštini, on poznaje algoritam detekcije i bilo koji ključ potreban za detekciju određenog pečata. Do danas nije predložen nijedan *watermarking* algoritam koji može sprečiti neovlašćeno uklanjanje pod ovim uslovima, mada su postojali pokušaji primenjivanja principa asimetričnog kriptografskog ključa za rešenje ovog problema.

2.1.17.4. Sprečavanje napada i bitniji napadi na sigurnost sistema DVP-a

Napadi na sigurnost sistema DVP-a se mogu sprečiti na sledeće načine:

- Neovlašćena detekcija DVP-a bez dešifrovanja zahteva da vodeni pečat ne sme promeniti statističke osobine Rada.
- Prikriveno uklanjanje zahteva vešt detektor koji može detektovati i preinačiti maskiranu deformaciju.
- Neovlašćeno uklanjanje zahteva sprečavanje suparnika da identifikuje granicu detektovane regije. Drugačiji je slučaj kada suparnik poseduje detektor.

Bitni poznati napadi na sigurnost sistema DVP-a :

- **Napad izokretanjem** je napad na nivou sistema u kom se uzorci Rada izokreću pre prezentovanja detektoru vodenog pečata i zatim se naknadno de-izokreću.
- **Patološko deformisanje** podrazumeva bilo koji proces koji održava verodostojnost Rada i koji bi mogao da bude koristan suparniku za prevaru detektora maskiranjem ili eliminisanjem vodenog pečata. Dve najčešće kategorije patološkog deformisanja su napad sinhronizacijom i napad linearnim filtriranjem i uklanjanjem šuma.
- **Napad kopiranjem** podrazumeva kopiranje vodenog pečata sa jednog Rada na drugi od strane suparnika.
- **Dvosmislen napad** kreira priviđenje da je vodeni pečat ugrađen u Rad kada se zapravo takvo ugrađivanje nije ni desilo i on se može smatrati neovlašćenim ugrađivanjem. Ova vrsta napada se može izvršiti i sa informisanom i slepom detekcijom.
- **Napad analizom osetljivosti** je tehnika koja se koristi za neovlašćeno uklanjanje vodenog pečata kada suparnik poseduje detektor crne kutije.
- **Napad opadanjem gradijenta**⁹⁹ podrazumeva da suparnik poseduje detektor koji izveštava stvarnu detektovanu vrednost i on koristi promene vrednosti, kako se Rad polako menja, da odredi nagib detektovane statistike u Radu zaštićenom vodenim pečatom.

3. ISTRAŽIVAČKI RAD: STUDIJE SLUČAJA

3.1. Antiforezički alat *Evidence Eliminator*

Evidence eliminator je softver proizveden od strane Engleske korporacije „Robin Hud softver ltd. Notingem“. On predstavlja najistaknutiji alat za čišćenje hard diska računara, sa Windows operativnim sistemom, koji poražava softvere koji koristi policija i državne službe. Objavljivao je na naslovnim stranama vodećih magazina širom sveta i poseduje izvrsnu reputaciju za kvalitet i inovacije u zaštiti sigurnosti klijenata, osiguravanju korporacijskih mreža i javnih računara u školama, koledžima, univerzitetima i bibliotekama. *Evidence eliminator* je najprodavaniji proizvod ovog tipa sa preko milion preuzimanja u Americi, Evropi... Hiljade pravosudnih i policijskih sistema su preuzimali i koristili u radu *Evidence eliminator*.

⁹⁹ Engl. *Gradient descent attacks*

Rutinski forenzički alati poput *EnCase*, *FTK*, *iLook*, *F.R.E.D.* itd. koje digitalni forenzičari i istražitelji kompjuterskog kriminala koriste u radu, mogu izvući (oporaviti) digitalne dokaze sa delova hard diska za koje obični korisnici računara misle da su prazni. Međutim, ti delovi su nakon, npr. reinstaliranja sistema, još uvek puni „osetljivih informacija“ koji možda nisu namerno preuzimane, a istovremeno takav materijal može predstavljati i ozbiljno krivično delo kompjuterskog kriminala. Digitalni forenzičar zna da se jednostavnim brisanjem (*Delete*), ili čišćenjem kante (*Recycle bin*), ili formatiranjem diska, ne mogu uništiti pojedine informacije uskladištene na hard disku, dragocene za dokazivanje kompjuterskog kriminala.

Sakrivanje istorije (*Hiding history*) rada na Internetu daje lažni osećaj sigurnosti, jer iako podaci izgledaju sakriveni, ne znači da su dokazi nestali iz računara. Čak i fajlovi koji se odnose na Internet pretragu, koje mi namerno ne čuvamo, ostaju snimljeni na hard disku kao trajni dokaz (na primer, tragovi u Registrima).

Kako su svega ovoga kompjuterski kriminalci svesni, *Evidence eliminator* je postao antiforenzički alat u masovnoj upotrebi. Ovaj alat je moćan program, jednostavan za upotrebu i nijedan drugi komercijalni program ne može da izvrši iste funkcije kao on. *Evidence eliminator* svakodnevno brzo i uspešno vrši duboko čišćenje kompjutera od kompromitujućeg materijala. Za njega se tvrdi da uništava:

- Windows SWAP file,
- Windows Application logs,
- Windows Temporary Files,
- Windows Recycle Bin,
- Windows Registry Backups,
- Windows Clipboard Data,
- Start Menu Recent Documents history,
- Start Menu Run history,
- Start Menu Find Files History,
- Start Menu Find Computer History,
- Start Menu Order Data,
- Start Menu Click History,
- Microsoft Internet Explorer privremeno otkucane URLs, index fajlove, keš istoriju,
- Microsoft Internet Explorer AutoComplete memoriju poslednje lokacije i pasvorde,
- Microsoft Internet Explorer Cookies (Selectivno čuvanje cookie za verzije 5 i više),
- Microsoft Internet Explorer Internet components (selektivno čuvanje komponenti),
- Microsoft Internet Explorer Download Folder memoriju
- Microsoft Internet Explorer Favoursites List,
- Microsoft Outlook Express v5+bazu podataka (Selectivno čuvanje pošte i vesti),
- Windows Media Player History,
- Windows Media Player PlayLists in Media Library,
- America OnLine Instant Messenger contacts,
- Netscape Navigator privremeno otkucane URLs, index fajlove, keš i istoriju,
- Netscape Navigator Cookies (Selectivno čuvanje cookie za verzije 4 i više),
- Netscape Mail v4+ poslate i izbrisane e-mails,
- Netscape Mail hidden files,
- Kastomizovane liste fajlova i foldera, sa ili bez njihovog sadržaja,
- Kastomizovane liste skeniranja tipova fajlova u specifičnim folderima,
- Kastomizovane liste skeniranja tipova fajlova u svim diskovima/particijama,
- Izbrisana imena fajlova, veličine i atributi iz struktura direktorijuma,
- Slobodan prostor klastera ("File Slack") iz fajlova svih tipova,
- Magnetski ostaci prethodnih fajlova/foldera,

- Sav slobodan nealocirani prostor na svim čvrstim diskovima, □
- Dokazuje o aktivnostima u mnogim drugim programima, koji koriste Plug-In module,
- Slack prostor i izbrisane ulaze u Windows Registry-ju,
- Datume i vremena kreiranja i modifikovanja na svim fajlovima i folderima,
- Windows Registry nizove,
- Common Dialog lokacije preuzimanja/memorisanja istorije,
- Trenutno bezbedno brisanje podataka iz Windows Registry (NT4/2000/XP).

Evidence eliminator obezbeđuje mnoge beneficije korisnicima:

- Najkvalitetniji profesionalni program,
- Značajno ubrzava Rad računara,
- Jednostavni korisnički interfejs,
- Automatsko podešavanje bitnih mesta u kojima se skladište dokazi,
- Skriveni način Rada obezbeđuje nevidljive operacije,
- Provera sigurnosti obezbeđuje zaštitu novih korisnika,
- Program se podešava samo jednom,
- Jednim klikom obezbeđuje se svakodnevna sigurnost,
- Sigurnost brisanja slična je standardima državnih i vojnih službi SAD-a (7-struko brisanje diska sa slučajnim naizmeničnim nizom bita 1 i 0),
- Eliminisanje osetljivih podataka i fajlva- čak i ako su zaključani Windows operativnim sistemom,
- Potpuna integracija sa Windows pretraživačem,
- „Vrući taster“ za zaštitu kante za otpatke (Pritiskom Ctrl-Del osigurava se kanta),
- Automatsko pokretanje sa startovanjem Windowsa omogućava trenutni odgovor,
- Automatsko isključivanje kada je kompletiran ATX/APM uključenog računara,
- Sve glavne funkcije su dostupne direktno sa podešene start bar ikone,
- Prihvaćeni sigurnosni standardi gašenja i restartovanja Windowsa (Win 95/98),
- Opcione komandne linije za *task schedulers*,
- Iscrpno beleženje svih operacija,
- „Test mode“ olakšava dijagnostiku i beleženje bilo kojih neregularnosti na sistemskim fajlovima,
- „Quickmode“ pokreće većinu funkcija brzo, u roku od minuta,
- Sigurnost FAT, FAT 32 i NTFS fajl sistema,
- Sigurnost brojnih testova koje program izvodi,
- Automatsko prelaženje sistemskih *screensaver-a*,
- Česte nadogradnje i tehničku podršku za najnovije operativne sisteme, *browser-e* i tehnologije.

