UNIVERSITETI I TIRANËS
FAKULTETI I EKONOMISË
DEPARTAMENTI INFORMATIKË DHE STATISTIKË E ZBATUAR
PROGRAMI BACHELOR

STEGANOGRAFIA PËR FSHEHJEN E INFORMACIONIT (IMAZHET)

Diploma: Bachelor Informatikë Ekonomike

Punoi:

Kejda Dusha

Pedagoge udhëheqëse:

Prof.Dr Besa Shahini

Tiranë, 2018

DEKLARATË

Unë e nënshkruara Kejda Dusha deklaroj që :Kjo mikrotezë përfaqëson punimin tim origjinal , përveç rasteve të citimeve dhe referencave si dhe që kjo mikrotezë nuk është përdorur më parë si mikrotezë apo projekt kursi në këtë universitet apo universitete të tjera.

Kejda Dusha
Tiranë më 27.09.2018

Falenderime

Falenderoj familjen për mbështetjen e ofruar gjatë gjithë këtyre viteve dhe Prof.Dr Besa Shahini për ndihmesën e dhënë gjatë punimit të kësaj mikroteze.

Abstrakt

Steganografia rrjedh nga fjala greke steganographic që do të thotë shkrim i fshehur/mbuluar. Ajo është shkenca e komunikimit sekret. Qëllimi i steganografisë është të fshehë ekzistencën e mesazhit nga pala e paautorizuar. Steganografia moderne e imazhit të sigurtë paraqet një detyrë të transferimit të informacionit të ngulitur/futur/fshehur në destinacion pa u zbuluar nga sulmuesi.Format e file-ve mbartëse që mund të përdoren janë të shumta, por imazhet dixhitale janë më të popullarizuara për shkak të shpeshtësisë së hasjes së tyre në internet. Për fshehjen e informacionit sekret në imazhe ekzistojnë një larmi e madhe e teknikave steganografike, disa prej të cilave janë më komplekse se të tjerët dhe të gjithë kanë pikat e tyre të forta dhe të dobëta.

Në këtë mikrotezë kam për qëllim përdorimin e teknikës më të përdorura të steganografisë së imazheve,atë LSB (Least Significant Bits) duke dhënë disa shembuj të fshehjes së informacionit. Në rastin e teknikës LSB, ideja e përgjithshme konsiston në zëvendësimin e biteve më pak të rëndësishme (least significant bit) të imazhit cover me bitet e mesazhit që do fshihet pa e dëmtuar shumë pamjen e imazhit cover (imazhit që shihet nga publiku i përgjithshëm).
Teknika LSB është ajo më e komplikuara pasi është e vështirë të diferencosh midis objektit-cover dhe objektit-stego nëse vetëm disa bite LSB të objektit cover janë zëvendësuar.Ky fakt do vihet re dhe gjatë punimit ku do paraqitet teknika LSB me zëvendësimin e numrave të ndryshëm të biteve për të parë ndikimin që sjell te imazhi.

Fjalë kyçe: Steganografi, LSB, Stego, imazh, mesazh sekret,, imazh cover, teknika

Listë tabelash dhe figurash

Përmbajtja

Kapitulli 1

Hyrje

1.1 Steganografia

Fjala steganografi rrjedh nga fjalët greke stegos dhe grafia që do të thonë përkatësisht mbulim/fshehje dhe shkrim , pra fshehje e shkrimit [1]. Steganografia është arti dhe shkenca e komunikimit sekret .Është praktika e enkodimit të informacioneve sekrete në një mënyrë të tillë që ekzistenca e informacionit të jetë e padukshme. Dokumentat origjinalë mund të quhen cover text, cover image ose cover audio. Pas futjes së mesazhit sekret ato quhen mediume-stego.Një stego-key përdoret për procesin e fshehjes /enkodimit në mënyrë që të ndalojë detektimin ose ekstraktimin e të dhënave të fshehura [2].

1.2 Steganografia dhe kriptografia

Kriptografia dhe steganografia kanë qëllime të ndryshme. Kriptografia fsheh përmbajtjen e mesazhit sekret nga një përgjues, ndersa steganografia fsheh edhe vetë ekzistencën e mesazhit.Për më tepër steganografia ofron më tepër konfidencialitet dhe siguri informacioni se kriptografia duke qenë se fokusi i tij është fshehja e vetë mesazhit. Edhe pse të dy fushat synojnë komunikimin sekret, ata kanë përkufuzime të ndryshme në termat e thyerjes së sistemit. Një sistem kriptografik konsiderohet i thyer nëse një sulmues mund të lexojë mesazhin sekret, ndërsa një sistem steganografik konsiderohet i thyer nëse një sulmues arrin ta zbulojë dhe më pas lexojë përmbajtjen e mesazhit të fshehur. Për më tepër një sistem steganografik quhet i dështuar nëse një sulmues dyshon për një skedar specifik apo metodë steganografike edhe nëse nuk e dekodon mesazhin.Për këtë arsye sistemet steganografike quhen më të ndjeshme ndaj thyerjeve se ato kriptografike. Në realitet steganografia shton shtresa të tjera sigurie, pasi kombinimi i dy metodave ofron një nivel mjaft të lartë të komunikimit privat. Si përfundim mund të themi që steganografia është një metodë plotësuese e kriptografisë dhe jo zëvendësuese e saj [13].

Kriteri/Metoda	**Steganografia**	**Kriptografia**
Bartësi	Çdo sinjal dixhital	Zakonisht bazuar në tekst,

		imazhe
Të dhëna sekrete	payload	Tekst i thjeshtë
Çelësi	opsional	I domosdoshëm
Skedari input	Të paktën dy skedarë përveç rastit të vetngulitjes	Një skedar
Objektivi	Komunikim sekret	Mbrojtje të dhënash
Rezultati	Skedar-stego	Skedar i koduar
Shqetësimi	Kapaciteti	Fuqia
Tipet e sulmeve	Steganaliza	Kriptanaliza
Dukshmëria	Asnjëherë	Gjithmonë
Dështon kur	Zbulohet	Dekodohet
Lidhja me bartësin	Jo i domosdoshëm.Mesazhi është më i rëndësishëm se bartësi	N/A
Fleksibiliteti	I lirë të përdorë çdo lloj bartësi	N/A
Historia	Shumë i lashtë përveç versionit dixhital	Shumë i lashtë përveç versionit dixhital

Tabelë 1. Krahasim midis Steganografisë dhe Kriptografisë

1.3 Rishikim literature

Termi steganografi filloi të përdorej në vitet 1500 pas shfaqjes së saj si term në librin e Trithemius mbi Steganografinë [3].

