

Kandidat:

mr.sci Damir Omerašević, dipl.ing.el.

Radni naslov teme projekta/disertacije:

Novi pristup kombinovanju kriptografije i steganografije za tajnu razmjenu poruka

I. OBRAZLOŽENJE TEME PROJEKTA/DISERTACIJE

U uvodnom dijelu ću ukratko opisati istoriju kriptografije i steganografije, te napraviti podjelu kriptografije i sakrivanja informacija. Na kraju uvodnog dijela ću ukratko opisati domen predloženog projekta/disertacije. Nakon uvodnog dijela slijedi pregled stanja u oblasti istraživanja i pregled tehnika baziranih na kriptografiji, steganografiji i kombinaciji kriptografije i steganografije. Detalji istraživanja dati su u motivaciji za istraživanje, ciljevima i planu istraživanja, te metodologiji istraživanja. Na kraju, predstavljeni su očekivani izvorni naučni doprinos projekta/disertacije, te polazna literatura.

A. Istorija kriptografije i steganografije

1) *Istorija kriptografije:* Kriptografija je nastala praktično od momenta od kada je čovjek počeo da komunicira putem razmjene pisanih poruka, jer je postojala i potreba da se zadrži privatnost razmijenjenih informacija. Primjena kriptografije, gledano sa istorijskog aspekta, uglavnom je bila vezana za političke i vojne svrhe. Smatra se da je najstariji poznati tekst koji sadrži jednu od bitnih komponenti kriptografije, izmjenu teksta, nastao prije skoro 4000 godina, u egipatskoj provinciji Menet Khufu [1], na nagrobnom natpisu plemića Khnumhotepa II (prikazan na Slici 1) u mjestu Beni Hassan [2].



Slika 1. Khnumhotep II [2]

Hijeroglifski natpisi sa grobnice Khnumhotepa II prikazani su na Slici 2. Prevodi posljednjih dvadeset vertikalnih natpisa otkrivaju da su neki rijetki hijeroglifski simboli korišteni umjesto običnih, uz nedosljednosti gramatičke sintakse. Neki egiptolozi vjeruju da su posebni odlomci iz nadgrobnog natpisa Khnumhotepa II namjerno transformisani kako bi se sakrilo izvorno značenje nadgrobnog natpisa [2][3].



Slika 2. Hijeroglifski natpis na grobnici Khnumhotepa II [2]

U petom vijeku prije nove ere Spartanci, ratničko društvo poznato po svojoj hrabrosti i vještini u borbi, razvili su kriptografski uređaj za slanje i primanje tajnih poruka. Ovaj uređaj, cilindar zvani skitala (eng. Scytale) [4], prikazan na Slici 3, bio je u posjedu pošiljaoca i primaoca poruke.



Slika 3. Skitala [4]

Za pripremu poruke, uski pojas (traka) pergamenta ili kože bio je omotan oko skitala i poruka je napisana preko njega. Nakon odmotavanja i prilikom prenošenja do primaoca poruke, traka prikazuje samo niz besmislenih slova, sve dok se ponovno ne namota na skitalu potpuno jednakog prečnika. Ovo je bio prvi oblik transpozicijske šifre, jer su slova ostala ista, ali se redoslijed promijenio. Ova tehnika je predstavljala osnovu za tehnike transpozicijskih šifri koje su nastale mnogo kasnije, zahvaljujući razvoju tehnike i tehnologije.

2) *Istorija steganografije*: Cjelokupna istorija steganografije može se pronaći u literaturi [1][5][6][7][8].

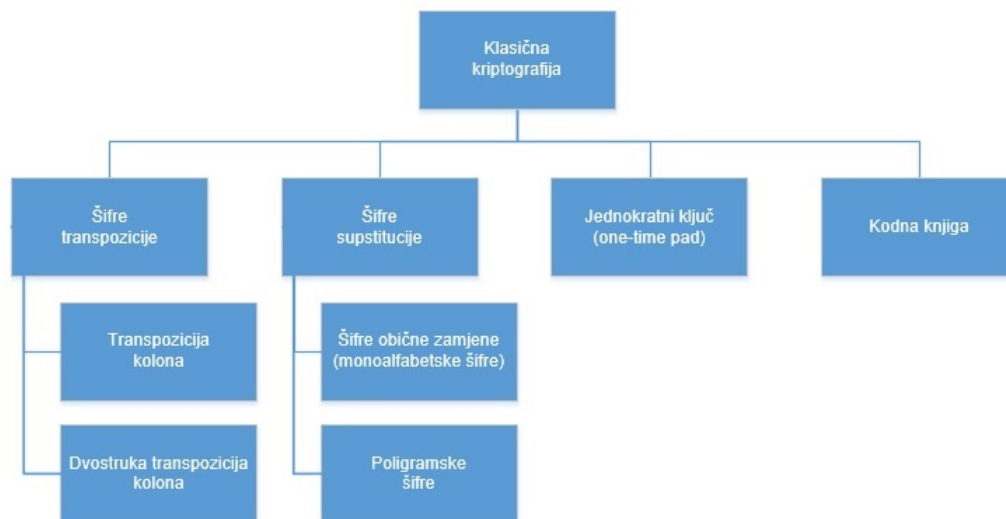
Smatra se da je najstarija steganografska poruka nastala u petom vijeku prije nove ere u Grčkoj, kada je Histaiacus naredio da se obrije glava jednog od robova, a nakon toga tetovirana mu je poruka na glavi. Nakon što je kosa ponovno narasla, Histaiacus je poslao roba sa tetoviranom porukom Aristagorasu iz Mileta. Poruka je poticala Aristagorasa na pobunu protiv kralja Perzije [9].

B. Podjela kriptografije

Kriptografiju, prema [10], dijelimo na:

- klasičnu, gdje se šifrovanje i dešifrovanje izračunavalo ručno i
- modernu, gdje računari šifruju i dešifruju poruke, prema istim principima kao i kod klasične kriptografije, ali šifrovanje može biti puno kompleksnije.

1) *Klasična kriptografija*: Podjela klasične kriptografije prikazana je na Slici 4.



Slika 4. Podjela klasične kriptografije

Šifre transpozicije premještaju znakove prema pravilu transpozicije, a rezultat je šifrovana poruka. U ovakvoj šifrovanoj poruci znakovi iz izvorne poruke mijenjaju raspored [11]. Koriste se transpozicije kolona i dvostruke transpozicije kolona.

Šifre supstitucije ili zamjene, za razliku od šifri transpozicije, znakovima iz izvorne poruke ne mijenjaju raspored, ali mijenjaju njihovu vrijednost, odnosno preslikavaju se u druge znakove [12]. U ovisnosti da

li se mijenja jedan znak ili grupa znakova istovremeno, sa nekim drugim znakom ili grupom znakova, postoje šifre obične zamjene i poligramske šifre. Koncept poligramske šifre koristi se u blokovskim šiframa moderne kriptografije.

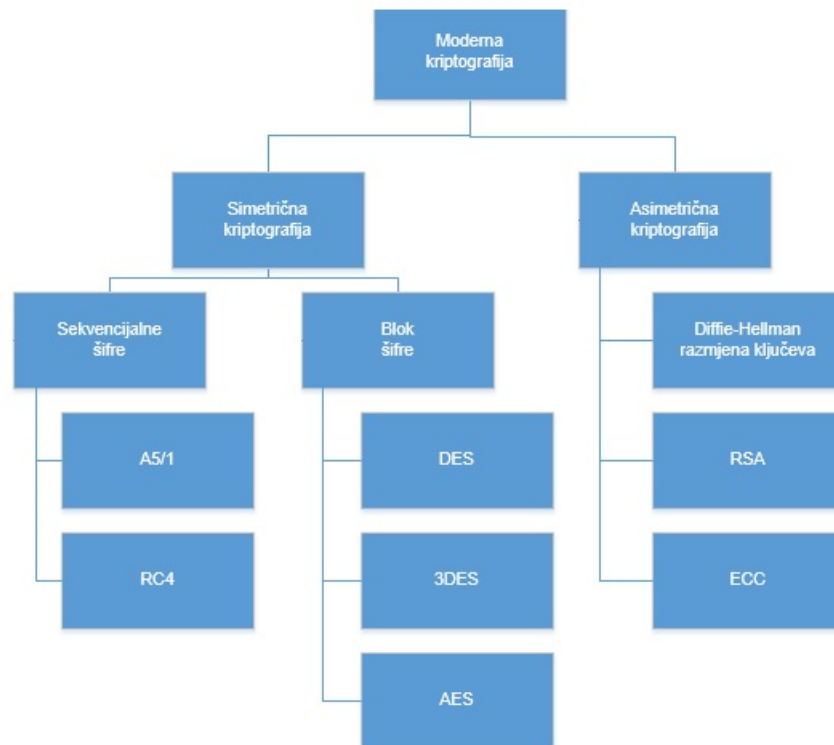
Jednokratni ključ (eng. One Time Pad - OTP) predstavlja jednu verziju simetrične kriptografije, za koju je dokazano da ima perfektu sigurnost [13]. Perfektna sigurnost [14] podrazumijeva apsolutnu sigurnost u odnosu na treću stranu, koja prisluškuje komunikacioni kanal i ima na raspolaganju neograničeno vrijeme i neograničene računarske resurse za dešifrovanje šifrovane poruke.