Iako ovaj antiforenzički alat značajno otežava rad digitalnog forenzičara, još uvek ostaje dovoljno tragova u računaru, koje vešti forenzičari sa moćnim forenzičkim alatima i tehnikama mogu otkriti i dokazati slučaj kompjuterskog kriminala.

Licencirani *Evidence eliminator* se može kupiti na zvaničnom sajtu www.evidence-eliminator.com.

3.2. Studija slučaja I: Detekcija i izvlačenje tajne poruke iz .bmp formata

Steganografija se najčešće primenjuje u slikama i audio fajlovima zbog njihove široke zastupljenosti na Internetu, pa su samim tim i najteži za detekciju zbog obilja informacija koje se svakodnevno plasiraju na mrežu. Pored toga, većina dostupnih steganografskih alata su osposobljeni za sakrivanje poruka, slika, HTML dokumenta, audio zapisa isl. u slike ili audio zapise kao nosioce.

U ovoj studiji slučaja, za nosioca je izabrana 24-bitna slika BMP formata¹⁰⁰, dok je tajna poruka slika JPEG formata¹⁰¹. Veličina slike je 56 KB. Softver korišćen za primenu steganografije je *wbStego 4.3*.



Slika 18.- Tajna poruka „vojska 1.jpg“

Kao fajlove nosioce ovaj program koristi .bmp fajlove, tekstualne fajlove, HTML i PDF fajlove. Kriptografija je primenjena pre šifrovanja i na taj način obezbeđena je visoka sigurnost. Iako neko ima saznanja da je sakrivena poruka u nosiocu, ne može je dešifrovati bez šifre. *wbStego4* nudi šifrovanje i razne algoritme koji su kompatibilni sa ranijim verzijama ovog programa, *wbStego 2.x* i *3.x*, kao i četiri algoritma za jaku kriptografiju: Blowfish, Twofish, CAST128, Rijndael (AES). Ovim se omogućava zaštita šifrom koja može imati i do 2 biliona karaktera, u ranijim verzijama do 256 karaktera. Ako se iskoristi jak algoritam za šifrovanje, ključ se generiše iz šifre korišćenjem heš algoritma SHA-1. Što je šifra duža i što više različitih karaktera i brojeva sadrži veća je sigurnost.



Slika 19.- Izgled prozora *wbStego* programa u poslednjem koraku

Za šifrovanje je korišćen *Blowfish* metod, jak kriptološki algoritam koji koristi 160-bitni ključ za šifrovanje (*passphrase*¹⁰²) i SHA-1 (*Secure Hash Algoritam*). Algoritam je

¹⁰⁰ Prikaz stegonosioca dat je na slici br.20.

¹⁰¹ Prikaz tajne poruke (slike) dat je na slici br.18.

¹⁰² Relativno duga lozinka koja sadrži seriju reči kao što su fraze i pune rečenice

korišćen u CBC (*Cipher Block Chaining*) modu.

Da bi se utvrdilo da li je na neku sliku primenjena steganografija, potrebno je izvršiti sledeće analize:

1. Vizuelnu analizu
2. Promene u osobinama fajla
3. Analizu heksadecimalnih podataka
4. Analizu histograma

1. Vizuelna analiza

Razlika između stego nosioca i stego medijuma nevidljiva je golim okom što se može učiti na slikama br. 20 i 21. Nevidljivost tajne poruke u steganografskom medijumu je jedan od najvažnijih zahteva koje steganografija mora da ispuni. Čak i kada se slika br. 21 uveća i posmatra nezavisno od slike br. 20 ne mogu se uočiti promene u pikselima ni u jednom njenom delu.



Slika 20.- Nosilac tajne poruke .bmp formata



Slika 21.- Steganografski medijum .bmp formata

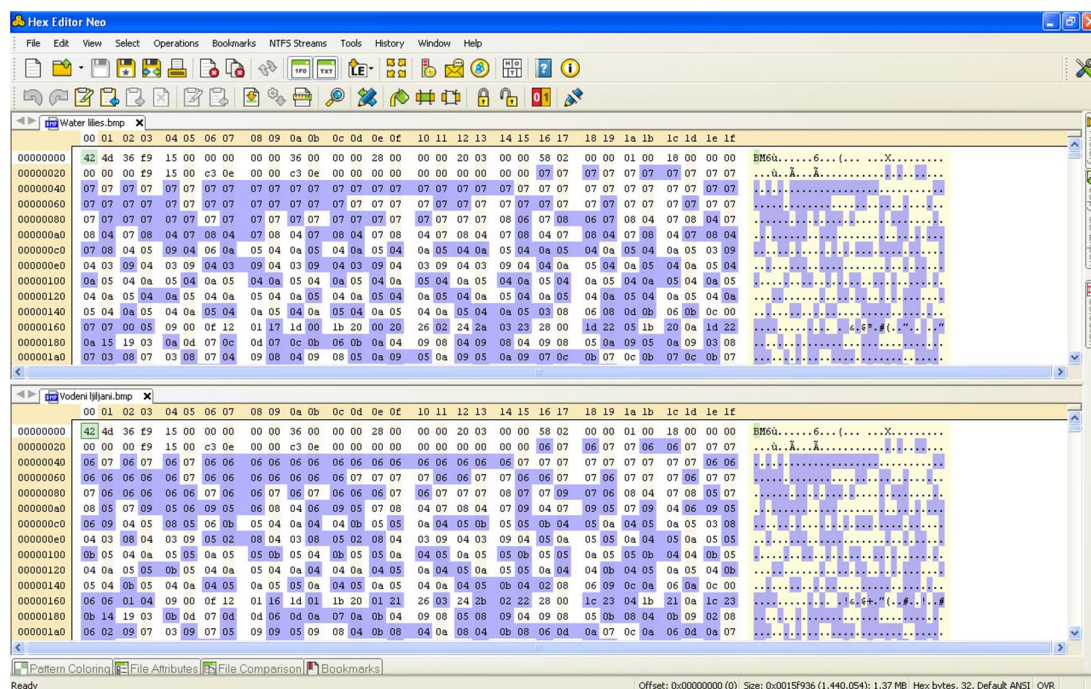
Promene u osobinama fajlova

U tabeli 5. dat je prikaz osobina. Detekcija steganografije je u ovom slučaju je veoma teška. Jedan od razloga jeste taj što su softveri za detekciju u najvećoj meri osposobljeni za detekciju samo pojedinih digitalnih formata, kao i detekciju primene pojedinih steganografskih softvera. S obzirom na to da nakon primene steganografije, sakrivanja tajne poruke u stego nosiocu, nije došlo do promene u veličini fajla, detekcija je teška čak i u slučaju da strana koja istražuje poseduje original.

Tabela 5.- Osobine fajlova .bmp ekstenzije

Naziv fajla	Datum kreiranja	Vreme kreiranja	Veličina fajla
Water lilies.bmp	22/10/2009	12:02:03 pm	1,37 MB
Vodeni ljljani.bmp	22/10/2009	12:05:12 pm	1,37 MB

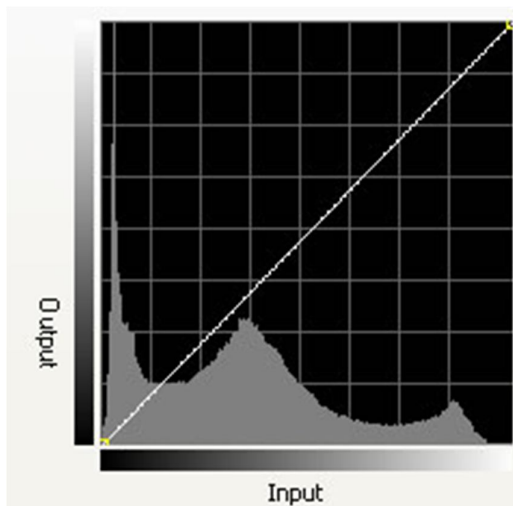
Analiza heksadecimalnih podataka



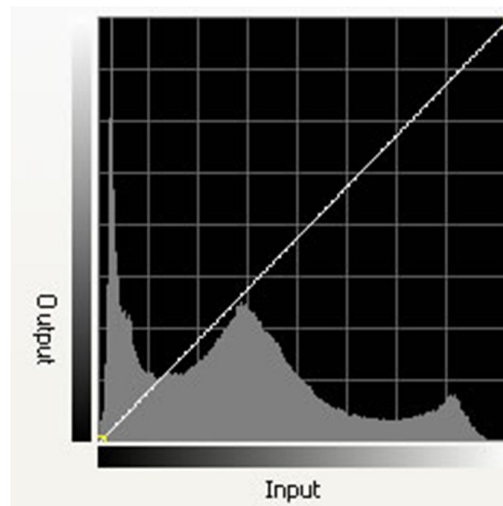
Slika 22.- Razlika u bitovima između slike „Water lilies.bmp“ i „Vodeni ljiljan.bmp“

Na slici br.24 predstavljene su razlike u heksadecimalnom zapisu. Analiza je vršena u programu „Hex Editor Neo“, upoređivanjem fajlova „Water lilies.bmp“ i „Vodeni ljiljan.bmp“. Plavom bojom su obeleženi bajtovi koji se razlikuju u fajlovima. U ovoj analizi prvi put nailazimo na čvrste dokaze da je na slici „Water lilies.bmp“ primenjena steganografija. Treba napomenuti da je ovu analizu nemoguće izvršiti ukoliko osoba koja ispituje stego medijum ne poseduje original sliku, odnosno stego nosioca. Pored toga, u okviru stegomedijuma identifikovan je format sakrivenog fajla kao *.bmp* format. Heksadecimalni zapis ovog formata je *42 4D*, dok je ASCII *BM*.