1.3.1 Steganografia dikur

Fjala steganografi do të thotë shkrim i fshehur. Origjina e saj daton që prej vitit 440 para erës sonë. Pavarësisht se termi steganografi filloi të përdorej në fund të shekullit të XV ,përdorimi i steganografisë si shkencë daton shumë më herët. Në kohët e lashta ,mesazhet fshiheshin pas tabelave të shkrimit prej dylli, në stomakun e lepujve, ose shkruheshin në kokat e skllevërve. Boja e padukshme është përdorur për shekuj me rradhë nga fëmijët dhe studentët për qejf ose për misione të fshehta nga spiunët dhe terroristët [6].

1.3.2 Steganografia sot

Shumica e sistemeve të sotme steganografike përdorin objekte të multimedias si imazhe, audio, video etj... si mjete për të fshehur mesazhet sepse shumë njerëz sot transmetojnë imazhe dixhitale përmes emaileve dhe formave të tjera të komunikimit në Internet. Steganografia moderne përdor mundësinë e fshehjes së mesazheve në file dixhitale multimediale si dhe brenda paketave të internetit[4].

Fshehja e informacionit në një medium kërkon ekzistencën e këtyre elementëve[2]:

1.Mediumin cover (C) që do fshehë mesazhin sekret.
2.Mesazhin sekret (M), që mund të jetë tekst i thjeshtë, imazh dixhital ose tip tjetër të dhënash.
3. Teknikat steganografike
4. Një stego-key (K) që mund të përdoret për të fshehur ose për të shfaqur një mesazh.
Në steganografinë moderne, bazuar në mediumin cover, steganografia mund të ndahet në pesë tipe: 1. Steganografia e tekstit
2.Steganografia e imazhit
3.Steganografia e audios
4.Steganografia e videos
5.Steganografia e protokollit

- **Steganografia e tekstit** Fshehja e informacionit në një file tekst është metoda më e zakonshme në steganografi. Metoda ka të bëjë me fshehjen e një mesazhi brenda një teksti. Zhvillimi i internetit dhe i tipit të formave të ndryshme të të dhënave dixhitale kjo metodë nuk ka më të njëjtën rëndësi si dikur. Steganografia e tekstit që përdor të dhëna dixhitale nuk është shumë e përdorur sepse file-t tekst kanë shumë pak të dhëna të tepërta.
- **Steganografia e imazhit** Imazhet janë mediumi më i përdorur i fshehjes së mesazheve sekrete në steganografi. Një mesazh fshihet në një imazh dixhital duke përdorur një algoritëm fshehjeje, duke përdorur një çelës sekret. Imazhi stego që përftojmë pas këtij procesi i dërgohet marrësit. Nga ana tjetër, imazhi stego procesohet nga algoritmi i ekstraktimit duke përdorur të njëjtin çelës. Gjatë procesit të dërgimit të imazhit, persona të paautorizuar mund ta shikojnë transmetimin e një imazhi por jo të mesazhit sekret.
- **Steganografia e audios** Steganografia e audios ka të bëjë me fshehjen e informacionit në një audio cover të padëmshëm në një formë të sigurtë. Siguria e komunikimit dhe transmetimit janë jetësore për sa i përket transmetimit të informacioneve të rëndësishme drejt marrësve të synuar duke i mohuar aksesin personave të paautorizuar. Softwaret ekzistues të stegangrafisë së audios mund të fshehin mesazhe në file-t e audios WAV dhe MP3.
- **Steganografia e videos** Steganografia e videos është një teknikë që fsheh çdo lloj file në një file video.
- **Steganografia e protokollit** Ka të bëjë me fshehjen e informacionit brenda protokolleve të rrjetit si TCP/IP. Informacioni mund të fshihet në headerin e paketës TCP/IP, në fusha që janë opsionale ose që nuk janë përdorur asnjëherë [7].

1.4 Aplikimet e steganografisë

- **Komunikime sekrete**[9] Një nga format e aplikimit që steganografia nuk e reklamon është komunikimi sekret, me qëllim shmangien e nxitjes së interesit ndaj dërguesit, mesazhit dhe marrësit. Një sekret tregtar, nje blueprint, ose informacione të tjera sensitive mund të transmetohen pa nxitur interesin e sulmuesve potencialë.
- **Mbrojtje e të drejtave të autorit** Mekanizma të mbrojtjes që bëjnë të mundur që të dhëna, kryesisht të dhëna dixhitale të mos kopjohen. Futja dhe analizimi i watermarks për të mbrojtur materiale me të drejta autori është një nga arsyet për rritjen e interesit në steganografinë dixhitale dhe fshehjen e të dhënave.
- **Feature tagging** Elementë të ndryshëm mund të fshihen brenda një imazhi, si emra individësh në një foto ose vendndodhje në një hartë. Kopjimi i imazhit stego gjithashtu kopjon të gjithë elementët e fshehur brenda në imazh dhe vetëm palët që kanë stego-key e dekodimit mund të ekstraktojnë dhe shikojnë elementët (mesazhi i fshehur)[11][12].

1.5 Objektivat

Objektivat e kësaj mikroteze janë:

- Të japë informacion mbi steganografinë, konceptet kryesore të saj dhe dallimin e saj nga kriptografia.
- Të fshehë një mesazh ose të dhënë sekrete në një imazh që funksionon si medium cover duke përdorur teknikën LSB dhe shfaqja e ndryshimeve që ndodhin.