Osnovni problem u praktičnoj primjeni za OTP predstavlja sigurno generisanje i razmjena OTP ključeva. Osim toga, OTP ključevi moraju biti potpuno slučajno generisani, što u praksi takođe predstavlja problem, te se ne smiju se ponovno koristiti.

Kodna knjiga (eng. Code Book) [15] je rječnik koji šifrue skup znakova (riječ ili frazu) sa odgovarajućom kodnom oznakom i obrnuto.

U zadnjih četrdesetak godina, zahvaljujući razvoju tehnike i tehnologije, klasična kriptografija se transformiše u modernu kriptografiju i postaje sastavni dio računarsko-komunikacione tehnologije.

2) *Moderna kriptografija*: Slika 5 prikazuje modernu kriptografiju, koju dijelimo na simetričnu i asimetričnu [16].



Slika 5. Podjela moderne kriptografije

Karakteristični predstavnici simetrične kriptografije su A5/1 i RC4.

A5/1 je sekvencijalna šifra koja se koristi za privatnost komunikacija u globalnom sistemu za mobilne komunikacije (eng. Global System for Mobile Communications - GSM), u Evropi i Sjedinjenim Američkim Državama. A5/1 sekvencijalna šifra ima mnogo sigurnosnih propusta [17].

Navodna RC4 [18] implementacija sekvencijalne šifre anonimno je postavljena 13.09.1994 godine, na internetskoj newsgroup-i sci.crypt, bez dozvole ili verifikacije autora Ron Rivesta [19][20]. Ime RC4 je [18] zaštićeno, tako da se RC4 veoma često naziva ARC4 ili ARCFOUR [18], da bi se izbjegli eventualni problemi sa autorskim pravima. Ovdje istovremeno koristim nazive RC4 i (A)RC4.

RC4 se koristi se u SSL (eng. Secure Socket Layers - SSL) [21] i WEP (eng. Wired Equivalent Privacy

- WEP) [22] protokolima, a ima sigurnosne propuste prilikom rasporeda ključeva (eng. key scheduling) [23].

Osnovni problemi simetrične kriptografije su distribucija ključeva i zamjena postojećih ključeva novim ključevima. Navedene probleme simetrične kriptografije rješava asimetrična kriptografija.

Simetrična kriptografija koristi jedan (simetrični, odnosno isti) ključ, a kod asimetrične kriptografije postoje dva različita ključa (tajni i javni), a samo korisnik koji ima odgovarajući tajni ključ može dešifrovati poruku koja je šifrovana javnim ključem.

Međutim, kada je sigurnu komunikaciju potrebno uspostaviti između određene grupe korisnika (N), javlja se problem upravljanja tajnim ključevima, jer bi svaki učesnik morao čuvati N-1 ključeva. Taj problem je moguće riješiti uspostavljanjem centra za raspodjelu ključeva (eng. Key Distribution Center - KDC). KDC predstavlja pouzdani server kojem svi učesnici vjeruju i koji je zaštićen od vanjskih opasnosti.

Matematički je praktično nemoguće odrediti tajni ključ ukoliko se poznaje javni, jer se u asimetričnoj kriptografiji primjenjuju funkcije čije se inverzne funkcije veoma teško mogu izračunati, na primjer:

- 1) logaritam po modulu nekog velikog cijelog broja,
- 2) pronalaženje prostih faktora velikih cijelih brojeva.

Karakteristični predstavnici asimetrične kriptografije su:

- standard enkripcije podataka (eng. Data Encryption Standard - DES),
- standard trostruke enkripcije podataka (eng. Triple Data Encryption Standard - 3DES),
- standard napredne enkripcije (eng. Advanced Encryption Standard - AES).

DES [24][25] je metoda simetričnog šifrovanja podataka razvijena od strane današnjeg američkog Nacionalnog instituta za standarde i tehnologiju (eng. National Institute of Standards and Technology - NIST), koji je bio izabran u američki federalni standard za obradu informacija (eng. Federal Information Processing Standard - FIPS) 1976. godine. DES je nastao kao potreba raznih državnih tijela za šifrovanje dokumenata i komunikacija koji se ne smatraju državnom ili vojnom tajnom, ali koji ne bi smjeli biti dostupni široj javnosti.

DES radi na principu upotrebe nizova znakova fiksne dužine od bitova običnog teksta, te ih kroz mnogo komplikovanih operacija (rundi) pretvara u bitni niz znakova šifrovanog teksta jednake dužine. U ovom slučaju to je 64 bita, gdje se 56 bita koristi u samom algoritmu dok ostalih 8 bita služi za provjeru parnosti, a kasnije budu odbačeni.

1998. godine, Electronic Frontier Foundation (EFF) izgradila je uređaj za dešifrovanje DES-a (eng. DES Cracker), čije su detaljne specifikacije dostupne na [26], i to za manje od 250.000 američkih dolara. Ovaj uređaj je dekodirao DES poruke za manje od sedam dana [27].

U [28] su se prvi puta prikazala nedokumentovana pravila dizajna DES algoritma i objašnjen je način probijanja DES-a koji ima maksimalno 8 rundi, i to samo u nekoliko minuta, na personalnom računaru. Kasniji radovi [29][30] prikazuju efikasnije načine probijanja DES šifre koja ima punih 16 rundi.

Danas se smatra kako je DES nesiguran za mnoge primjene, u najvećoj mjeri zbog male veličine ključeva (56-bit), što dovodi do probijanja zaštite za manje od 24 sata [31], po cijeni manjoj od 10.000 američkih dolara [32].

3DES jednostavno povećava veličinu ključa, primjenom DES algoritma tri puta uzastopno, sa tri različita ključa. Veličina ključa je sada 168 bita (3 puta po 56), čime je izbjegnuta problem dešifrovanja 3DES-a korištenjem EFF DES Cracker-a.

Nekada se vjerovalo kako se povećana sigurnost može postići korištenjem 3DES-a, ali proteklih godina skoro da je izbačen je iz upotrebe, od strane svog nasljednika AES-a (eng. Advanced Encryption Standard - AES).

AES, poznat još kao i Rijndael, a razvila su ga dva belgijska programera-matematičara Joan Daemen

i Vincent Rijmen. 2001. godine nakon 5 godina standardizacije prihvaćen je od NIST-a te predstavlja zamjenu za DES, iako je bilo i drugačijih mišljenja, kao što je opisano u [33].

Nova komparativna studija DES, 3DES i AES [34] testirala je devet različitih parametara, među kojima su dužina ključa, tip šifre (koji je bio redukantan, jer su sva tri bila simetrična), veličina bloka šifre, godina nastanka, sigurnost i prostor ključeva, kako bi se postigla efikasnost, te fleksibilnost i sigurnost. Rezultat ove studije je potvrdio da AES ima najbolje karakteristike od sva tri poređena standarda, po svim testiranim parametrima.