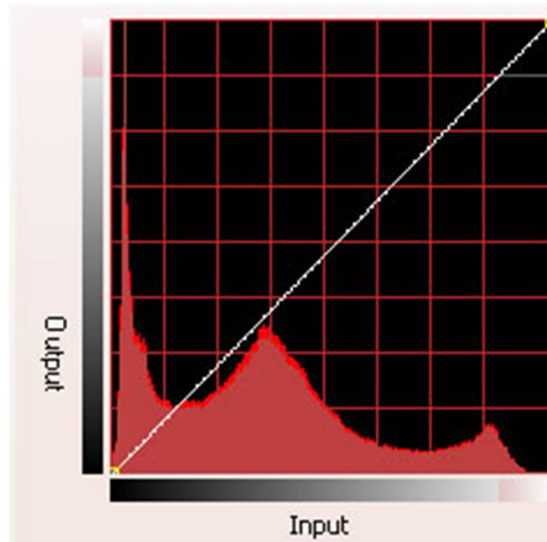
2. Analiza histograma



Slika 23.- Histogram slike „Water lilies.bmp“



Slika 24.- Histogram slike „Vodeni ljiljan.bmp“



Slika 25.- Upoređivanje histograma slika „Vodeni ljljani.bmp i „Water lilies.bmp“

U analizi histograma upoređivani su histogrami stegonosioca i stego medijuma histograma koji su prikazani na slikama br. 23 i 24. Preklapanjem histograma uočavamo razliku koja je na slici br.25 predstavljena tamno crvenom bojom. Kao i u prethodnoj analizi, analizi heksadecimalnih podataka, i ovu analizu je nemoguće sprovesti ukoliko ne posedujemo originalnu sliku, odn. stego nosioca.

Prema prethodnim analizama sledi da je lako utvrditi da li je neka slika stegonosioc ukoliko nam je dostupna originalna slika. Problem se javlja kada u toku istrage ne posedujemo original ili računar na kom je izvršen prestup. Dodatni problem kod ove analize slučaja predstavlja format slike .bmp, jer je većina softwera za detekciju steganografije usko specijalizovana za detekciju slika sa .jpg ekstenzijom.

Da bi se u slikama drugih formata detektovala prisutnost tajne poruke, na te slike se može primeniti napad na najmanje važne bitove (LSB napad). Postoji nekoliko podkategorija ovog napada, a s obzirom da nam je cilj da detektujemo primenjenu steganografiju, primenićemo **hi-kvadrat** test.

Hi-kvadrat test

Za LSB ugrađivanje, vrednost paranih piksela ostaje ili nepromenjena ili je podignuta za 1, dok je vrednost neparnih ili ostala nepromenjena ili je smanjena.

Neka $T_c[j], j = 0, \dots, 255$ označava intenzitet histograma stego nosioca i T_s odgovarajući histogram stego slike nakon ugrađivanja qn bita, gde je n ukupan broj piksela i $0 \leq q \leq 1$. Iz ovoga sledi da ugrađujemo q bitova po pikselu (bpp-bits per pixels) ili da je q relativna dužina poruke.

Da bismo izračunali T_s kao funkciju od T_c i q pretpostavićemo da je poruka slučajni niz bitova, što je razumna pretpostavka ako je poruka šifrovana ili kompresovana. Očekivani broj

piksela $2i$ će biti promenjen u $2i+1$ i iznosiće $\frac{q}{2}T_c[2i]$ iz razloga što će prosečno jedna polovina bitova već odgovarati najmanje važnim bitovima u pikselima. Slično tome,

očekivani broj piksela $2i+1$ koji će biti promenjen u $2i$ je $\frac{q}{2}T_c[2i+1]$.

S toga, možemo napisati:

$$E\{T_s[2i]\} = \left(1 - \frac{q}{2}\right)T_c[2i] + \frac{q}{2}T_c[2i+1]$$

Jednačina 1

$$E\{T_s[2i+1]\} = \frac{q}{2}T_c[2i] + \left(1 - \frac{q}{2}\right)T_c[2i+1]$$

Za ugrađivanje cele slike, gde je $q=1$, sledi da je $E\{T_s[2i]\} = E\{T_s[2i+1]\}$

Drugim rečima, histogramski intervali (*histograms bins*) $2i$ i $2i+1$ će imati približno jednaku vrednost i to će prouzrokovati promenu stepenika u histogramu.

Značajno je to da je suma $T_s[2i] + T_s[2i+1] = T_c[2i] + T_c[2i+1]$ invarijanta¹⁰³ LSB ugrađivanja. Teorijski očekivana vrednost za $T_s[2i]$ s toga iznosi

$T_s[2i] = \frac{T_s[2i] + T_s[2i+1]}{2}$. Iz ovoga sledi da je moguće detektovati ugrađivanje LSB metodom, za $q+1$, testiranjem da li je $T_s[2i] = T_s[2i+1]$.

Za testiranje možemo koristiti samo parne vrednosti piksela i primenićemo statistički test koji može potvrditi da parne vrednosti $T_s[2i]$ prate poznatu raspodelu $\bar{T}_s[2i]$. U ovom delu ćemo primeniti Parsonsov hi-kvadrat test da bi odredili da li je $T_s[2i] = \bar{T}_s[2i]$. Hi-kvadrat test počinje izračunavanjem hi-kvadrat statistike S

$$S = \sum_{i=1}^k \frac{(T_s[2i] - \bar{T}_s[2i])^2}{\bar{T}_s[2i]}$$

Jednačina 2

sa $(k-1)=127$ stepeni slobode.

Pretpostavimo da parne vrednosti piksela zaista prate verovatnoću iznosa funkcije $T_s[2i]$, statistički test, S , prati hi-kvadrat distribuciju sa $k-1$ stepenom slobode. U praksi je primećeno da slobodni intenziteti (*bins*) moraju biti dodati tako da $T_s[2i] > 4$ da bi se osiguralo da S bude približno hi-kvadrat distribuiran.

Male vrednosti S ukazuju da podaci prate očekivanu distribuciju i iz toga možemo zaključiti da slika sadrži poruku ugrađenu LSB metodom. S druge strane, visoke vrednosti statističkog testa ukazuju na to da nema ugrađene poruke.

Statistički značaj S je meren korišćenjem, tzv. *p-vrednosti*, koja predstavlja mogućnost da bi hi-kvadrat distribuiran slučajnom varijablom sa $k-1$ stepeni slobode dostigao vrednost veću ili jednuku S :

$$p(S) = \frac{1}{2^{\frac{k-1}{2}} \Gamma\left(\frac{k-1}{2}\right)} \int_S^{\infty} e^{-\frac{x}{2}} x^{\frac{k-1}{2}-1} dx$$

Jednačina 3

Ukoliko slika ne sadrži sakrivenu poruku, S je veliko, a $p(S) \approx 0$. U praksi, računamo prag vrednosti S_{th} tako da $p(S_{th}) = \alpha$, gde je α izabran stepen važnosti. Za nivo pouzdanosti, α , odlučujemo da slika sadrži tajnu poruku ako $p(S) > \alpha$, ili, ekvivalentno tome, $S < S_{th}$.