Kapitulli 2

2.1 Imazhi

Një imazh është një foto që është krijuar ose kopjuar dhe ruajtur në formë elektronike.
Një imazh mund të përshkruhet në aspektin e grafikës vektoriale ose grafikut raster. Një imazhi i ruajtur në formën raster nganjëherë quhet një bitmap. Një hartë imazhi është një skedar që përmban informacione që i lidhin vende të ndryshme në një imazh të caktuar me linke hypertext.Një imazh është një koleksion i numrave që përbëjnë dritë të ndryshme intensitet në fusha të ndryshme të imazhit. Kjo përfaqësim numerik formon një grid dhe pikat individuale janë referuar si pixels. Imazhet përdorin 8 bit për çdo piksel dhe janë në gjendje të shfaqin 256 ngjyra të ndryshme ose hije të grisë. Imazhet me ngjyra digjitale zakonisht ruhen në skedarë 24-bitësh dhe përdorin modelin e ngjyrave RGB. Të gjitha variacionet e ngjyrave për çdo pixel të një imazhi 24-bitësh rrjedhin nga tre ngjyrat kryesore: e kuqe, jeshile dhe blu, dhe çdo ngjyrë primare përfaqësohet nga 8 bit[4]. Kështu në një piksel të caktuar, mund të ketë 256 sasi të ndryshme të ngjyrave të kuqe, jeshile dhe blu [5].

2.2 Kompresimi i imazhit

Tek imazhet ekzistojnë dy lloje kompresimi: kompresimi me humbje (lossy) dhe kompresimi pa humbje (lossles). Në kompresimin pa humbje , çdo bit i të dhënave që ishte fillimisht në file mbetet aty dhe pasi file është dekompresuar. I gjithë informacioni është ruajtur si në fazën fillestare. Formatet më të njohura të imazheve që përdorin kompresimin pa humbje janë GIF (Graphical Interchange Format) dhe BMP(Bitmap File). Kompresimi me humbje e zvogëlon një file-n duke fshirë informacione të caktuara, kryesisht informacione të tepërta. Kur file kompresohet vetëm një pjesë e informacionit fillestar gjendet akoma aty. Në këtë rast imazhi që do përftojmë do jetë i ngjashëm me imazhin fillestar por jo i njëjtë. Shembull i një formati imazhi që përdor këtë teknikë kompresimi është JPEG (Joint Photographic Experts Group)[8].

2.3 Steganografia e imazheve

Disa nga teknikat më të njohura të steganografisë së imazheve janë:

2.3.1 Least significant bit insertion (LSB)

Steganografia e bazuar në teknikën LSB është një nga metodat më të thjeshta që fsheh mesazhe sekrete në LSB-të e vlerave te pixelave pa shkaktuar ndryshime të dallueshme. Për syrin e njeriut ndryshimet që ju ndodhin imazheve me ndryshimin e LSB janë të pakapshme. Futja e biteve të mesazhit mund të bëhet thjeshtë ose në mënyrë të rastësishme.

Avantazhet e teknikës LSB janë:

- Degradimi i imazhit origjinal nuk është i lehtë.
- Kapaciteti i fshehjes është më i madh.

Disavantazhet e teknikës LSB janë:

- Qëndrueshmëria (robustness) është e ulët
- Të dhënat e fshehura mund të shkatërrohen nga sulme të thjeshta

2.3.2 Masking dhe filtering

Masking dhe filtering është një teknikë steganografike që zakonisht përdoret në imazhet 24 bitë-she. Kjo teknike përdor algoritme specifike ose formula matematikore për të zgjedhur pixel-ë specifikë në një imazh. Këto pixel-ë të zgjedhur mund të përdoren për të fshehur informacionin, i cili më pas do duket si një pjesë integrale e imazhit cover. Duke përdorur filtrat e duhur (formulat matematikore) për të zgjedhur pixelat e imazhit, siguria e teknikës së përdorur rritet dhe kapacitetit i fshehjes së informacionit mund të rritet duke zgjedhur shumë pixel[5].

Avantazhet e Masking dhe Filtering jane:

- Është shumë më e qëndrueshme (robustness) se teknika LSB.

Disavantazhet:

- Mund të përdoret vetëm për imazhet grayscale dhe është e kufizuar deri në 24 bite.

2.3.3 Teknikat e transformimit

Në këtë teknikë mesazhi futet në koefiçientët e ndryshuar të imazhit duke i dhënë më shumë kapacitet të ruajtjes së informacionit dhe qëndrueshmëri ndaj sulmeve. Shumica e sistemeve steganografike të sigurta në ditët e sotme përdorin këtë teknikë. Kjo për arsye se kjo teknikë ndryshe nga teknika LSB e fsheh informacionin në zona të imazhit që janë më pak të ekspozuara ndaj kompresimit, cropping dhe procesimit të imazhit[3].
Teknikat e transformimit janë të tipeve të ndryshme:

1. Teknika e transformimit Discrete Fouirer (DFT)
2. Teknika e transformimit Discrete cosine (DCT)
3. Teknika e transformimit Discrete Wavelet(DWT)

2.4 Karakteristikat e teknikave të fshehjes së të dhënave

Perceptueshmëria - A e ndryshon procesi i fshehjes së informacionit mediumin cover (imazhin) në një nivel vizual të papranueshëm.

Kapaciteti - Sa informacion mund të fshihet në medium duke pasur parasysh lidhjen që ekziston midis kapacitetit dhe ndryshimit vizual që i ndodh mediumit.

Qëndrueshmëria ndaj sulmeve - A mund ti rezistojë informacioni i fshehur sulmeve që mund të vijnë na një medium stego i manipuluar, me qëllim shkatërrimin ose ndryshimin e të dhënave të fshehura

Rezistenca ndaj ndërhyrjeve - I referohet vështirësisë që ka një sulmues për të ndryshuar një mesazh pasi është futur në një imazh-stego[8].

2.5 Steganaliza e imazheve

Steganaliza është thyerja e steganografisë dhe është shkenca e detektimit të informacioneve të fshehura (mesazheve sekrete). Objektivi kryesor i steganalizës është thyerja e steganografisë dhe detektimi i imazheve-stego. Pothuajse të gjithë algoritmet steganalitike bazohen në algoritmat e steganografisë duke prezantuar diferencat statistikore midis imazheve stego dhe atyre cover.
Steganaliza është e tre tipeve të ndryshme:

Sulmet vizuale zbulojnë informacionin e fshehur, që ndihmon në ndarjen e imazhit në nivele bitesh për analiza të mëtejshme.