AES koristi ključeve veličine 128, 192 ili 256 bita, a većina kalkulacija se odvija u specijalnom konačnom polju brojeva. Radi u poljima 4×4 bajta, a svaka runda kriptiranja sastoji se od 4 koraka (dodaj-modificirani-ključ, zamjena okteta, pomicanje redova, pomicanje kolona). Od 2006. godine AES je podložen tzv. bočnim (eng. side channel) napadima. To su napadi koji nisu bazirani na propustima u algoritmu već na informacijama o fizičkoj implementaciji: trošenju električne energije, vremenima izračuna podataka, i sl..

Najčešće su napadani AES podaci s redukovanim brojem rundi kriptiranja, jer budući da AES koristi 10 rundi za 128-bitne ključeve, 12 za 192-bitne, 14 za 256-bitne, napadi se obavljaju s redukovanim brojem rundi: 7 za 128-bitne, 8 za 192-bitne i 9 za 256-bitne ključeve. Zbog toga kriptografi sumnjaju u sigurnost AES-a.

Moderne šifre koje su standardizirane, poput naprednog enkripcijskog standarda (eng. Advanced Encryption Standard - AES) ili Rivest Shamir Adleman - RSA, dobro su poznate. One nemaju slabosti koje će nekome omogućiti dešifrovanje šifrovanog teksta bez ispravnog ključa, u razumnom roku. Sve moderne šifre provode Kerckhoffov princip [35] da je sigurnost sistema u sigurnosti tajnog ključa. Zbog toga tajni ključ treba biti siguran.

Postoje dva moguća načina za napad na tajni ključ. Jedan od njih je da isprobate sve moguće vrijednosti ključa dok se ispravan ključ ne pogodi, što je napad grubom silom (eng. Brute Force). Kako bi spriječili tu vrstu napada, ključ treba biti što je moguće duži.

Drugi način za napad je pokušati se dočepati tajnog ključa. Kako bi se zaštitio tajni ključ, razvijeni su različiti protokoli za kreiranje/razmjenu (eng. Establishment) ključeva. Svi rješavaju problem kako na siguran način tajni ključ učiniti dostupnim svim parovima koje ga trebaju koristiti za šifrovanje i/ili dešifrovanje poruka.

1976. godine, kriptografija javnih ključeva postala je osnovom za sigurnu komunikaciju putem otvorenog kanala komunikacije, nakon objave rada Diffie-Hellmana (DH) 'Novi pravci u kriptografiji' [36]. Odmah nakon toga se dogodila i prekretnica između klasične ere i moderne kriptografije, kada su uvedeni RSA algoritam i DH.

Moderne kriptografije se zasniva na ideji da je ključ koji se koristi za šifrovanje vaših podataka može biti javan, a ključ koji se koristi za dešifrovanje vaših podataka mora biti privat.

RSA algoritam razvili su Rivest, Shamir i Adleman 1977. godine. Sigurnost algoritma temelji se na složenosti izračunavanja vrlo velikih prim brojeva. Do ovog trenutka algoritam se pokazao prilično sigurnim, iako mnoge stvari koje se podrazumijevaju prilikom upotrebe algoritma nisu dokazane.

Postoji nekoliko vrsta napada na RSA algoritam koji u određenim slučajevima mogu biti uspješni. Čak i napad primjenom grube sile, uz odgovarajuće resurse može dati pozitivne rezultate. Izbjegavanjem šifriranja kratkih poruka, digitalnog potpisivanja nasumičnih dokumenata, te maskiranjem kriptografskih operacija, ti napadi se mogu efikasno onemogućiti. Adekvatnim izborom dužine kriptografskih ključeva moguće je spriječiti i napade primjenom grube sile.

Da je adekvatan izbor dužine kriptografskih ključeva bitan, govori i činjenica da je NIST postavio krajnji datum zamjene 1024-bitnih sa 2048-bitnim ključevima do kraja 2013. godine [37].

Može se zaključiti da RSA algoritam i više od trideset godina nakon svoje pojave i dalje predstavlja sigurno rješenje, čija upotreba uz do sada poznate tehnike napada nije ugrožena.

Kriptografija elipsastih krivih (eng. Elliptic Curve Cryptography - ECC) je pristup kriptografije sa korištenjem javnih ključeva, koji su neovisno predložili krajem osamdesetih godina prošlog vijeka Koblitz [38] i Miller [39].

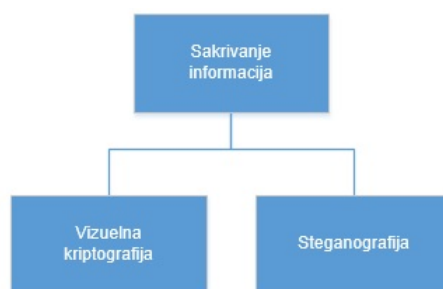
ECC je u širokoj upotrebi od 2004. godine, dok je 2006. godine ECC odobren od strane NIST.

ECC nudi veću sigurnost, uz korištenje ključa manje dužine, u poredjenju sa drugim algoritmima asimetrične kriptografije. Ako uporedimo 2048 RSA ključ (koji je trenutni industrijski standard), ECC-256 ključ je 10.000 puta teže probiti [40], dok Symantecov ECC-256 certifikat nudi ekvivalentnu sigurnost kao i 3072-bitni RSA certifikat [40].

Osim moderne kriptografije, u zadnjih dvadesetak godina intenzivno se koriste i napredne verzije tehnika sakrivanja informacija.

C. Sakrivanje informacija

Podjela sakrivanja informacija (eng. Information Hiding) prikazana je na Slici 6.



Slika 6. Podjela sakrivanja informacija

Iako je osnovna ideja u oba domena sakrivanja informacija slična, steganografija i vizuelna kriptografija koriste različite metodologije da bi zaštitile podatke.

Steganografija pokušava omogućiti sakrivanje postojanja tajne poruke koju želimo razmijeniti.

Ono što razlikuje istorijske steganografske metode od modernih je, u stvari, samo oblik nosača medija za tajnu poruku [41]. Istorijski metodi oslanjali su se na fizičku steganografiju, gdje su nosači medija bili takođe fizički, kao što je npr. ljudska koža [9].

U modernoj steganografiji, poruke se veoma često kriju unutar različitih (multi)medijskih datoteka, kao što su slike, audio ili video zapisi. Ovi tipovi datoteka imaju veću informacionu redundanciju u odnosu na obične datoteke podataka i mogu podnijeti manje promjene sa veoma malo vidljivog utjecaja kada se reprodukuju. Ova činjenica se koristi da se ugrade tajne poruke putem "nevidljivih" promjena. Različite tehnike su razvijene kako bi se bolje sakrile promjene.

Vizuelna kriptografija [42] omogućava sakrivanje informacija (tajnih poruka) u slici, i to na takav način da ljudsko biće može dešifrovati tajnu poruku bez upotrebe računara i bez bilo kakvih računanja. Jedini uslov je poznavanje, odnosno korištenje ispravnog ključa.

Kombinovanje steganografije i vizuelne kriptografije može predstavljati potencijalno veliko područje za istraživanje, naročito u forenzici [43], što je van domena predloženog projekta/disertacije.

D. Domen predloženog projekta/disertacije

Projekat/disertacija se bavi teorijskim aspektom istraživanja, uz praktičnu implementaciju dijelova predloženog pristupa, iz kripto-stego oblasti, odnosno oblasti koja predstavlja kombinaciju metoda iz kriptografije i steganografije. Osim analize postojećeg stanja u kriptografiji i steganografiji, u radu se namjerava prezentovati novi tzv. CryptoStego pristup za tajnu razmjenu poruka.

Novi CryptoStego pristup [44] predlaže metodu uspostavljanja kriptografskog ključa, na temelju skupa slika koje dijele pošiljaoc i primaoc. Osnovna ideja je da se koriste (multi)medijske datoteke za kreiranje tajnog ključa za šifrovanje.

Sa predloženim pristupom, prostor ključeva, a takođe i dužina ključa, su praktično neograničeni. Osim toga, nema potrebe za razmjenu ključeva. Ključevi se generišu iz (multi)medijskih datoteka koje imaju obje strane. Strane samo povremeno moraju izmijeniti informacije koji skup datoteka će koristiti. Ova informacija može biti dinamički ažurirana korištenjem šifrovanog kanala koji se uspostavi između strana.