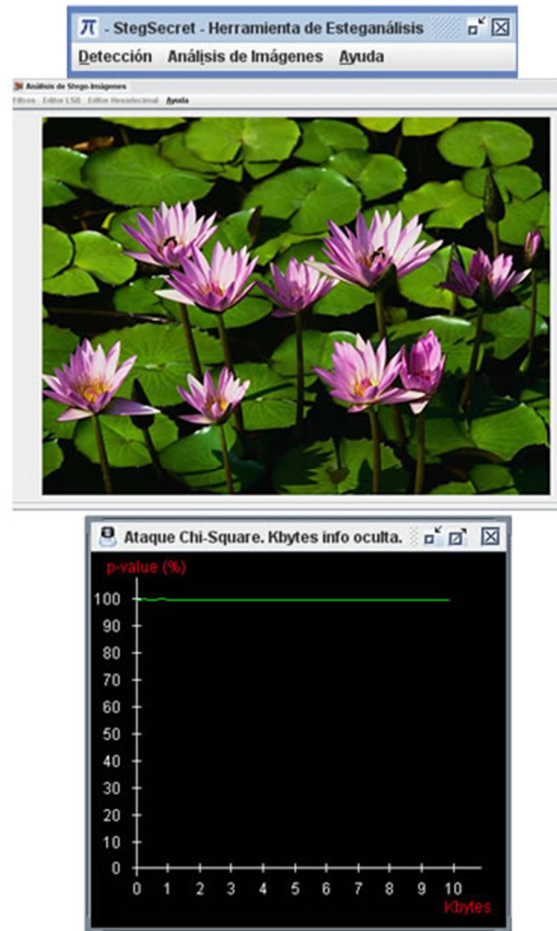
Do sada smo razmatrali potpuno ugrađenu sliku sa $q=1$ bit po pikselu. Ako je stego slika ugrađivana sekvencijalno, ali ne u potpunosti, možemo skenirati stego sliku istim redom kojim smo ugradili poruku i izračunati p za set posećenih piksela. Nakon kratkotrajne inicijalne faze, p -vrednost će biti blizu 1 i uskoro će pasti na 0 kada stignemo na kraj poruke i ostaće na 0 dok ne potrošimo sve piksele. Do ovoga dolazi zbog toga što statistički test S prestaje da prati hi-kvadrat distribuciju. S toga, za sekvencijalno ugrađivanje ovaj test, pored

¹⁰³ Svojstvo ili vrednost koja pri datim trans-formacijama ostaje nepromenjena.

toga što određuje, sa visokom verovatnoćom, da je nasumična poruka ugrađena, procenjuje dužinu ugrađene poruke.

Ako pikseli koji su nosioci poruke u slici selektovani pseudoslučajno, pre nego sekvencijalno, ovaj test je neefikasan, osim ako je većina piksela zauzeta ugrađenom porukom.

Uz pomoć softvera XStegSecret.Beta.v0.1, koji je na internet dostupan kao *freeware*,¹⁰⁴ primenjen je hi-kvadrat napad na sliku "Vodeni ljljani.bmp". Na slici br.26 je dat prikaz rezultata napada, iz čega se može zaključiti da je slika nosioc cele tajne poruke, jer je p-vrednost u najvećem delu grafikona 100% i njegova vrednost se pri kraju poruke ne bliži 0.



Slika 26.- Hi-kvadrat napad na sliku „Vodeni ljljani.bmp“

Softver StegAlyzerSS

StegAlyzerSS (*Steganography Analyzer Signature Scanner*) je najistaknutiji kompjuterski forenzički alat za istragu, detekciju, analizu i obnavljanje poruke u digitalnoj steganografiji. On forenzičarima omogućava skeniranje celog fajl sistema, pojedinačnih direktorijuma ili individualnih fajlova na prisustvo heksadecimalnih bajtova ili potpisa određenih steganografskih aplikacija. Kada se detektuje poznati potpis, moguće je izvući sakrivenu informaciju uz pomoć StegAlyzerSS-a ili korišćenjem udružene steganografske aplikacije. Pretraživanje potpisa i mogućnost automatskog izvlačenja tajne poruke nije moguće nekim drugim steganalitičkim softverom.

¹⁰⁴ stegsecret.sourceforge.net

Pored skeniranja fajlova slepom detekcijom (*blind detection*) ova aplikacija detektuje i potencijalne nosioce sakrivene poruke.

Metodologija stegaAlyzerSS

- ✓ Korišćen operativni system: *Microsoft Windows XP Service Pack 2*
- ✓ Funkcionalne analize:
 - detekcija sakrivenih korisnih podataka korišćenjem pretrage bazirane na potpisu
 - detekcija sakrivenih korisnih podataka korišćenjem dodatne analize
 - identifikacija potencijalnih fajlova nosioca osetljivih na modifikaciju najmanje važnih bitova
- ✓ Korišćeni softveri:
 - Microsoft Word 2003 Service Pack 3
 - Microsoft Paint verzija 5.1 Service Pack 2
 - Microsoft Notepad verzija 5.1 Service Pack 2
 - WinHex v.11.0
 - CrypArkan v.1.0
 - InPlain View v.1.0
 - wbStego4 v.4.2 / wbStego 4.3 open
 - wbStego v2.0 / wbStego 2.1
 - JPegX v.1.00.6
 - Camouflage v.1.0.4
 - Camouflage v.1.1.2
 - Camouflage v.1.2.1
 - Cloak v.7.0
 - Data Stash v.1.1
 - Data Stash v.1.1b
 - Data Stash v.1.0
 - Hiderman
- ✓ Korišćen hardver:
 - Gateway E4200
 - 128MB RAM
 - Jabil Pentium III BX Motherboard
 - BIOS Revision P21
 - Quantum Fireball Ict10 20GB Hard Drive

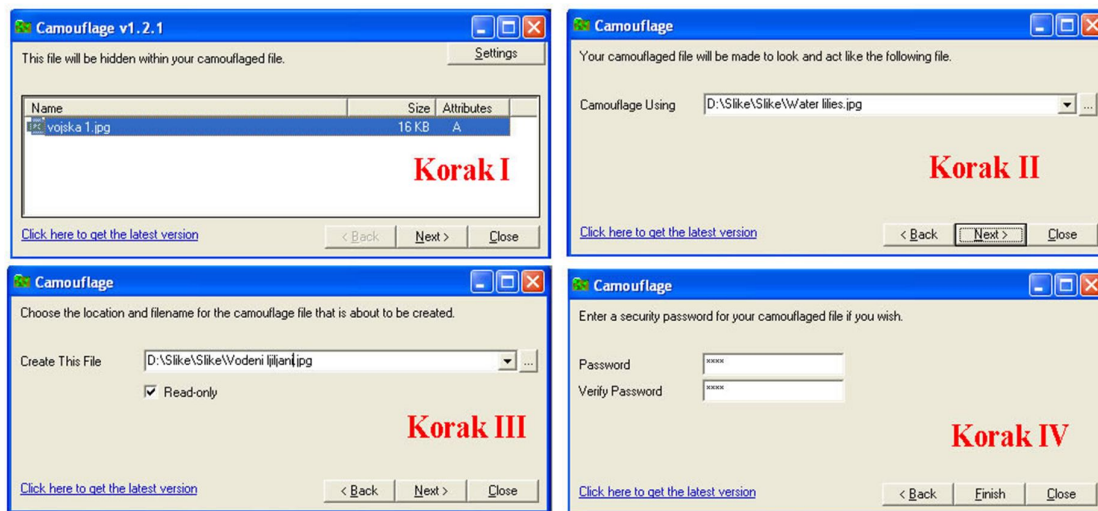
Analiza ovom aplikacijm detektovala je slike “Vodeni ljiljani.bmp” i “Water lilies.bmp” kao fajlove koji su osetljivi na LSB modifikaciju, što potvrđuje prethodno testiranje hi-kvadrat testom. Problem koji se javlja jeste taj što StegAlyzerSS nije pronašao potpis korišćenog steganografskog alata iako se program wbStego4 v.4.3 nalazi na listi programa čiji potpis ovaj alat treba da identifikuje.

3.3. Studija slučaja II: Detekcija i izvlačenje tajne poruke iz .jpg formata

U ovoj studiji slučaja korišćene su iste slike korišćene u prethodnoj studiji slučaja s tom razlikom da su formati tih slika .jpg.

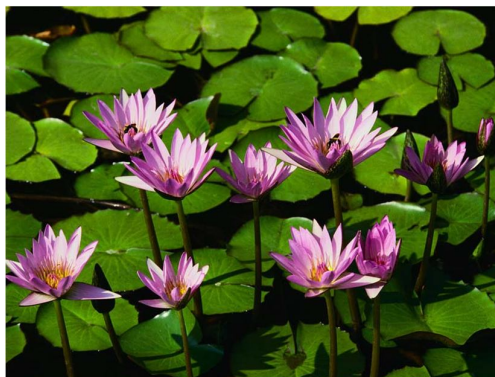
Steganografski softver korišćen u ovoj studiji slučaja je *Camouflage v.1.2.1*.¹⁰⁵ prilikom sakrivanja tajne poruke u stegonosioca korišćena je šifra *aaaa*.