Sulmet statistikore mund të jenë pasive ose aktive. Sulmet pasive përfshijnë identifikimin e prezencës ose mungesën e mesazhit sekret ose të algoritmit të përdorur për fshehjen e mesazhit Sulmet aktive përdoren për të zbuluar gjatësinë e mesazhit sekret, vendndodhjen e mesazhit sekret ose çelësin sekret të përdorur për fshehjen e mesazhit.

Sulmet strukturore - Formati i file-t të të dhënave ndryshon me futjen e mesazhit sekret në file. Identifikimi i këtyre ndryshimeve strukturore na ndihmon të zbulojmë prezencën ose mungesën e fileve imazh/tekst.

2.5.1 Mjetet steganalitike

Ekzistojnë disa mjete steganalitike në treg si PhotoTitle, 2Mosaic dhe StirMark Benchmark etj...Këto mjete steganalitike mund të heqin çdo përmbajtje steganografike nga çdo imazh. Kjo arrihet duke e shkatërruar mesazhin sekret me anë të dy teknikave: break apart dhe resample[10].

Kapitulli 3

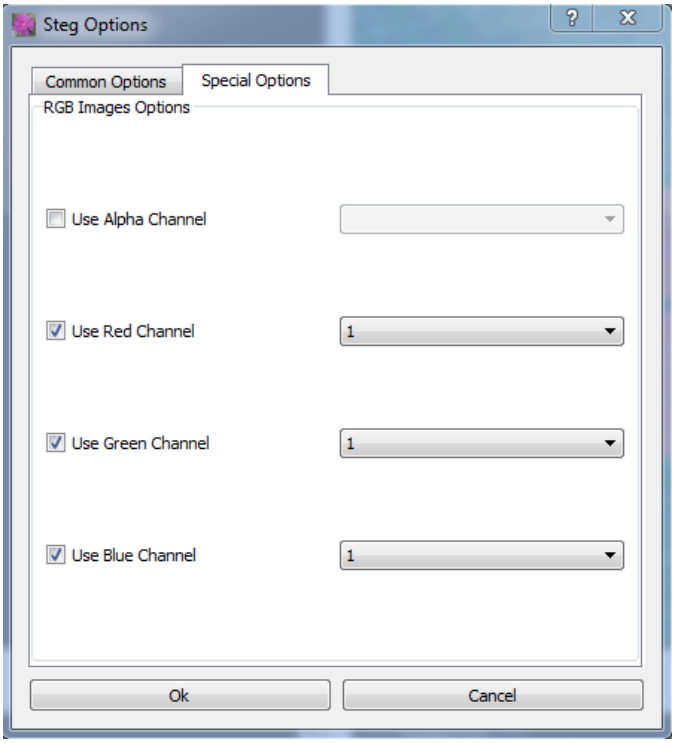
Fshehja e sigurtë e informacionit

3.1 Teknika Least-Significant Bit (LSB)

Biti më pak i rëndësishëm (pra biti i 8) i disa ose të gjitha byteve brenda një imazhi zëvendësohet me një bit të mesazhit të fshehtë. Imazhet dixhitale janë kryesisht të dy llojeve (i) imazhe 24 bit dhe (ii) imazhe 8 bit. Në imazhet 24 bitëshe mund të fshehim tre bite informacioni në çdo piksel, një në çdo pozicion LSB të tre tetë biteve. Rritja ose ulja e vlerës duke ndryshuar LSB nuk e ndryshon pamjen e imazhit; shumë kështu që imazhi stego rezulton pothuajse i njëjtë si imazhi cover. Në imazhet 8 bitëshe vetëm një bit i informacionit mund të fshihet.

3.1.1 Steg për fshehjen e informacionit

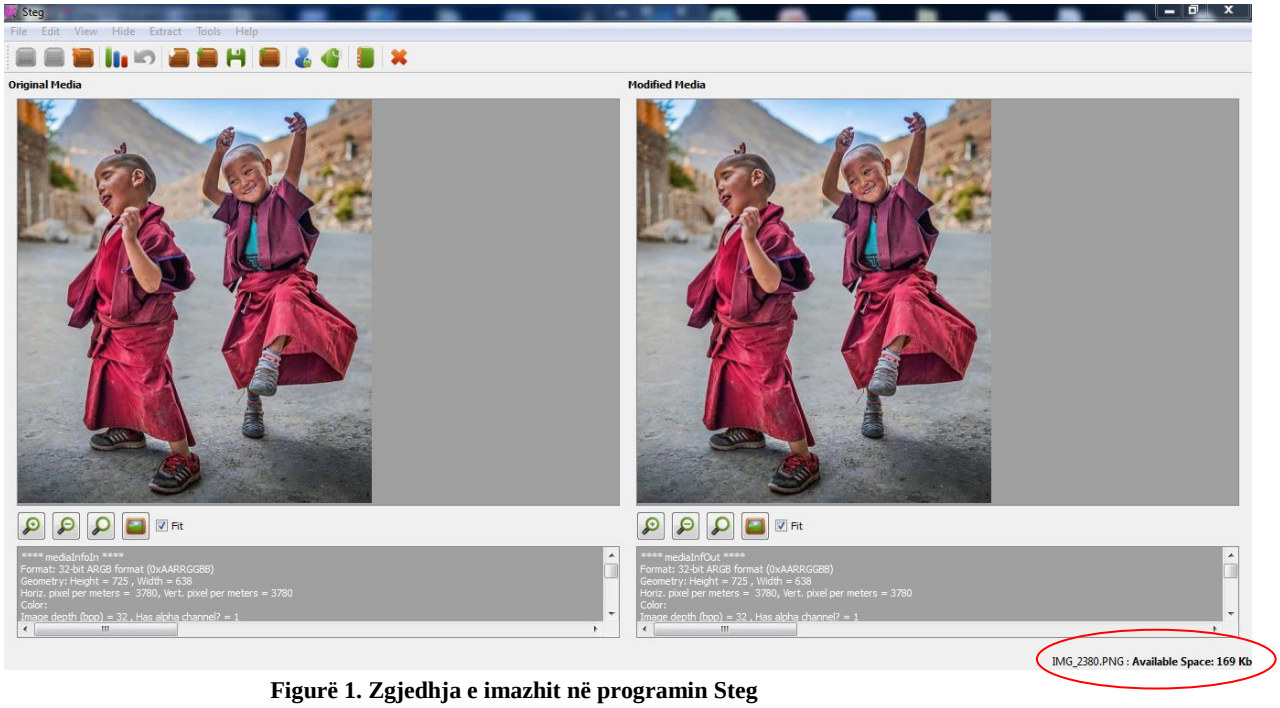
Steg është një program i cili përdor teknikën LSB për fshehjen e informacionit ne imazhe ,e si e tillë ne presim që ndryshimi në imazh pas futjes së mesazhit sekret nuk do jetë i dallueshëm me sy të lirë. Të dhënat që do fshihen mund të jenë tekst ose imazhe. Steg të lejon përdorimin e imazheve të formateve të ndryshme si cover image e në të njëjtën kohë lejon përdorimin e teknikave të ndryshme për fshehjen e mesazhit sekret. Imazhet cover me të cilat do punojnmë janë imazhe lossles (png).
Ajo që do paraqes në këtë kapitull është fshehja e një file tekst në një imazh dhe fshehja e një imazhi në imazh duke treguar ndryshimin që ndodh vizualisht tek imazhi .Gjithashtu do tregoj dy forma të fshehjes së mesazhit sekret (të kriptimit) ,ajo auto (opsion në Steg) ku fshehja dhe ekstraktimi i mesazhit sekret kryhet direkt pas klikimit të opsioneve dhe formën e kriptimit me çelësa publikë dhe privatë ,të cilat gjenerohen nga RSA key pair generator (opsion në Steg) ,të cilat e lejojnë ekstraktimin (nxjerrjen e mesazhit sekret) vetëm pas futjes së çelësave.