Metoda je jednostavna, brza i sigurna. Moguće veličine ključa su gotovo neograničene. Predložena metoda se implementira u programskom jeziku C [45].

II. PREGLED STANJA U OBLASTI ISTRAŽIVANJA

Osnovni problemi kreiranja ključeva sa različitim vrstama prenošenja ključeva i različitim protokolima za razmjenu ključeva su dobro opisani u knjigama [46][47].

Steganografija se bavi načinima ugradnje tajne poruke na nosač medija [48]. Karakteristike nosača medija ovise o količini tajnih podataka koji se mogu sakriti, o percepciji/primjetnosti nosača medija i njegovoj jačini (eng. Robustness) [49][50][51][52][53] .

Steganografija tajnu poruku najčešće sakriva unutar digitalne slike [54][55], koja služi kao nosač slika. Za nosač sliku se koriste razni formati slika, kao što su npr. JPEG format (eng. Joint Photographic Experts Group - JPEG) [56][57], bitmape (eng. Bitmap - BMP) [57] i GIF format (eng. Graphics Interchange Format - GIF) [58][57].

Steganografske metode dijelimo na:

- Substitucijske sisteme, bazirane na kodiranju najmanje značajnih bitova (eng. Least Significant Bits - LSB),
- Transformacije domena, gdje je tajna poruka uključena u transformacijski prostor signala/poruke.

Najpopularniji steganografski substitucijski sistem je tzv. LSB kodiranje. LSB kodiranje se može koristiti na bilo kojem formatu slike, tako što se najmanje značajni biti slike nosača mijenjaju sa bitima tajne poruke.

LSB kodiranje ostavlja vidljive promjene na slici nosaču. Korištenjem genetičkog algoritma (eng. Genetic Algorithm - GA), razlike između originalne slike i stego-slike, odnosno slike sa upisanom tajnom porukom, mogu biti smanjene, ali se ne mogu potpuno ukloniti. U radu [59] opisana je kombinacija GA i PR (eng. Path Relinking - PR) metoda, koja daje bolje rezultate od GA, korištenjem substitucijskih matrica. U radu [60] je opisana ideja i dat je prijedlog kako upisati relativno kratku tajnu poruku u nosač sliku. Rad [60] bi se mogao koristiti kao osnova za kreiranje protokola za razmjenu inicijalnih ključeva, koji opisuju prostor CryptoStego (multi)medijskih datoteka.

Nova stegoanalitička metoda RS (eng. Regular Singular - RS) prepoznavanja [61] može direktno odrediti da li je stego-slika sigurna bez vizuelne inspekcije. Unapređenje RS metode opisano je zajedno sa ekperimentalnim rezultatima i objavljeno u [62].

Jsteg je prvi javno dostupan steganografski metod zasnovan na transformaciji domena, koji se koristi na JPEG formatu slika. Jsteg mijenja jedan LSB u diskretnu cosinus transformaciju (eng. Discrete Cosinus Transformation - DCT) koeficijentima sa jednim bitom tajne poruke, a danas su razvijene mnoge stegoanalitičke tehnike kojima se napada Jsteg [63][54][64][65].

Outguess [7] je takođe steganografski metod zasnovan na transformaciji domena. Outguess koristi pseudo-slučajan generator brojeva da bi na "slučajan" način odabrao odgovarajuće DCT koeficijente. Jedan LSB od "slučajno" odabranih DCT koeficijenata se mijenja sa šifrovanim bitom tajne poruke.

Steganografski sistemi bazirani na JPEG formatu nisu podložni vizualnim napadima [64], jer koriste DCT za transformaciju blokova piksela u DCT koeficijente, čime se znatno kompresuje slika, a što ne utiče na kvalitet prikazane slike, dok su sistemi bazirani na BMP i GIF formatima slika podložni vizualnim napadima, jer se kodiranje slike vrši za svaki piksel posebno.

Da bi se izbjegli vizualni napadi u BMP formatima slika, u [66] je predstavljena ideja steganografije konverzijom tajne poruke u odgovarajuću BMP sliku koja sadrži tekst tajne poruke, a nakon toga se

putem LSB zamjene BMP slika ugrađuje u jednu nosač sliku. Tajna poruka i originalna BMP slika sa tekstom može se rekonstruisati iz stego slike tokom procesa ekstrakcije podataka.

U zadnjem desetljeću postignut je značajan napredak u razvoju teoretskih osnova steganografije [67][68][69][70][71][72][73][74]. Trenutno najaktuelniji pregled steganografskih metoda od 2003. do 2013. godine objavljen je početkom decembra 2013. godine u [75].

Postoje istraživanja koliki su teoretski limiti steganografije [48] u odnosu na stepen sigurnosti koji pruža slika nosač informacije, kao što je OTP kod kriptografije. Hopper i ostali su u radu [76] prezentovali potrebne i dovoljne uslove za postojanje sigurne steganografije, bez obzira na kanal komunikacije.

Moderna steganografija teži tome da može biti otkrivena samo ukoliko se zna tajni dijeljeni ključ, što je veoma slično Kerckhoff-ovom principu u kriptografiji [35], koji kaže da sigurnost kriptografskog sistema leži u poznavanju ključa.

Kriptografija proučava matematičke tehnike koje se odnose na aspekte informacijske sigurnosti, kao što su: povjerljivost, integritet podataka, autentifikacija entiteta i porijekla podataka [46].

Istorijski pregled kriptografije može se detaljnije pronaći u [15], dok se više formalni pristup koristi u [47][77][78][79].

Pojavile su se različite ideje u vezi kombinovanja kriptografije i steganografije i postoji mnogo radova koji kombinuju kriptografiju i steganografiju [7][80][81][82][83][84], ali prema autoru dostupnim podacima, njihovo težište je uglavnom na steganografiji, gdje se koristi nosač (eng. Cover) medij.

Kombinovanjem kriptografije i steganografije dodajemo još jedan nivo sigurnosti [85] i dodatno otežavamo dešifrovanje tajnih poruka.

Novi pravci kombinovanja steganografije i kriptografije dati su u [86]. Osnovna ideja je da se tajna poruka uključi u više od jednog stego objekta koji služe kao nosači, uz korištenje nove metode statičkog parsiranja steganografije (eng. Static Parsing Steganography- SPS) [87].

SPS ideja ima dva glavna koraka:

- Više nosača slike (eng. Multiple Cover Objects - MCO), koju dijele strana pošiljaoca i primaoca, kao i tajna poruka koja se šalje, pretvaraju se u bite,
- šifriranje tajne poruke bazirane na nosačima slike, što se svodi na problem nalazenja najdužeg zajedničkog podstringa od dva stringa korištenjem generaliziranog sufiksnog drveta [88].

Kriptoanalitičar mora odrediti tri ključna elementa da bi potpuno otkrio tajnu poruku:

- Ukupan broj nosač medija koji se koristi za sakrivanje poruke,
- Sve stego-objekte koji se koriste kako bi se sakrila poruka,
- Algoritam (tajni ključ) koji se koristi da se sarije poruka u nosačima medija.

Druga ideja je da se sakrije šifrovani tekst unutar slike, korištenjem steganografije, kao što je to predloženo u [89]. Da bi se dalje stvari zakomplikovale, [90] predlaže šifrovanje izvorne poruke dva puta prije nego što se sakrije u slici. Rad [91] predlaže šifrovanje i sakrivanje u jednom koraku što smanjuje vrijeme i resurse. CryptoStego pristup je bitno drugačiji, mnogo jednostavniji i rješava drugi problem.

Ideja da se koriste različite (multi)medijske datoteke za generisanje kriptografskih ključeva takođe nije nova. Većina predloženih rješenja je generisala personalizirane ključeve, bazirane na biometrijskim osobinama, kao što su otisak prsta [92], glas [93] ili lice [94]. Detaljan pregled metoda generisanja biometrijskih ključeva i problema može se naći u [95]. Međutim, sve pomenute ideje zahtijevaju odgovarajuće vrijeme procesiranja, što produžava ukupno vrijeme šifrovanja. CryptoStego metoda posuđuje neke od ideja iz ovog područja istraživanja, ali ne predlaže trajne personalne ključeve, već jednokratne sesijske ključeve.