¹⁰⁵ Koraci sakrivanje tajne poruke prikazani su na slici br.27

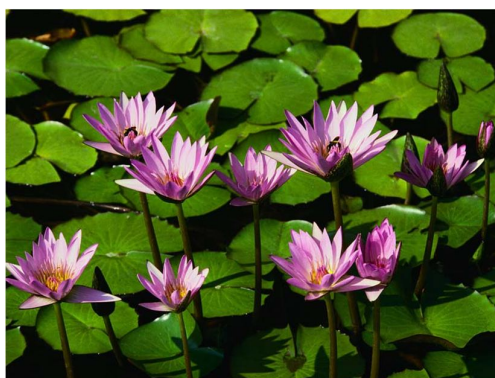


Slika 27.- Koraci sakrivanja tajne poruke alatom *Camouflage*

Vizuelna analiza



Slika 28.- Nosilac tajne slike .jpg formata



Slika 29.- Steganografski medijum .jpg formata

Razlika između stego nosioca i stego medijuma nevidljiva je golim okom što se može uočiti na slikama br. 28 i 29. Uvećanjem slike br.29 i posmatranjem nezavisno od slike br.28 ne mogu se uočiti promene u pikselima ni u jednom njenom delu.

Promene u osobinama fajla

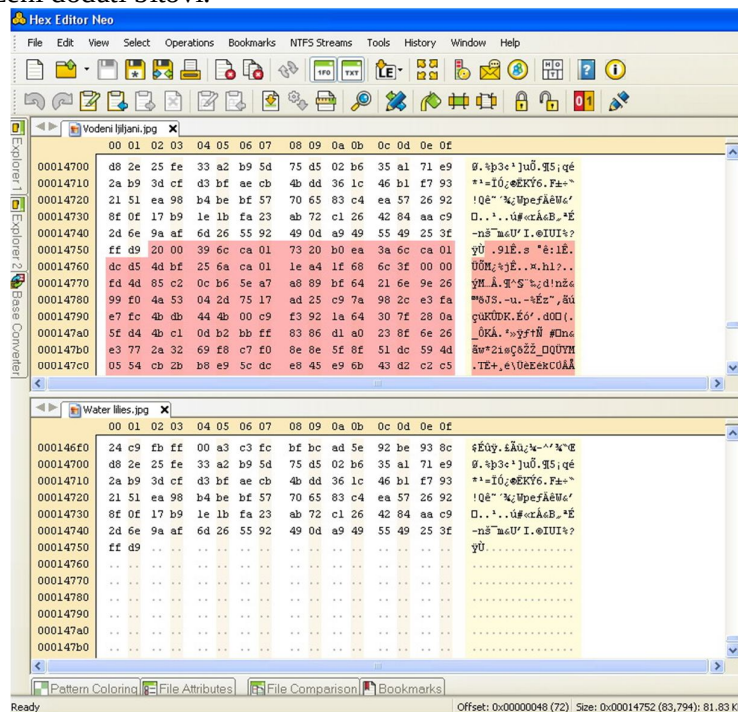
Tabela 6.- Osobine fajlova .jpg ekstenzije

Naziv fajla	Datum kreiranja	Vreme kreiranja	Veličina fajla
Water lilies.jpg	20/10/2009	01:02:21 pm	84 KB
Vodeni ljiljani.jpg	23/11/2009	02:03:18 pm	100 KB

Analizom promena u osobinama fajla došlo se do podatka¹⁰⁶ da postoji razlika u veličini fajlova, što već samo po sebi ukazuje na promene fajla „Vodeni ljiljani.jpg”, odn. ukazuje da su tom fajlu dodati podaci.

Analiza heksadecimalnih podataka

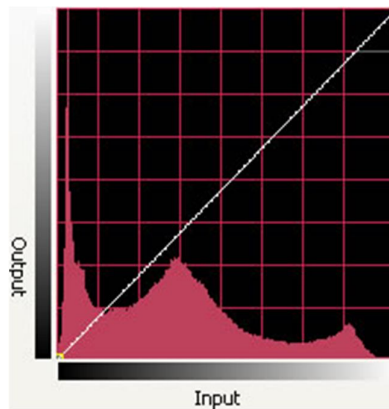
Analiza heksadecimalnih podataka vršena je softverom koji je korišćen i u prethodnoj studiji slučaja „Hex Editor Neo“. Analizom su se učvrstili dokazi iz prethodne analize, te se na slici br. 30 jasno vidi da slika „Vodeni ljiljani.jpg“ sadrži dodatno ugrađene podatke. Crvenom bojom su obeleženi dodati bitovi.



Slika 30.- Razlika u bitovima između slike „Water lilies.jpg“ i „Vodeni ljiljani.jpg“

Analiza histograma

¹⁰⁶ Podaci su prikazani u tabeli br.6.

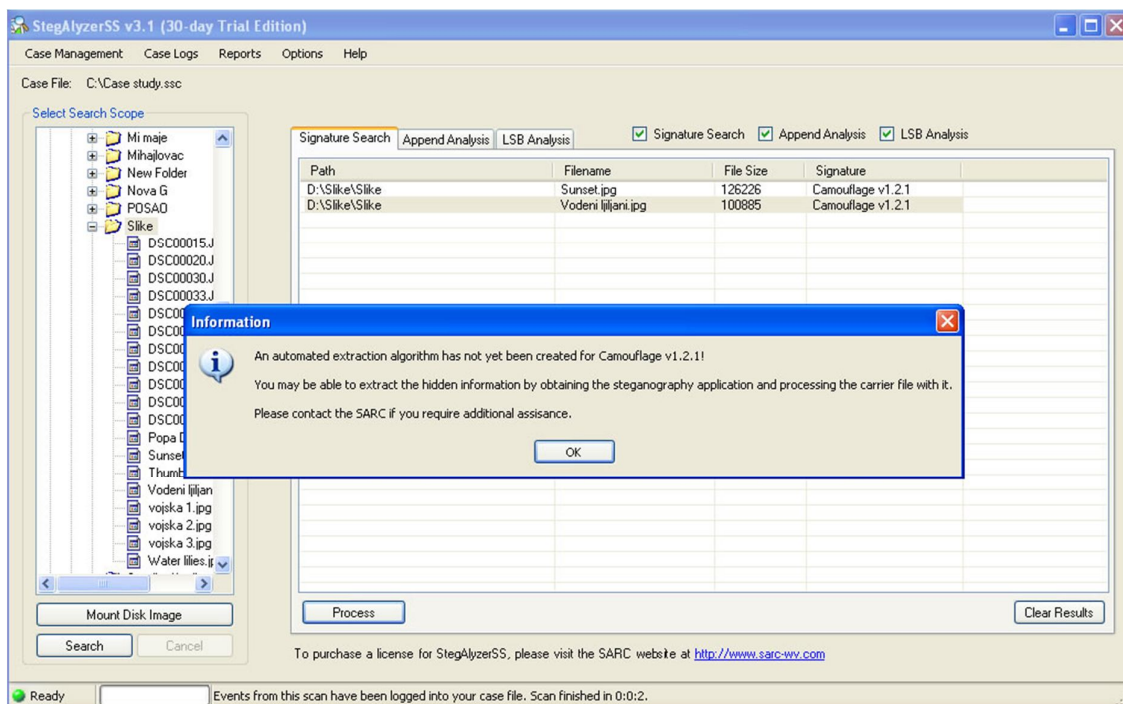


Slika 31.- Uspoređivanje histograma slika „Vodeni ljljani.jpg“ i „Water lilies.jpg“

Analizom histograma nije ustanovljena razlika između stegomedijuma i stegonosioca što je prikazano na slici br.31.

S obzirom na to da smo ustanovili postojanje dodatnih podataka, upotřebićemo StegAlzyerSS kako bismo došli do dodatnih informacija.

Analizom StegAlyzerSS-a dolazimo do podatka da su detektovana dva fajla kao stegonosioci. Softver pronalazi potpis steganografskog alata koji je korišćen. U pitanju je *Camouflage* v1.2.1. Pri pokušaju da se procesuiraj fajl „Vodeni ljljani.jpg“ StegAlyzerSS javlja obaveštenje da algoritam za izvlačenje tajne poruke nije kreiran. Prikaz dat na slici br.32. Korišćenjem dodatne analize možemo pristupiti heksadecimalnom zapisu fajla koji izaberemo. Ovom analizom utvrđeno je da je fajl koji je ugrađen u stegonosioca .jpg ekstenzije. Do ovog zaključka smo došli pronalaženjem heksadecimalnog zapisa *FF D8 FF E0 00 10 4A 46 49 46 00* ili ASCII *JFIF*. LSB analiza nije dala nikakav rezultat.