Figurë 0.Zgjedhja e numrit të biteve për teknikën LSB

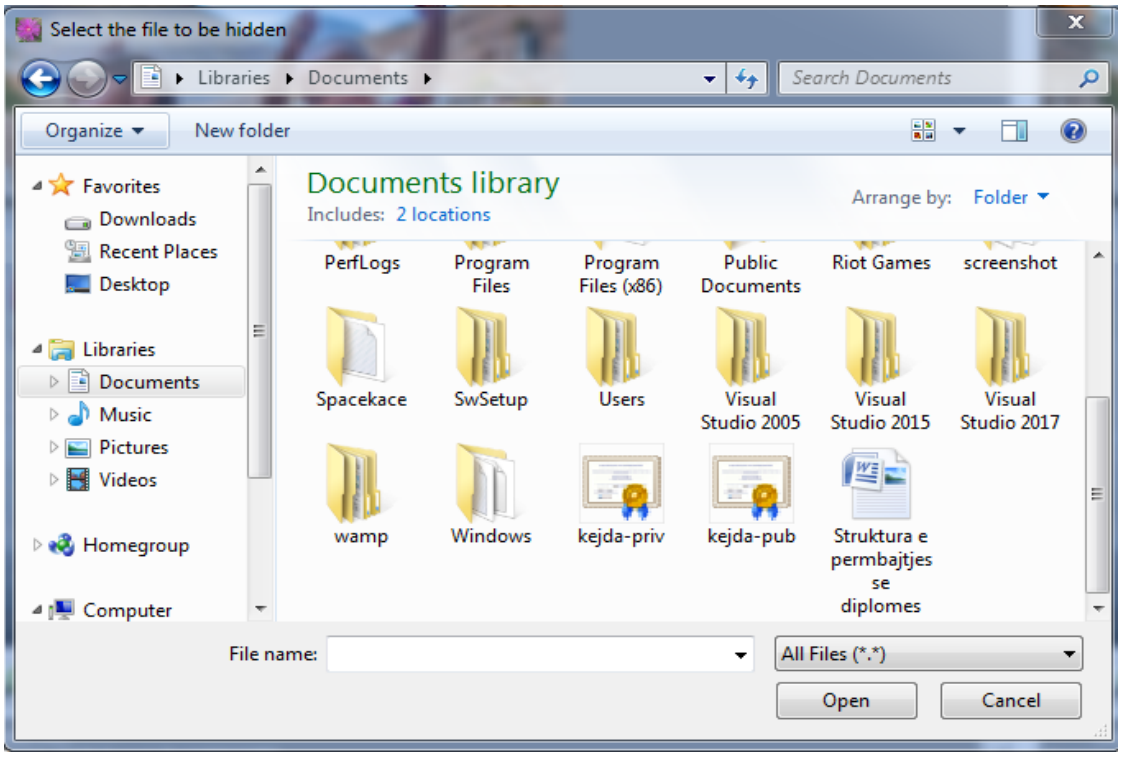
3.2 Fshehja e një file tekst në një imazh

Fillimisht zgjedhim foton që do përdorim si cover image për mesazhin tonë sekret.



Figurë 1. Zgjedhja e imazhit në programin Steg

Pas zgjedhjes së imazhit që do përdoret si cover ,zgjedhim të dhënat që do fshehim.



Figurë 2. Zgjedhim file-n që do fshehim

Në rastin tonë zgjedhim një file tekst me emrin "Struktura e përmbajtjes së diplomës".
Pas fshehjes së file-t do kemi këtë imazh.

Figurë 3 .Imazhi origjinal

Figurë 4.Imazhi stego

Siç vërehet dhe në figurë imazhi stego nuk ka asnjë ndryshim me sy të lirë nga imazhi origjinal. Arsyeja kryesore për këtë është fakti se e dhëna e fshehur është tekst dhe madhësia e file-t është e vogël .Procesi i ekstraktimit (nxjerrjes) së file-t të fshehur bëhet direkt me butonin extract ,dhe mesazhi sekret do ruhet në një direktori që ne zgjedhim.