Najsličnija ideja predloženoj u CryptoStego prikazana je u [96]. Njihova metoda koristi osobine slike za generisanje ključeva. Proces generisanja ključeva je prilično komplikovan, što zahtijeva i duže vrijeme procesiranja. Takođe, u [96] koriste vlastiti algoritam za šifrovanje.

TABELA I
STRUKTURA PORUKE

Indeks datoteke i	Pozicija p u datoteci P_i	Biti šifrovane poruke
1 bajt	4 bajta	L - dužina u bitima

Osnovna ideja je da se koriste bitove slike direktno i da se ne izmišlja novi algoritam za šifrovanje. Slijedi opis formalnog modela CryptoStego.

A. CryptoStego - formalni model

Pošiljaoc i primaoc trebaju imati uređen skup datoteka koje su, i to svaka od njih ponaosob, mnogo veće od tajne poruke koja se razmjenjuje. Za svaku poruku koja se šifrira, pošiljaoc izabere datoteku iz skupa i poziciju unutar te datoteke. Biti (eng. bit - BInary digiT) izvorne poruke se XORuju sa bitima odabrane datoteke, od odabrane pozicije unutar odabrane datoteke, da bi se kreirala šifrovana poruka. šifrovana poruka, zajedno sa indeksom odabrane datoteke i pozicijom unutar te datoteke, šalje se primaocu. Korištenjem indeksa i pozicije, primaoc može pretvoriti šifrovani tekst u izvornu poruku XORovanjem sa bitima iste datoteke, od iste pozicije.

Formalni model ima sljedeću notaciju:

- P - uređen skup datoteka
- i - indeks datoteke
- P_i - odabrana datoteka
- p - početna pozicija u bitima u datoteci P_i
- $bP_i(k)$ - bit k u datoteci P_i
- M - izvorna poruka
- L - dužina izvorne poruke
- C - šifrovana poruka
- bM_j - bit j izvorne poruke
- bC_j - bit j šifrovane poruke

Korištenjem gornje notacije, proces šifrovanja može se opisati sa:

$for j = 1 to L$

$$bC_j = bM_j \oplus bP_i(p + j - 1)$$

Slično, dešifrovanje se može opisati sa:

$for j = 1 to L$

$$bM_j = bC_j \oplus bP_i(p + j - 1)$$

Kako poruke koje sadrže šifrovanu poruku trebaju uključiti indeks datoteke "i" i početnu poziciju "p", definisao sam format poruke, čija je struktura data u Tabeli I.

Gore opisani format poruke pretpostavlja da u skupu postoji maksimalno 256 datoteka. Pozicija je definisana sa četiri bajta, što omogućava 2^{32} , preko 4 milijarde pozicija.

Očigledno je da sigurnost predloženog metoda leži u sigurnosti skupa datoteka. Skup datoteka može se posmatrati kao glavni (eng. Master) ključ ili neka vrsta ključa za šifriranje ključa (eng. Key Encryption Key - KEK), dok biti datoteka koji se koriste da šifruju poruke imaju ulogu sesijskih (eng. session) ključeva.

Veličina glavnog ključa praktično je neograničena, budući da je broj mogućih skupova datoteka praktično neograničen.

Postoje problemi u implementaciji vezano za veličinu skupa i veličinu datoteka, što može ograničiti moguću veličinu ovoga "glavnog" ključa za konkretnu implementaciju.

III. MOTIVACIJA ZA ISTRAŽIVANJE

Kada govorimo o kriptografiji i steganografiji, postavlja se pitanje performansi, odnosno vremena i resursa potrebnih za izračunavanje ključeva, kao i trajanja procesa šifrovanja, odnosno dešifrovanja.

Bez obzira da li se radi o asimetričnoj ili simetričnoj kriptografiji, za sada ne postoji dokazana perfektna sigurnost, niti za jedan kriptografski algoritam, osim za OTP - jednokratni ključ. Međutim, u vremenu u kojem se pojavio ovaj mehanizam razmjene tajnih poruka, tehnološki nije bilo moguće organizovati, na siguran način, proces razmjene, prenošenja ili transporta ključeva [97], bez susreta subjekata koji učestvuju u komunikaciji.

IV. CILJEVI I PLAN ISTRAŽIVANJA

Osnovni cilj projekta/disertacije je baziran na analizi trenutnog stanja u oblasti istraživanja i na ličnoj motivaciji, a odnosi se na kreiranje novog CryptoStego pristupa u kombinovanju kriptografije i steganografije za tajnu razmjenu poruka.

Da bi osnovni cilj bio ostvaren, istraživanje će biti koncipirano prema sljedećem:

- 1) Analiza i detaljna izrada pregleda stanja u oblasti istraživanja.
- 2) Kreiranje CryptoStego kriptografskih ključeva i poruka, te poređenje sa (A)RC4 simetričnom šifrom. CryptoStego se poredi sa (A)RC4 stream šifrom [18], upoređujući zauzeće procesorskog vremena i memorije, od strane oba algoritma.
- 3) Mjerenje slučajnosti u raznih multimedijским datotekama dostupnim na javnim ili privatnim servisima interneta, radi korištenja odgovarajućih tipova datoteka koji su pogodni za korištenje u svrhu ekstrakcije jednokratnog ključa. Pogodni tipovi datoteka služice kao ulazni podatak u CryptoStego.
- 4) Kreiranje protokola za sigurnu razmjenu ključeva, odnosno informacija o lokacijama multimedijalnih sadržaja, radi mogućnosti povlačenja sadržaja sa javnih ili privatnih servisa na internetu i pripreme za inicijalizaciju dobivenih sadržaja, te inicijalizacija podataka potrebnih za ekstrakciju jednokratnog ključa, kao što je prethodno detaljnije opisano u Sekciji II-A.

V. METODOLOGIJA ISTRAŽIVANJA

Da bi se uradila navedena istraživanja u okviru projekta/disertacije i da bi bili u mogućnosti uporediti pojedine kriptografske algoritme sa metodama i algoritmima razvijenim u istraživanjima tokom izrade projekta/disertacije, koristi se programski jezik C [45]. Programski jezik C, odnosno verzija kompajlera za Windows operativni sistem Borland C++, izabran je zbog portabilnosti i razumijevanja napisanih algoritama [106].

Programsko okruženje MATLAB [107] se koristi za konceptualna pojašnjenja i efikasno prikazivanje pojedinih algoritama.

Za mjerenje performansi kriptografskih algoritama napisanih u programskom jeziku C, koristi se program Intel®VTune™ Amplifier XE 2011 [108]. Rezultat predloženih algoritama u projektu/disertaciji će se smatrati boljim ako je brže izvršavanje, a manje zauzeće RAM memorije.

VI. OČEKIVANI IZVORNI NAUČNI DOPRINOS PROJEKTA/DISERTACIJE

Uzimajući u obzir moja dosadadašnja istraživanja, smatram da mogu predložiti novi CryptoStego pristup, baziran na kombinaciji kriptografije i steganografije, koji može dati bolje rezultate u poređenju sa sličnim pristupima, predloženim u autoru dostupnoj postojećoj literaturi.

Na osnovu izvršene analize do sada prikupljenih naučnih radova, knjiga i drugih članaka na ovu temu (spisak je dat u literaturi) koji će poslužiti kao osnova za dalje istraživanje, napraviću prijedlog protokola za sigurnu razmjenu ključeva. Ovo planiram poslati na neku od referentnih konferencija u 2014. godini, čime bih u velikoj mjeri zaokružio istraživanje na ovom projektu/disertaciji.

Kao sekundarne doprinose ovog projekta/disertacije ističem sljedeće:

- 1) Analizu korištenja različitih tipova multimedijalnih fajlova dostupnih na javnim ili privatnim servisima interneta, koji su pogodni za svrhu ekstrakcije jednokratnog ključa.
- 2) Kreiranje Cryptostego kriptografskih ključeva i poruka.