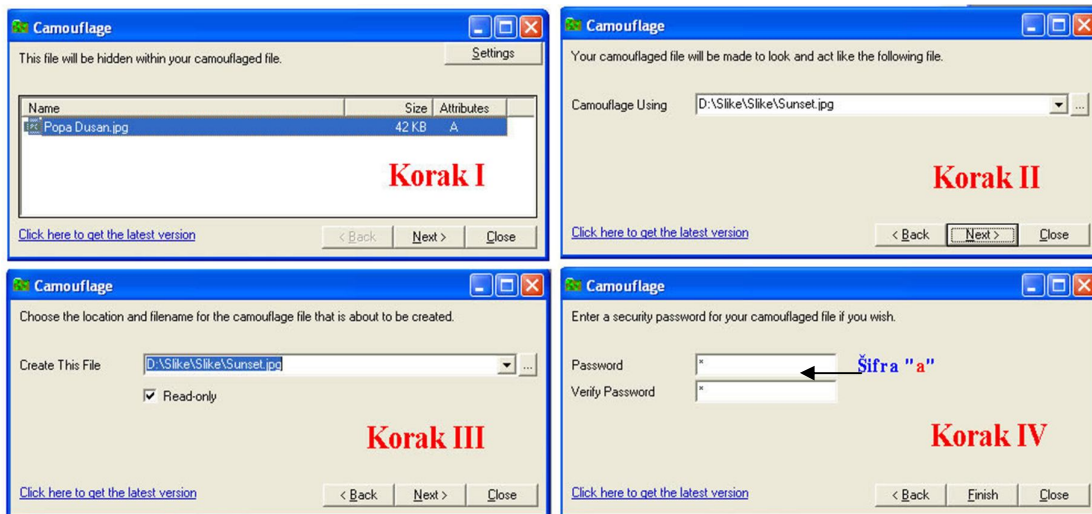
Slika 32.- Prikaz detekcije potpisa steganografskog programa

S obzirom na to da nam je poznat steganografski program kojim je tajna poruka ugrađena u stegonosica, daljim istraživanjem došlo se do sledećeg rezultata:

- Potpis programa Camouflage v.1.2.1 je sa **T.**.
- Zbog slabe kriptozastite moguće je pronaći šifru kojom je zaštićeno izvačenje tajne poruke.

U ovoj studiji slučaja biće prikazano na koji način možemo promeniti korišćenu šifru bez posedovanja originala.

Uzećemo dve nasumično odabrane slike “Sunset.jpg”, koja će poslužiti kao stegonosioc, i sliku “Popa Dusan.jpg” koja će biti tajna poruka¹⁰⁷.



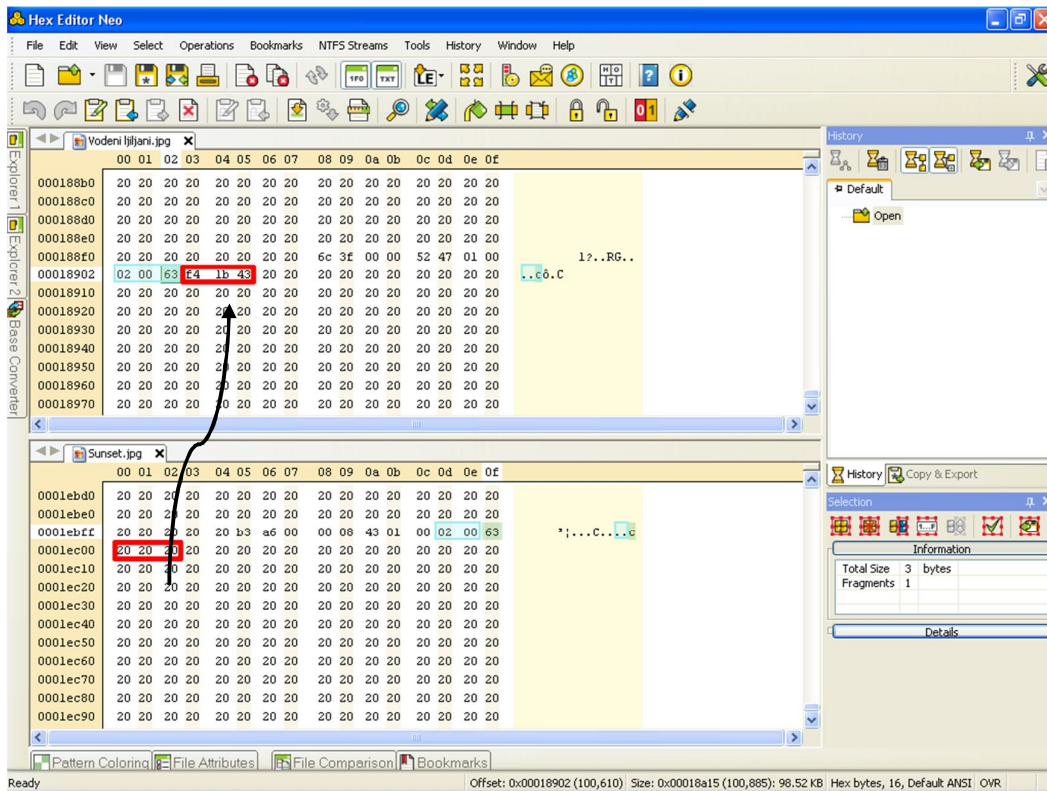
Slika 33.- Sakrivanje nasumično odabrane tajne poruke u nasumično odabranog stegonosioca

Cilj nam je da u fajlu “Sunset.jpg”, u *Hex editor*-u, pronađemo heksadecimalni zapis *00 20 00 63*. Softver *Camouflage v.1.2.1* šifru krije u 10-20 redu, nakon bitova *00 00 20 00*, ili *00 20 00* s tim da se redovi broje počev od kraja heksideciamlnog zapisa ka prvom redu. Nakon lokalizovanja ovog heksadecimalnog zapisa, isti postupak primenjujemo na sliku “Vodeni ljljani.jpg”.

Kada smo lokalizovali *00 20 00 63* u oba heksidecimalna zapisa, zamenićemo bitove u slici “Vodeni ljljani.jpg” sa bitovima iz slike “Sunset.jpg”, s tim što 63 ne menjamo, jer 63 predstavlja početak naše šifre “a”¹⁰⁸. Dakle menjamo bitove *f4 1b 43* sa *20 20 20* kako bismo obrisali ostatak šifre i zamenili je željenom, a to je „a“.

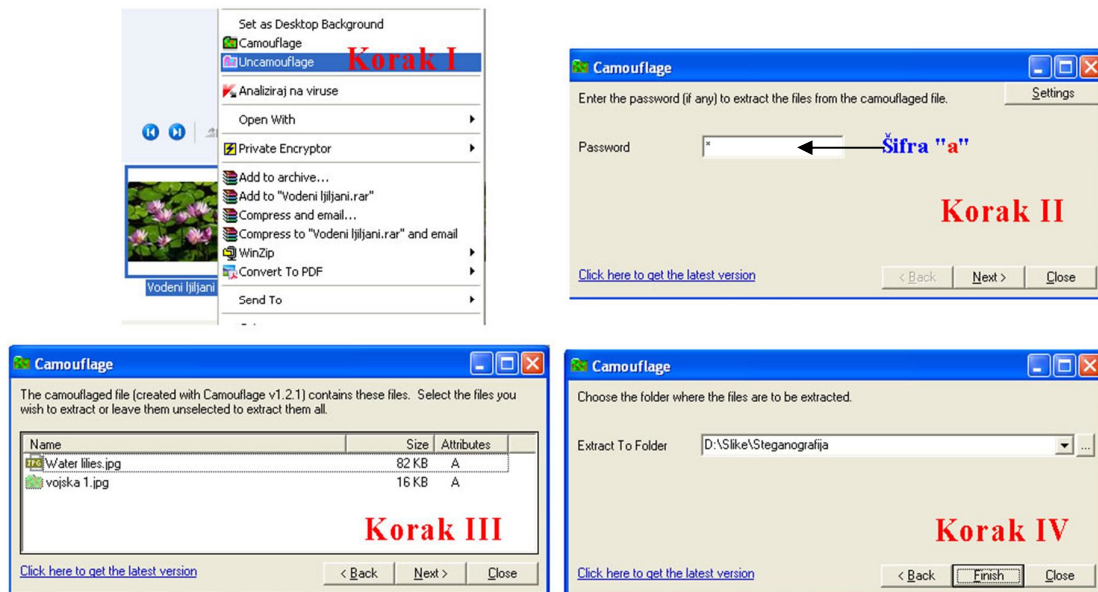
¹⁰⁷ Na slici br.35 je prikazano sakrivanje tajne poruke

¹⁰⁸ Promena bitova prikazana na slici br.34



Slika 34.- Promena bitova zbog dešifrovanja

Primenjene promene nad fajlom čuvamo i otvaramo ga kao što je prikazano na slici br.35.



Slika 35.- Koraci za izvlačenje tajne poruke novom šifrom

Ovo je jedan veoma uspešan postupak za izvlačenje tajne poruke ukoliko je ona ugrađena alatom *Camouflage* v1.2.1.