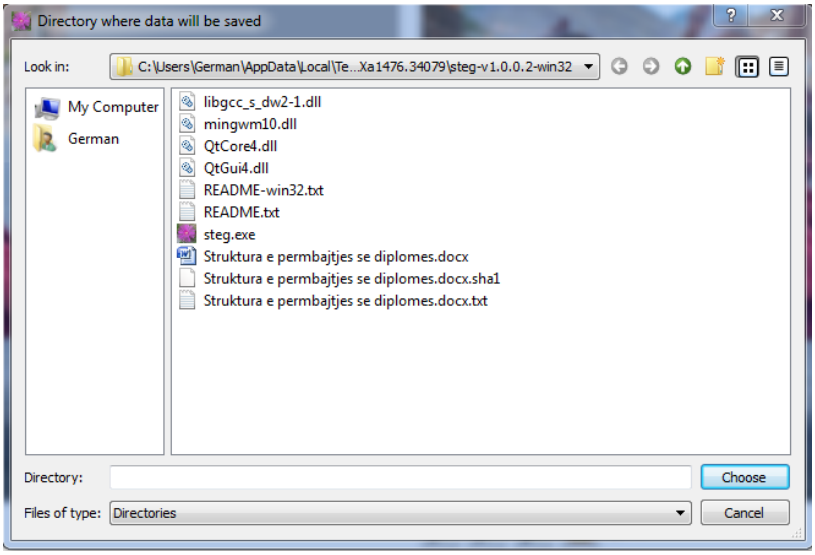
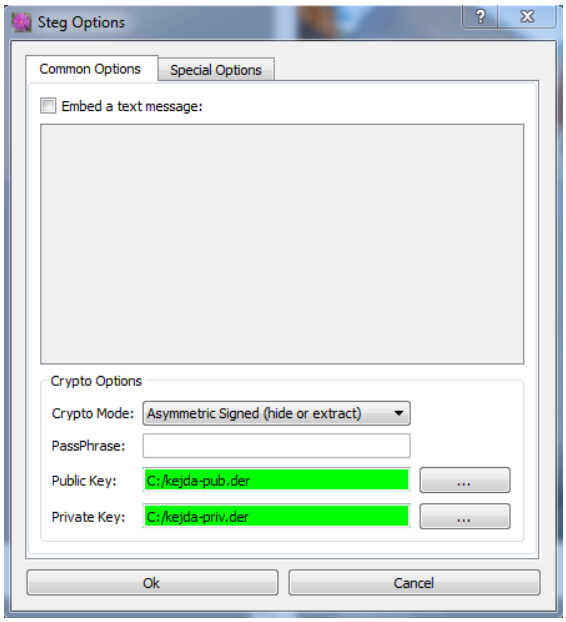


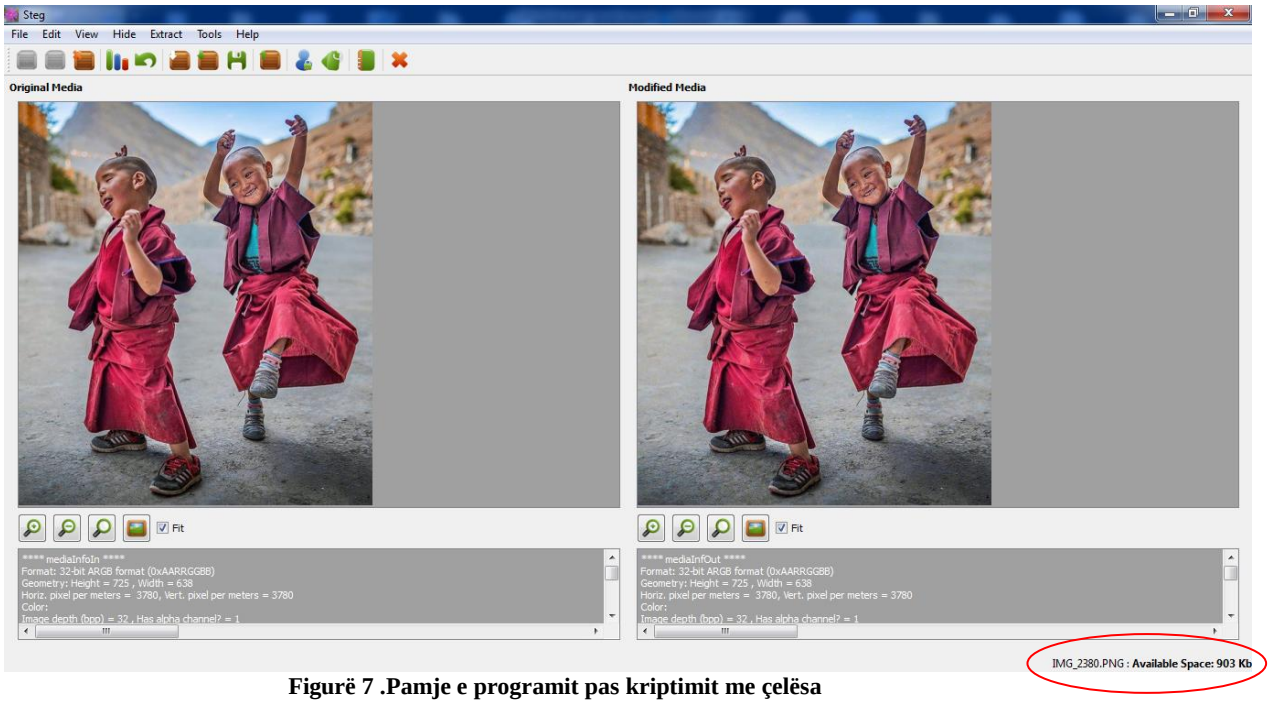
Figure 5 .Ekstraktimi i file-t të fshehur

3.2.1 Fshehja dhe kriptimi i një file tekst në një imazh

Në këtë rast do zgjedhim opsionin e kriptimit me çelësa publikë dhe privatë të cilët siç e përmenda më parë gjenerohen nga RSA key-pair generator dhe ruhen në një direktori për tu përdorur më vonë.