Osim ovog doprinosa, očekuje se stvaranje preduslova za definisanje i razvijanje novih pravaca istraživanja u oblastima kriptografije i steganografije, odnosno kombinaciji kriptografije i steganografije.

POLAZNA LITERATURA

- [1] D. Kahn, *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. Scribner, December 1996.
- [2] machinae.com, "Cryptology: Khnumhotep ii," 2013. [Online]. Available: <http://www.machinae.com/crypto/khnumhotep.html>
- [3] I. G. H. Network, "Cryptography," *Global History Network, IEEE*, 2013, [Online; accessed 07.12.2013.].
- [4] Wikipedia, "Scytale," 2013. [Online]. Available: <http://en.wikipedia.org/wiki/Scytale>
- [5] N. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," *Computer, IEEE*, vol. 31, no. 2, pp. 26–34, 1998.
- [6] J. C. Judge, "Steganography: Past, Present, Future," U.S. Department of Energy, Tech. Rep., Dec. 2001. [Online]. Available: <https://e-reports-ext.llnl.gov/pdf/245799.pdf>
- [7] N. Provos and P. Honeyman, "Hide and seek: an introduction to steganography," *Security Privacy, IEEE*, vol. 1, no. 3, pp. 32–44, 2003.
- [8] J. C. Judge, "Steganography: Past, Present, Future," SANS Institute, Tech. Rep., Oct. 2003. [Online]. Available: <https://www.sans.org/reading-room/whitepapers/steganography/steganography-past-present-future-552>
- [9] P. Moulin and R. Koetter, "Data-hiding codes," *Proceedings of the IEEE*, vol. 93, no. 12, pp. 2083–2126, 2005.
- [10] D. Y. Lu, "Introduction to security," 2013, course CSCE 455/855: Distributed Operating Systems. [Online]. Available: cse.unl.edu/~ylu/csce855/notes/crypto_pres.ppt
- [11] S. Hasinoff, "Solving substitution ciphers," 2003. [Online]. Available: <http://people.csail.mit.edu/hasinoff/pubs/hasinoff-quipster-2003.pdf>
- [12] T. Jakobsen, "A fast method for the cryptanalysis of substitution ciphers," *Cryptologia*, vol. 19, pp. 265–274, 1995.
- [13] T. Tantau, "The one-time pad algorithm - the simplest and most secure way to keep secrets," in *Algorithms Unplugged*, B. Vöcking, H. Alt, M. Dietzfelbinger, R. Reischuk, C. Scheideler, H. Vollmer, and D. Wagner, Eds. Springer, 2011, pp. 141–146. [Online]. Available: <http://dblp.uni-trier.de/db/books/collections/Voecking2011.html#Tantau11>
- [14] C. E. Shannon and W. Weaver, *A Mathematical Theory of Communication*. Champaign, IL, USA: University of Illinois Press, 1963.
- [15] S. Singh, *The Code Book: The Evolution of Secrecy from Mary, Queen of Scots, to Quantum Cryptography*, 1st ed. New York, NY, USA: Doubleday, 1999.
- [16] J. Katz and Y. Lindell, *Introduction to Modern Cryptography (Chapman & Hall/Crc Cryptography and Network Security Series)*. Chapman & Hall/CRC, 2007.
- [17] A. Biryukov, A. Shamir, and D. Wagner, "Real time cryptanalysis of a5/1 on a pc," in *Fast Software Encryption*, ser. Lecture Notes in Computer Science, G. Goos, J. Hartmanis, J. Leeuwen, and B. Schneier, Eds. Springer Berlin Heidelberg, 2001, vol. 1978, pp. 1–18, [Online; accessed 12.12.2013. Alternative url: <http://cryptome.org/a51-bsw.htm>]. [Online]. Available: http://link.springer.com/content/pdf/10.1007%2F3-540-44706-7_1.pdf
- [18] Wikipedia, "Rc4," 2013, [Online; accessed 11.4.2013.]. [Online]. Available: <http://en.wikipedia.org/wiki/Rc4>
- [19] D. Sterndark, "Rc4 algorithm revealed," 1994, [Online; accessed 11.4.2013.]. [Online]. Available: <https://groups.google.com/group/sci.crypt/msg/10a300c9d21afca0>
- [20] R. J. J. Jenkins, "Isaac and rc4," 1996, [Online; accessed 11.4.2013.]. [Online]. Available: <http://burtleburtle.net/bob/rand/isaac.html>
- [21] S. A. Thomas, *SSL and TLS Essentials: Securing the Web with CD-ROM*. New York, NY, USA: John Wiley & Sons, Inc., 2000.
- [22] A. H. Lashkari, F. Towhidi, and R. S. Hosseini, "Wired equivalent privacy (wep)," in *Proceedings of the 2009 International Conference on Future Computer and Communication*, ser. ICFCC '09. Washington, DC, USA: IEEE Computer Society, 2009, pp. 492–495. [Online]. Available: <http://dx.doi.org/10.1109/ICFCC.2009.32>
- [23] S. R. Fluhrer, I. Mantin, and A. Shamir, "Weaknesses in the key scheduling algorithm of rc4," in *Revised Papers from the 8th Annual International Workshop on Selected Areas in Cryptography*, ser. SAC '01. London, UK, UK: Springer-Verlag, 2001, pp. 1–24. [Online]. Available: <http://dl.acm.org/citation.cfm?id=646557.694759>
- [24] National Institute of Standards and Technology, *FIPS PUB 46-3: Data Encryption Standard (DES)*. pub-NIST:adr: pub-NIST, Oct. 1999, supersedes FIPS 46-2. [Online]. Available: <http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf>
- [25] N. I. of Standards and Technology, "Data encryption standard," in *In FIPS PUB 46, Federal Information Processing Standards Publication*, 1977, pp. 46–2.
- [26] E. F. Foundation, *Cracking DES: Secrets of Encryption Research, Wiretap Politics and Chip Design*, M. Loukides and J. Gilmore, Eds. Sebastopol, CA, USA: O'Reilly & Associates, Inc., 1998, [Online; accessed 12.12.2013.]. [Online]. Available: http://w2.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/HTML/19980716_eff_des_faq.html#howsitwork
- [27] C. Paar and J. Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer-Verlag New York Inc, 2010.
- [28] E. Biham and A. Shamir, "Differential cryptanalysis of des-like cryptosystems," in *Proceedings of the 10th Annual International Cryptology Conference on Advances in Cryptology*, ser. CRYPTO '90. London, UK, UK: Springer-Verlag, 1991, pp. 2–21. [Online]. Available: <http://dl.acm.org/citation.cfm?id=646755.705229>
- [29] D. Coppersmith, "The data encryption standard (des) and its strength against attacks," *IBM J. Res. Dev.*, vol. 38, no. 3, pp. 243–250, May 1994. [Online]. Available: <http://dx.doi.org/10.1147/rd.383.0243>