4. ZAKLJUČCI

1. Steganografija je veoma pouzdana antiforenzička tehnika. Ukoliko se isprate svi zahtevi koje je potrebno da jak steganografski metod ispuni, detekcija je veoma otežana, čak i onemogućena. Ukoliko bi skrivena poruka iznosila manje od 5% veličine stegonosioca i ukoliko bi bio primenjen jak algoritam, mala je verovatnoća za detektovanjem.
2. Većina steganografskih alata radi po principu promene najmanje važnog bita, što je jedna od svetlih tački za detekciju primenjene steganografije. Većina detektora radi po principu ispitivanja promene i upoređivanja bitova, pa je procenat pozitivne detekcije samim tim veći.
3. Nedostatak većine detektora jeste taj što su usko specijalizovani za detekciju tajnih poruka u slikama *.jpg* formata, pa slike drugih formata, poput *.bmp* ili *.gif* mogu proći kroz detektor neidentifikovane kao stegomedijumi. Razumljivo je što su detektori usmereni na detektovanje slika *.jpg* formata, jer je taj format slike najzastupljeniji na Internetu. Ovaj format je najpogodniji za transfer preko Interneta zbog veličine. Poređenja radi, za primer će se uzeti slika koja je korišćena kao stegonosioc „Water lilies“. Veličina slike u *.jpg* formatu je 81.8 KB, dok je veličina u *.bmp* formatu 1.37 MB. Prednost *.bmp* formata može se posmatrati i sa te strane da se u njega može sakriti veća poruka ukoliko za tim postoji potreba.
4. Detekcija steganografije je laka ukoliko imamo dostupnu originalnu sliku. Ova vrsta detekcije može se sprovesti jedino pod uslovom da detekcija treba da se izvrši na zaplenjenom računaru. Ova situacija bi olakšala umnogome posao forenzičara, jer je tada i veća mogućnost da je korišćen steganografski alat dostupan, pa samim tim i lako izvlačenje skrivene poruke. Ukoliko se radi o detekciji u okruženju kakav je Internet, naivna je pretpostavka da će stego nosioc biti dostupan. Dovoljno je samo promeniti mu naziv i tu se mogućnost upoređivanja stegomedijuma i stegonosioca gubi.
5. Ukoliko je forenzičaru dostupan stegonosioc može izvršiti: vizuelnu analizu, promene u osobinama fajla, analizu heksadecimalnih podataka i analizu histograma.
 - Vizuelnom analizom nemoguće je detektovanje skrivene poruke u obe studije slučaja, jer je kao stegonosioc izabrana slika sa velikim brojem boja i mnogostrukim prelazima.
 - Analizom promena u osobinama fajlova, u ***I studiji slučaja*** nismo dobili podatak da postoji sakrivena poruka, jer se veličine fajlova slažu u bajt, dok se u ***II studiji*** ova analiza pokazala kao uspešna, jer se veličine stegonosioca i stegomedijuma razlikuju.
 - Analizom heksadecimalnih podataka došlo se do prve naznake u ***I studiji slučaja*** da postoji sakrivena poruka, jer se upoređivanjem bajtova vidi da se razlikuje dosta veći broj bajtova. U ***II studiji slučaja*** se jasno vidi da u stegonosiocu postoje dodati podaci.
 - Analiza histograma je u ***I studiji slučaja*** pokazala da je u stegonosiocu sakrivena tajna poruka, jer se preklapanjem histograma pokazalo da postoje statističke anomalije. U ***II studiji slučaja*** ova analiza nije dala rezultate.
6. U ***I studiji slučaja*** za detekciju su korišćeni detektori „Stegdetect“, „StegSpy V2.1“ i „StegAlyzerSS“. Detektori „Stegdetect“ i „StegSpy V2.1“ su propustili da identifikuju sliku „Vodeni ljliljani.bmp“ kao stegomedijum i ovim je dokazano da *.bmp* format, iako veći, nudi dobru mogućnost za sakrivanje tajne poruke. Detektorom „StegAlyzerSS“ je uspešno detektovano postojanje tajne poruke u fajlu „Vodeni ljliljani.bmp“. Nedostatak ovog detektora jeste taj što, iako po specifikaciji detektuje potpis programa wbStego4, ovaj korak nije uspešno sproveden. Konsultacijom sa osobom iz Centra za analizu i istraživanje u Sarc-u, izvršeno je ponovno testiranje StegAlyzerSS-a, nakon čega su

utvrdili da ovaj program ne može da detektuje potpis wbStego4 softvera i on samo detektuje tekstualne fajlove u okviru slike kada je steganografija primenjena pomoću programa wbStego4. Primenom ovog softvera je, i pored njihove tvrdnje, detektovan slikovni format sakriven u slikovnom nosiocu, kao i potencijalni stegonosioc, ali zbog nedostataka informacija o tome koji je steganografski program korišćen, nije moguće izvući tajnu poruku iz fajla „Vodeni ljliljani.bmp“.

U **II studiji slučaja** detektovan je fajl „Vodeni ljliljani.jpg“ kao stegomedijum i pored toga je detektovan potpis korišćenog steganografskog programa Camouflage v.1.2.1. StegAlyzerSS je i u ovoj studiji slučaja pokazao nedostatak: iako je detektovao kojim steganografskim programom je sakrivena tajna poruka, nije moguće dalje procesuirati detektovani fajl, jer algoritam za izvlačenje tajne poruke nije kreiran. Daljim istraživanjem se došlo do uvida u to koja je sintaksa potpisa ovog programa, kao i na koji način se može promeniti šifra koja štiti izvlačenje tajne poruke bez posedovanja originalnog stegonosioca. Ovaj postupak je uspešno primenjen, i iz fajla „Vodeni ljliljani.jpg“ je uspešno izvučena tajna poruka „Vojska1.jpg“.

7. Ukoliko forenzičaru nije dostupan stegonosioc, a nije mu poznato da li je u nekom fajlu sakrivena tajna poruka, potrebno je izvršiti više testova da bi se stekao uvid u postojanje stegomedijuma. Postoji više vrsta testova. U **I studiji slučaja** je primenjen hi-kvadrat test koji je jedan od LSB metoda. Ova statistika prvog reda, hi kvadrat test (X^2), meri vrednost suvišnih informacija i/ili deformaciju u medijumu. Ova merenja mogu doprineti prognozi poput one da li je sadržaj bio menjan ili izgleda sumnjivo. Rezultati ispitivanja su pokazala da se promene na bitovima najmanjeg značaja (LSB), gde se inače implementira tajna poruka, vrlo jasno uočavaju, te da je p-vrednost, koja pokazuje procenat prognoze zastupljenosti tajne poruke, 100% u najvećem delu grafikona.
8. Na osnovu rezultata ovog istraživanja može se zaključiti da je sakrivanje tajne poruke u .bmp formatu mnogo delotvornije i mnogo teže za detektovanje u odnosu na .jpg format. Isti postupak se može primeniti i za sakrivanje digitalnog vodenog pečata, s tom razlikom da tajna poruka nosi podatke o vlasniku i druge podatke potrebne za identifikovanje i dokazivanje vlasništva. Za ugrađivanje digitalnog vodenog pečata se ne savetuje korišćenje postojećih gotovih aplikacija dostupnih na Internetu iz razloga što su za te aplikacije dostupni alati kojima se na veoma jednostavan način vodeni pečat izvlači ili degradira, čime se otežava ili onemogućava dokazivanje prava vlasništva u slučaju spora.