Figurë 6 .Zgjedhja e opsionit të kriptimit me çelësa publikë dhe privatë

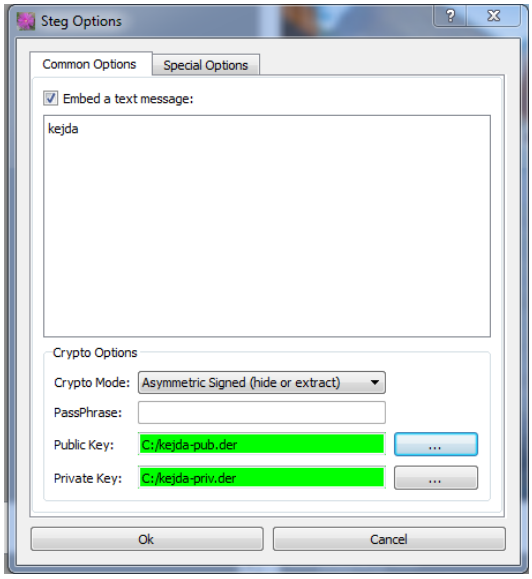


Figurë 7 .Pamje e programit pas kriptimit me çelësa

Figurë 8 .Imazhi origjinal

Figurë 9.Imazhi stego

Siç shihet nga figurat dhe në këtë rast ndryshimi në imazh nuk shihet me sy të lirë .Ajo që ne na tregon dallimin midis dy teknikave në këtë program është available space (hapësira në dispozicion pas fshehjes së file-t) që ne kemi në secilin rast .Nga figura shohim që hapësira që kemi në dispozicion pas fshehjes së file-t me çelësa publikë dhe privatë kemi më shumë hapësirë se sa në rastin e fshehjes dhe ekstraktimit direkt të file-t.



Figurë 10 .Fshehja e tekstit direkt

Në këtë rast kemi fshehur përveç file-t tekst (dokument word) kemi fshehur dhe një tekst të shkurtër (kejda) me opsionin embedd text. Pas procesit të ekstraktimit do shfaqet dhe një file me këtë tekst krahas atij word .

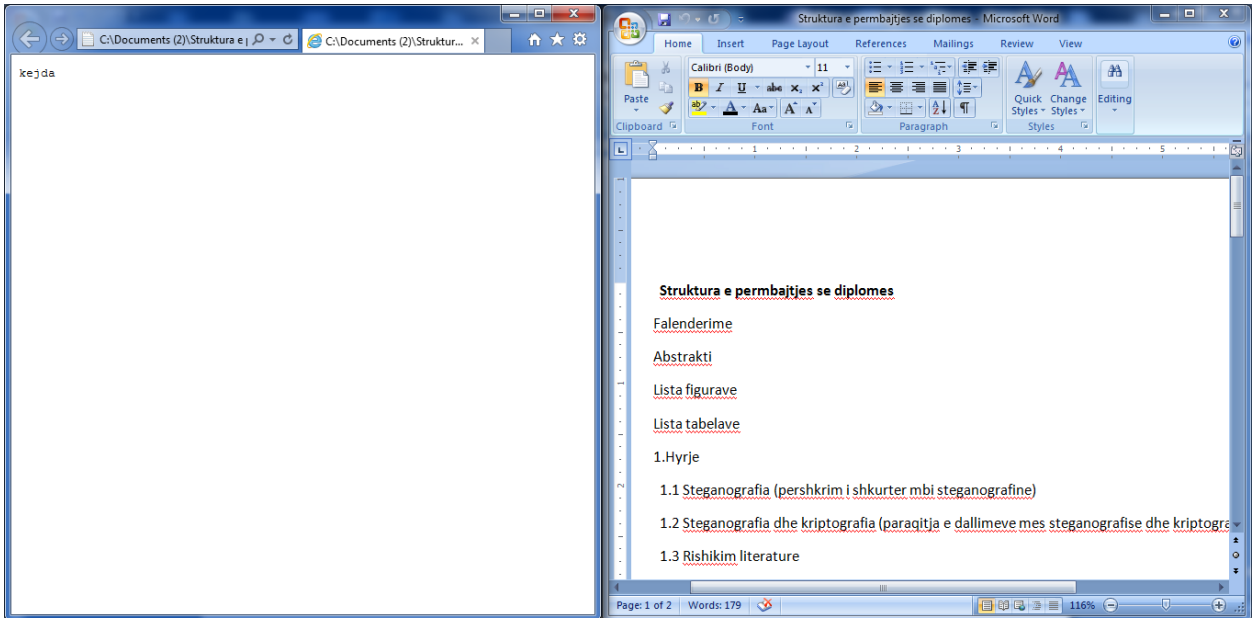
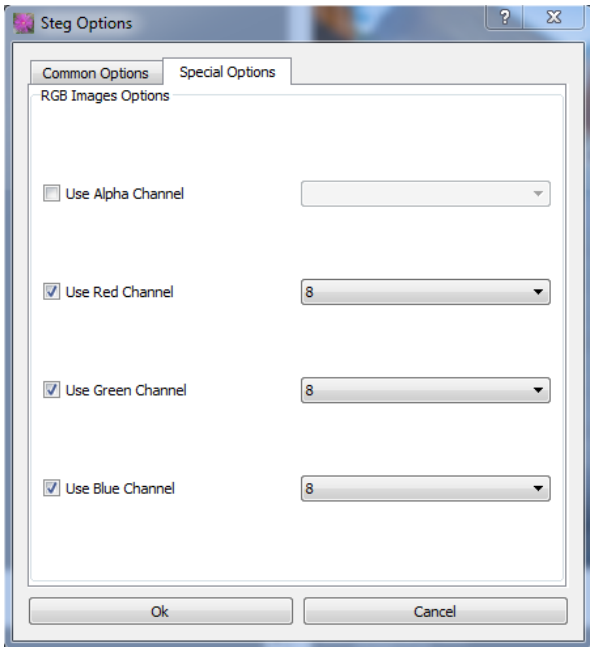


Figure 11.Filet e fshehura pas ekstraktimit

Ajo që duhet përmendur është se në të dy rastet e mësipërme nuk e kemi ndryshuar numrin e biteve që do zëvendësohen me anë të teknikës LSB ,pra kemi lënë opsionin ekzistues që zëvendëson një bit të secilës ngjyrë (R,G,B) prandaj nuk ekziston asnjë lloj ndryshimi i kapshëm me sy të lirë. Në rast se ndryshojmë numrin e biteve që zëvendësohen do kemi një rezultat të tillë ky ndryshimi është i vogël ,por nëse shikohet me vëmendje mund të dallohet me sy të lirë.