- [30] E. Biham and A. Shamir, "Differential cryptanalysis of the full 16-round des," in *Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology*, ser. CRYPTO '92. London, UK, UK: Springer-Verlag, 1993, pp. 487–496. [Online]. Available: <http://dl.acm.org/citation.cfm?id=646757.705534>
- [31] S. GmbH, "Break des in less than a single day," 2008. [Online]. Available: <http://www.sciengines.com/company/news-events/74-des-in-1-day.html?eab1dd0ce8f296f6302f76f8761818c0=0b59c5b91984fe01986ef3bbc6de9871>
- [32] S. Kumar, C. Paar, J. Pelzl, G. Pfeiffer, A. Rupp, and M. Schimmler, "How to break des for 8,980," in *International Workshop on Special-Purpose Hardware for Attacking Cryptographic Systems — SHARCS'06, Cologne, Germany, 2006*. [Online]. Available: <http://www.sharcs.org>
- [33] H. Rehman, S. Jamshed, and A. ul Haq, "Why triple des with 128-bit key and not rijndael should be aes," in *Students Conference, 2002. ISCON '02. Proceedings. IEEE*, vol. 2, 2002, pp. 12–13.
- [34] H. O. Alanazi, B. B. Zaidan, A. A. Zaidan, H. A. Jalab, M. Shabbir, and Y. Al-Nabhani, "New comparative study between des, 3des and aes within nine factors," *CoRR*, vol. abs/1003.4085, 2010. [Online]. Available: <http://arxiv.org/pdf/1003.4085v1>
- [35] A. Kerckhoffs, "La cryptographie militaire - Partie I," *Journal des sciences militaires*, vol. IX, pp. 5–83, Jan 1883.
- [36] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theor.*, vol. 22, no. 6, pp. 644–654, Sep. 2006. [Online]. Available: <http://dx.doi.org/10.1109/TIT.1976.1055638>
- [37] E. B. Barker and A. L. Roginsky, "Sp 800-131a. transitions: Recommendation for transitioning the use of cryptographic algorithms and key lengths," NIST, Gaithersburg, MD, United States, Tech. Rep., 2011. [Online]. Available: <http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf>
- [38] N. Kobitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, Jan. 1987.
- [39] V. S. Miller, "Use of elliptic curves in cryptography," in *Lecture Notes in Computer Sciences; 218 on Advances in cryptography—CRYPTO 85*. New York, NY, USA: Springer-Verlag New York, Inc., 1986, pp. 417–426. [Online]. Available: <http://dl.acm.org/citation.cfm?id=18262.25413>
- [40] B. Rowland, "Introducing algorithm agility: Ecc and dsa," Nov. 2013. [Online]. Available: <http://www.symantec.com/connect/blogs/introducing-algorithm-agility>
- [41] N. S. Group, "History and evolution of steganography," 2013, stegano.net. [Online]. Available: <http://stegano.net/tutorial/steg-history.html>
- [42] M. Naor and A. Shamir, "Visual cryptography," in *EUROCRYPT*, ser. Lecture Notes in Computer Science, A. D. Santis, Ed., vol. 950. Springer, 1994, pp. 1–12. [Online]. Available: <http://dblp.uni-trier.de/db/conf/eurocrypt/eurocrypt94.html#NaorS94>
- [43] A. Nandakumar, P. Harmya, N. Jagadeesh, and S. Anju, "A secure data hiding scheme based on combined steganography and visual cryptography methods," in *Advances in Computing and Communications*, ser. Communications in Computer and Information Science, A. Abraham, J. Lloret Mauri, J. Buford, J. Suzuki, and S. Thampi, Eds. Springer Berlin Heidelberg, 2011, vol. 191, pp. 498–505. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-22714-1_51
- [44] D. Omerasevic, N. Behlilovic, and S. Mrdovic, "Cryptostego - a novel approach for creating cryptographic keys and messages," in *Systems, Signals and Image Processing (IWSSIP), 2013 20th International Conference on*, 2013, pp. 83–86.
- [45] D. M. Ritchie, "The c programming language," 1988.
- [46] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. CRC Press, Oct. 1996, vol. 19964964. [Online]. Available: <http://dx.doi.org/10.1201/9781439821916>
- [47] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition*, 2nd ed. Wiley, Oct. 1996.
- [48] R. Anderson and F. Petitcolas, "On the limits of steganography," *IEEE Journal of Selected Areas in Communications*, vol. 16, pp. 474–481, 1998.
- [49] M. M. Amin, M. Salleh, S. Ibrahim, M. R. Katmin, and M. Z. I. Shamsuddin, "Information hiding using steganography," in *Telecommunication Technology, 2003. NCTT 2003 Proceedings. 4th National Conference on*, 2003, pp. 21–25.
- [50] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," *Computer*, vol. 31, no. 2, pp. 26–34, Feb. 1998. [Online]. Available: <http://dx.doi.org/10.1109/MC.1998.10029>
- [51] G. Sahoo and R. K. Tiwari, "Some new methodologies for secured data coding and transmission," *International Journal of Electronic Security and Digital Forensics*, vol. 3, no. 2, pp. 120–137, 2010-06-30T00:00:00. [Online]. Available: <http://www.ingentaconnect.com/content/ind/jesdf/2010/00000003/00000002/art00003>
- [52] L. Marvel, C. Retter, and J. Boncelet, C.G., "A methodology for data hiding using images," in *Military Communications Conference, 1998. MILCOM 98. Proceedings., IEEE*, vol. 3, 1998, pp. 1044–1047 vol.3.
- [53] C. Cachin, "An information-theoretic model for steganography," in *Information Hiding*, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 1998, vol. 1525, pp. 306–318. [Online]. Available: http://dx.doi.org/10.1007/3-540-49380-8_21
- [54] J. Fridrich and M. Goljan, "Practical steganalysis of digital images - state of the art," in *In Proceedings of SPIE*, 2002, pp. 1–13.
- [55] H. Wang and S. Wang, "Cyber warfare: Steganography vs. steganalysis," *Commun. ACM*, vol. 47, no. 10, pp. 76–82, Oct. 2004. [Online]. Available: <http://doi.acm.org/10.1145/1022594.1022597>
- [56] G. K. Wallace, "The jpeg still picture compression standard," *Communications of the ACM*, pp. 30–44, 1991.
- [57] J. Miano, *Compressed Image File Formats: JPEG, PNG, GIF, XBM, BMP*, ser. ACM Press Series. Addison Wesley, 1999. [Online]. Available: http://books.google.ba/books?id=_nJLvY757dQC