5. LITERATURA

1. Anderson R., Needham R. i Shamir A., *Steganographic file system*, Proceedings of the Second International Workshop on Information Hiding (IH '98), Lecture Notes in Computer Science, vol. 1525. D. Aucsmith, ed., Portland, Oregon, April 14-17, 1998. Springer-Verlag, Berlin, Nemačka, pp. 73-82. Dostupno na: <http://www.fbi.gov/cgi-bin/outside.cgi?http://www.cl.cam.ac.uk/ftp/users/rja14/sfs3.pdf>, 1998.
2. Abbate J., *Inventing the Web*, Proc. of the IEEE, 87(11):1999–2002, 1999.
3. Arnold M., Schmucker M., and Wolthusen S. D., *Techniques and Applications of Digital Watermarking and Content Protection*. Artech House, Norwood, Massachusetts, 2003.
Dostupno na: <http://www.fbi.gov/cgi-bin/outside.cgi?http://www.warchalking.org/>.
4. Artz D., *Digital Steganography: Hiding data within data*, IEEE Internet Computing 5(3):75-80. Dostupno na: http://www.cc.gatech.edu/classes/AY2003/cs6262_fall/digital_steganography.pdf, (2001).
5. Bas P., Chassery J.-M., and Macq B., *Robust watermarking based on the warping of predefined triangular patterns*, Security and Watermarking of Multimedia Contents II, SPIE-3971:99–109, 2000.
6. Bauer, F. L. *Decrypted Secrets: Methods and Maxims of Cryptology*, 3rd ed. Springer-Verlag, New York, 2002.
7. Bloom J. A., Cox I. J., Kalker T., Linnartz J-P, Miller M. L., and Traw B., *Copy protection for DVD video*, Proc. of IEEE, 87(7):1267–1276, 1999.
8. Boneh. D. and J. Shaw, *Collusion-secure fingerprinting for digital data*, In: Proceedings of Advances in Cryptology—CRYPTO'95, volume Lecture Notes in Computer Science 963, pages 452–465, 1995.
9. Broughton R. S. and Laumeister W. C., *Interactive video method and apparatus*, United States Patent, 4,807,031, 1989.
10. Carol Carr and Patricia E. O'Neill, *Adding INSPEC to your chemical search strategy—et's get physical*, Database, 18(2):99–102, 1995.
11. Cayre F., C. Fontaine, and T. Furon, *A theoretical study of watermarking security*, Proceedings International Symposium on Information Theory (ISIT), pages 1868–1872, 2005.
12. "Classical Steganography, Cardano Grille",
Dostupno na: <http://library.thinkquest.org/27993/crypto/steg/classic1.shtml>
13. Cox J., Kilian J., Leighton F. T., Shamoon and T., *Secure spread spectrum watermarking for multimedia*. IEEE Trans. on Image Processing, 6(12):1673–1687, 1997.
14. Cox J., Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, and Ton Kalker, *Digital watermarking and steganography: Second edition*, Morgan Kaufmann Publishers, 2008.
15. Craver S., Memon N., Yeo B.L., and Yeung M. M., *Can invisible watermarks solve rightful ownerships?*, IBM Technical Report RC 20509, IBM Research, July 1996. IBM
Dostupno na : <http://www.research.ibm>
16. Curran K., *An evaluation of image based steganography methods*, International journal of digital evidence, knjiga 2., izdanje 2, 2003.
17. Curran, K. and Bailey, K., *An evaluation of image-based steganography methods*. International Journal of Digital Evidence [Online]. (Fall 2003). Dostupno na: http://www.fbi.gov/cgi-bin/outside.cgi?http://www.ijde.org/docs/03_fall_steganography.pdf.
18. Chandramouli R., *Mathematical approach to steganalysis*, In: Proceedings of the SPIE Security and Watermarking of Multimedia Contents IV, vol. 4675. International Society for Optical Engineering, San Jose, California, January 21-24, pp. 14-25. Dostupno na : <http://www.fbi.gov/cgi-bin/outside.cgi?http://www.ece.stevens-tech.edu/%7Emouli/spiesteg02.pdf>, 2002

19. Чековский, С., Овсянников В., *Скрытая утечка информации*, ЕПОС публикации : Информационная безопасность, 2002.
20. Dartmouth College, Institute for Security Technology Studies, *A Novel Software for Detection of Hidden Messages within Digital Images* [Online]. (December 29, 2003). Dostupno na : <http://www.fbi.gov/cgi-bin/outside.cgi?http://www.ists.dartmouth.edu/text/steganography.php>
21. David Kahn, *The Codebreakers—The Story of Secret Writing*, Scribner, New York, 1967.
22. David Kilburn. Dirty linen, dark secrets. *Adweek*, 1997.
23. Emil Frank Hembrooke, *Identification of sound and like signals*, United States Patent, 3,004,104, 1961.
24. Farid H., *Detecting Steganographic Messages in Digital Images*, Technical Report TR2001-412, Dartmouth College, Computer Science Department, 2001. Dostupno na : <http://www.cs.dartmouth.edu/~farid/publications/tr01.pdf>.
25. Fridrich, J. and Du, R., *Secure steganographic methods for palette images*, In: Proceedings of the 3rd Information Hiding Workshop, Lecture Notes in Computer Science, vol. 1768. Dresden, Germany, September 1999. Springer-Verlag, Berlin, Germany, 2000, pp. 47-60. Dostupno na : http://www.fbi.gov/cgi-bin/outside.cgi?http://www.ws.binghamton.edu/fridrich/Research/ihw99_paper1.dot.
26. Friedman G. L., *The trustworthy camera: Restoring credibility to the photographic image*, IEEE Trans. on Consumer Electronics, 39(4):905–910, 1993.
27. Fries B. and Fries M., *MP3 and Internet Audio Handbook*, TeamCom Books, Burtonsville, Maryland, 2000.
28. Hartung F. and Girod B., *Watermarking of uncompressed and compressed video*. *Signal Processing*, 66(3):283–301, 1998.
29. “*Hidden in Plain Sight-Steganography*”, Counterintelligence News and Developments, Izdanje 2, Jun 1998. Dostupno na: www.nacic.gov/pubs/news/1998/jun98.htm
30. Home and Garden Television, “*Clues in the Quilts*”. Dostupno na: http://www.hgtv.com/HGTV/project/0,1158,CRHO_project_7305.00.html
31. Jackson J. T., Gregg H., Gunsch G. H., Claypoole R. L., and Lamont G. B., *Blind Steganography detection using a computational immune system: A work in progress*, International Journal of Digital Evidence [Online], (Winter 2003) (December 21, 2003). Dostupno na: http://www.fbi.gov/cgibin/outside.cgi?http://www.ijde.org/docs/02_winter_art4.pdf
32. James M. Barton, *Method and apparatus for embedding authentication information within digital data*, United States Patent, 5,646,997, 1997.
33. Johnson, N. F. and Jajodia, S., *Exploring steganography: Seeing the unseen*, Computer (1998A) 31(2):26-34. Dostupno na : <http://www.fbi.gov/cgibin/outside.cgi?http://www.jjtc.com/pub/r2026.pdf>.
34. Johnson, N. F., Duric, Z. and Jajodia, S., *Information Hiding: Steganography and Watermarking: Attacks and Countermeasures*, Kluwer Academic, Norwell, Massachusetts, 2001
35. Kahn D., *Codebreakers: The Story of Secret Writing*, Revised ed., Scribner, New York, 1996.
36. Kolata Gina, “*A Mystery Unraveled, Twice*”, Dostupno na: <http://www.cryptome.unicast.org/cryptome022401/tri.crack.htm>
37. Macq B. M. and J-J. Quisquater, *Cryptology for digital TV broadcasting*, Proc. of the IEEE, 83(6):944–957, 1995.
38. moreCrayons, *color cube* [Online]. (December 12, 2003). Dostupno na: <http://www.fbi.gov/cgibin/outside.cgi?http://www.morecrayons.com/palettes/webSmart/colorcube.php>.

39. Oostveen J., Kalker T., and Haitisma J., *Feature extraction and a database strategy for video fingerprinting*, In *5th Int. Conf. on Visual Information Systems*, volume LNCS 2314, pages 117–128. Springer-Verlag, 2002.
40. Peron CSJ, Legary M., *Digital anti-forensics: emerging trends in data transformation techniques*,
Dostupno na: <http://www.seccuris.com/documents/papers/Seccuris-Antiforensics.pdf>.
41. Petitcolas Fabien A. P., “*History of Steganography*”,
Dostupno na: www.cl.cam.ac.uk/~fapp2/steganography/history.html
42. Ray Dolby, *Apparatus and method for the identification of specially encoded FM stereophonic broadcasts*, United States Patent, 4,281,217, 1981.
43. Rogers M., *Anti-forensics*, 2005.
Dostupno na: <http://www.cyberforensics.purdue.edu/docs/Lockheed.ppt> ;
44. Seward J., *Debtor's digital reckonings*, International Journal of Digital Evidence, Fall 2003 [Online]. (Januar 3, 2004). Dostupno na :
http://www.fbi.gov/cgi-bin/outside.cgi?http://www.ijde.org/docs/03_fall_seward.pdf.
45. Simmons, G.J., *The Prisoner's Problem and the Subliminal Chanel*, In: Proceedings of CRYPTO `83, 1984.
46. Simpson J. and Weiner E., editors. *Oxford English Dictionary*. Oxford University Press, 2000.
47. Singh Simon, “*The Cipher of Mary Queen of Scots*” ,
Dostupno na: www.arch.columbia.edu/DDL/cad/A4513/S2001/r9/
48. “*The Science of Secrecy, Steganography*”.
Dostupno na : <http://www.channel4.com/plus/secrecy/page1b.html>
49. Tirkel, A., Rankin, G., Schyndel, R., Ho, W., Mee, N., & Osborne, C., 1993. *Electronic watermark*. Proceedings of Digital Image Computing, Technology and Applications, DICTA 93, (pp. 666-673).
50. Trithemius Johannes, “*Steganographia: hoe est ars per occultam scripturam animi sui voluntatem absentibus aperiendi certa*”.
Dostupno na: <http://www.esotericarchives.com/tritheim/stegano.htm>
51. Wayner P., *Disappearing Cryptography: Information Hiding: Steganography & Watermarking 2nd. ed.*, Morgan Kaufmann, San Francisco, California, 2002.
52. William M. Tomberlin, Louis G. MacKenzie, and Paul K. Bennett, *System for transmitting and receiving coded entertainment programs*, United States Patent, 2,630,525, 1953.
<http://www.digitalwatermarkingalliance.org/news.asp>
53. <http://www.drmwatch.com/drmtech/article.php/3587141>
54. http://www.en.wikipedia.org/wiki/Nazca_Lines
55. <http://www.evidence-eliminator.com>
56. http://www.fbi.gov/hq/lab/fsc/backissu/july2004/research/2004_03_research01.htm
- 57.