- [58] C. Incorporated, "Gif graphics interchange format: A standard defining a mechanism for the storage and transmission of bitmap-based graphics information," Columbus, OH, USA, 1987.
- [59] A. Brazil, A. Sanchez, A. Conci, and N. Behlilovic, "Hybridizing genetic algorithms and path relinking for steganography," in *ELMAR, 2011 Proceedings*, 2011, pp. 285–288.
- [60] A. Sanchez, A. Conci, E. Zeljkovic, N. Behlilovic, and V. Karahodzic, "A new approach to relatively short message steganography," in *Telecommunications (BIHTEL), 2012 IX International Symposium on*, 2012, pp. 1–4.
- [61] J. Fridrich, M. Goljan, and R. Du, "Reliable detection of lsb steganography in color and grayscale images," *IEEE Multimedia*, vol. 8, pp. 22–28, 2001.
- [62] X. Luo, B. Liu, and F. Liu, "Improved rs method for detection of lsb steganography," in *Computational Science and Its Applications – ICCSA 2005*, ser. Lecture Notes in Computer Science, O. Gervasi, M. Gavrilova, V. Kumar, A. LaganÃ, H. Lee, Y. Mun, D. Taniar, and C. Tan, Eds. Springer Berlin Heidelberg, 2005, vol. 3481, pp. 508–516. [Online]. Available: http://dx.doi.org/10.1007/11424826_54
- [63] T. Zhang and X. Ping, "A fast and effective steganalytic technique against jsteg-like algorithms," in *Proc. 8th ACM Symp. Applied Computing*. ACM Press, 2003, pp. 307–311.
- [64] A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems - breaking the steganographic utilities ezstego," in *Jsteg, Steganos, and S-Tools - and Some Lessons Learned*, ser. Lecture Notes in Computer Science. Springer-Verlag, 2000, pp. 61–75.
- [65] X. Yu, Y. Wang, and T. Tan, "On estimation of secret message length in jsteg-like steganography," *Pattern Recognition, International Conference on*, vol. 4, pp. 673–676, 2004.
- [66] A. Asif, S. Hannan, R. Manza, and R. J. Ramteke, "Conversion of bitmap text images for data hiding," in *Computational Intelligence and Computing Research (ICCIC), 2010 IEEE International Conference on*, 2010, pp. 1–4.
- [67] M. Backes and C. Cachin, "Public-key steganography with active attacks," *IACR Cryptology ePrint Archive*, vol. 2003, p. 231, 2003. [Online]. Available: <http://dblp.uni-trier.de/db/journals/iacr/iacr2003.html#BackesC03>
- [68] C. Hundt, M. Liskiewicz, and U. WÃlfel, "Provably secure steganography and the complexity of sampling," in *ISAAC*, ser. Lecture Notes in Computer Science, T. Asano, Ed., vol. 4288. Springer, 2006, pp. 754–763. [Online]. Available: <http://dblp.uni-trier.de/db/conf/isaac/isaac2006.html#HundtLW06>
- [69] T. V. Le and K. Kurosawa, "Bandwidth optimal steganography secure against adaptive chosen stegotext attacks," in *Information Hiding*, ser. Lecture Notes in Computer Science, J. Camenisch, C. S. Collberg, N. F. J. 0001, and P. Sallee, Eds., vol. 4437. Springer, 2006, pp. 297–313. [Online]. Available: <http://dblp.uni-trier.de/db/conf/ih/ih2006.html#LeK06>
- [70] N. Dedic, G. Itkis, L. Reyzin, and S. Russell, "Upper and lower bounds on black-box steganography," *CoRR*, vol. abs/0806.0837, 2008. [Online]. Available: <http://dblp.uni-trier.de/db/journals/corr/corr0806.html#abs-0806-0837>
- [71] N. Hopper, "On steganographic chosen covert security," in *Automata, Languages and Programming*, ser. Lecture Notes in Computer Science, L. Caires, G. Italiano, L. Monteiro, C. Palamidessi, and M. Yung, Eds. Springer Berlin Heidelberg, 2005, vol. 3580, pp. 311–323. [Online]. Available: http://dx.doi.org/10.1007/11523468_26
- [72] A. Lysyanskaya and M. Meyerovich, "Provably secure steganography with imperfect sampling," in *Public Key Cryptography*, ser. Lecture Notes in Computer Science, M. Yung, Y. Dodis, A. Kiayias, and T. Malkin, Eds., vol. 3958. Springer, 2006, pp. 123–139. [Online]. Available: <http://dblp.uni-trier.de/db/conf/pkc/pkc2006.html#LysyanskayaM06>
- [73] L. von Ahn and N. J. Hopper, "Public-key steganography," in *In: Advances in Cryptology – Proceedings of Eurocrypt 2004*. Springer-Verlag, 2004, pp. 323–341.
- [74] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Review: Digital image steganography: Survey and analysis of current methods," *Signal Process.*, vol. 90, no. 3, pp. 727–752, Mar. 2010. [Online]. Available: <http://dx.doi.org/10.1016/j.sigpro.2009.08.010>
- [75] S. Singh and A. Singh, "A review on the various recent steganography techniques," in *International Journal of Computer Science and Network*, December 2013, vol. 2, pp. 142–156. [Online]. Available: <http://ijcsn.org/IJCSN-2013/2-6/IJCSN-2013-2-6-152.pdf>
- [76] N. J. Hopper, J. Langford, and L. von Ahn, "Provably secure steganography," in *Advances in Cryptology: CRYPTO 2002*. Springer, 2002, pp. 77–92.
- [77] W. Mao, *Modern Cryptography: Theory and Practice*. Prentice Hall Professional Technical Reference, 2003.
- [78] D. Davies, "A brief history of cryptography," *Inf. Sec. Techn. Report*, vol. 2, no. 2, pp. 14–17, 1997. [Online]. Available: <http://dblp.uni-trier.de/db/journals/istr/istr2.html#Davies97>
- [79] A. D'Agapeyeff, *Codes and Ciphers - A History Of Cryptography*. Hesperides Press, 2008.
- [80] K. Bhowal, A. J. Pal, G. S. Tomar, and P. Sarkar, "Audio steganography using ga," *Computational Intelligence and Communication Networks, International Conference on*, pp. 449–453, 2010.
- [81] T. Sharp, "An implementation of key-based digital signal steganography," in *Proceedings of the 4th International Workshop on Information Hiding*, ser. IHW '01. London, UK, UK: Springer-Verlag, 2001, pp. 13–26.
- [82] C.-K. Chan and L.-M. Cheng, "Hiding data in images by simple lsb substitution," *Pattern Recognition*, vol. 37, no. 3, pp. 469–474, 2004. [Online]. Available: <http://dblp.uni-trier.de/db/journals/pr/pr37.html#ChanC04>
- [83] I.-C. Lin, Y.-B. Lin, and C.-M. Wang, "Hiding data in spatial domain images with distortion tolerance," *Computer Standards & Interfaces*, vol. 31, no. 2, pp. 458–464, 2009. [Online]. Available: <http://dblp.uni-trier.de/db/journals/csi/csi31.html#LinLW09>
- [84] R.-Z. Wang, C.-F. Lin, and J.-C. Lin, "Image hiding by optimal lsb substitution and genetic algorithm," *Pattern Recognition*, vol. 34, no. 3, pp. 671–683, 2001. [Online]. Available: <http://dblp.uni-trier.de/db/journals/pr/pr34.html#WangLL01>
- [85] J. Krenn, "Steganography and steganalysis," 2004. [Online]. Available: <http://www.krenn.nl/univ/cry/steg/article.pdf>

- [86] K. Challita, "Combining Steganography and Cryptography: New Directions," *International Journal of New Computer Architectures and their Applications (IJNCAA)*, vol. 1, no. 1, 2011. [Online]. Available: <http://sdiwc.net/digital-library/combining-steganography-and-cryptography-new-directions>
- [87] H. Farhat, K. Challita, and J. Zalaket, "Static parsing steganography," in *DICTAP (1)*, ser. Communications in Computer and Information Science, H. Cherifi, J. M. Zain, and E. El-Qawasmeh, Eds., vol. 166. Springer, 2011, pp. 485–492. [Online]. Available: <http://dblp.uni-trier.de/db/conf/dictap/dictap2011-1.html#FarhatCZ11>
- [88] D. Gusfield, *Algorithms on Strings, Trees, and Sequences: Computer Science and Computational Biology*. Cambridge University Press, January 1997. [Online]. Available: <http://www.amazon.ca/exec/obidos/redirect?tag=citeulike09-20&path=ASIN/0521585198>
- [89] P. Marwaha and P. Marwaha, "Visual cryptographic steganography in images," in *Computing Communication and Networking Technologies (ICCCNT), 2010 International Conference on*, 2010, pp. 1–6.
- [90] S. Usha, G. Kumar, and K. Boopathybagan, "A secure triple level encryption method using cryptography and steganography," in *Computer Science and Network Technology (ICCSNT), 2011 International Conference on*, vol. 2, 2011, pp. 1017–1020.
- [91] S. Song, J. Zhang, X. Liao, J. Du, and Q. Wen, "A novel secure communication protocol combining steganography and cryptography," *Procedia Engineering*, vol. 15, no. 0, pp. 2767 – 2772, 2011, [Online; accessed 11.4.2013.]. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S1877705811020224>
- [92] C. Soutar and G. Tomko, "Secure private key generation using a fingerprint," in *Cardtech/Securetech Conference Proceedings*, vol. 1, 1996, pp. 245–252.
- [93] F. Monrose, M. Reiter, Q. Li, and S. Wetzel, "Cryptographic key generation from voice," in *Security and Privacy, 2001. S P 2001. Proceedings. 2001 IEEE Symposium on*, 2001, pp. 202–213.
- [94] A. B. Teoh, D. C. Ngo, and A. Goh, "Personalised cryptographic key generation based on facehashing," *Computers & Security*, vol. 23, no. 7, pp. 606 – 614, 2004. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0167404804001701>
- [95] L. Ballard, S. Kamara, and M. K. Reiter, "The practical subtleties of biometric key generation," in *17th USENIX Security Symposium*, 2008.
- [96] B. Santhi, K. Ravichandran, A. Arun, and L. Chakkarapani, "A novel cryptographic key generation method using image features," *Research Journal of Information Technology*, vol. 4, no. 2, pp. 88–92, 2012.
- [97] VISA, "Visa europe data field encryption: Device and key management guidance," 2010. [Online]. Available: http://www.visaeurope.com/en/businesses__retailers/payment_security/idoc.ashx?docid=849b2be1-10b9-4bb5-8b8e-74f546777440&version=-1
- [98] S. Holzner, *Borland C++ for Windows programming (3. ed.)*, ser. Brady programming library. Brady Publishing, 1994.
- [99] MATLAB, *version 7.14.0 (R2012a)*. Natick, Massachusetts: The MathWorks Inc., 2012.
- [100] I. S. Network, *Intel VTune Amplifier XE*, 2011. [Online]. Available: <http://software.intel.com/en-us/intel-vtune/>