Figurë 12.Ndryshimi i numrit të biteve për teknikën LSB

Figurë 13.Imazhi stego pas ndryshimit të biteve

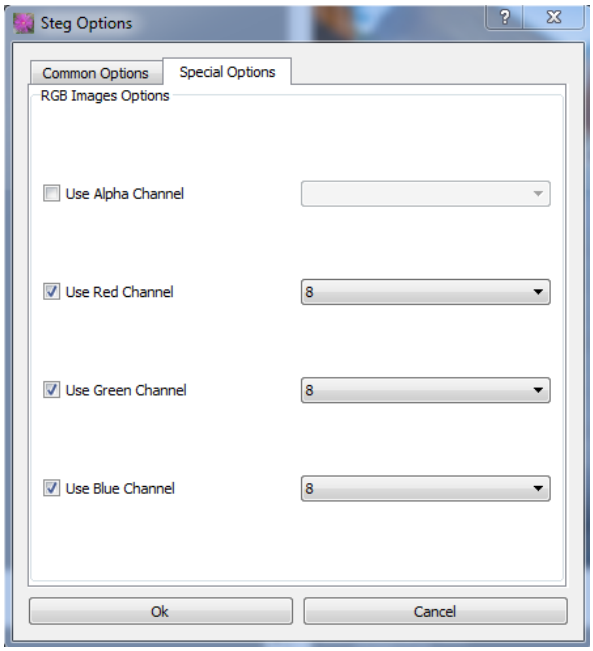
3.3 Fshehja e një imazhi në një imazh

Ashtu si në rastin e fshehjes së një file tekst ,dhe në këtë rast pas zgjedhjes së imazhit që do përdorim si imazh cover ,zgjedhim imazhin që ne duam të fshehim. Problemi fillestar që hasim është gjetja e një imazhi cover e cila ka hapësirë të mjaftueshme për të fshehur imazhin që ne duam. Për këtë arsye imazhi që do fshehim duhet të jetë më e vogël (në byte) se imazhi cover.
Në rastin e fshehjes së imazhit me metodën crypto auto do kemi këto rezultate.

Figurë 14. Imazhi cover

Figurë 15.Imazhi stego

Siç vërehet dhe në këtë rast nuk ka ndryshim të imazhit që mund të dallohet me sy të lirë edhe pse në këtë rast informacioni i fshehur është imazh ,por fakti që vetëm një bit zëvendësohet me teknikën LSB bën që ndryshimi të jetë i papërfillshëm. Nëse do ndryshojmë bitet që do zëvendësohen me teknikën LSB imazhi stego që përftojmë do ketë një ndryshim lehtësisht të dallueshem .



Figurë 16.Ndryshimi i numrit të biteve

Figurë 17.Imazhi stego pas ndryshimit të biteve

Imazhi që do marrim pas ekstraktimit është imazhi që kemi fshehur.

Figurë 18 .Imazhi i fshehur pas ekstraktimit

3.3.1 Fshehja dhe kriptimi i një imazhi në një imazh

Ashtu si në rastin e fshehjes së file-t text zgjedhim opsionin Assymetric Signed ,që bën kriptimin e imazhit të fshehur me anë të çelësave publikë dhe privatë. Imazhi stego që përftojmë nuk ka ndryshim vizual të dallueshëm me sy të lirë ,kjo për arsye se kemi lejuar zëvendësimin e vetëm një biti LSB për ngjyrat RGB. Imazhi që përftojmë është ky:

Figurë 19.Imazhi stego

Nga ana tjetër ,nëse do ndryshojmë numrin e biteve të zëvendësueshëm (LSB) si më sipër, imazhi stego që do përftojmë një imazh stego me ndryshime lehtësisht të dallueshme si më poshtë :

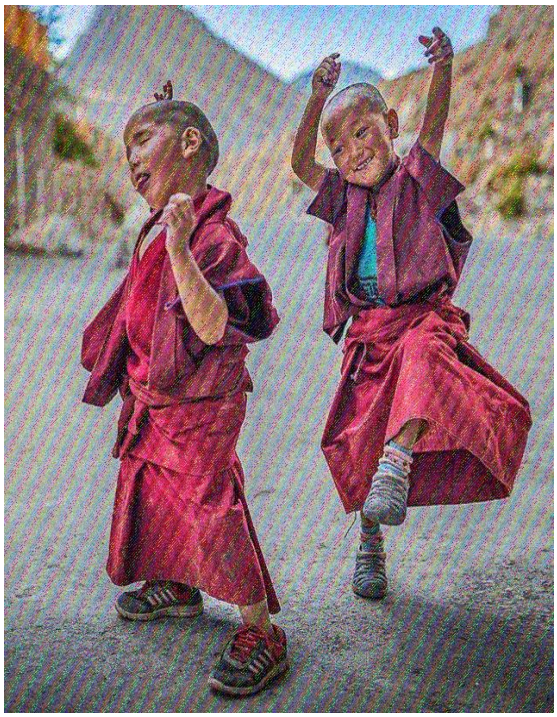


Figure 10. Imazhi stego

Kapitulli 4

Konkluzione

Ashtu siç e parashikuam në fillim, përdorimi i teknikës LSB për fshehjen e informacioneve në imazh bën të mundur që mesazhi i fshehur të mos ketë ndikim në pamjen e imazhit cover në mënyrë që të dallohet me sy të lirë ,por siç e pamë nuk ndodh gjithmonë kështu. Në rastin e fshehjes së një file tekst në imazh ,pavarësisht teknikës që përdorëm (auto ose me çelësa) dhe numrit të biteve te teknika LSB ndryshimi vizual nuk ishte shumë i madh (në rastin e dytë) , ndërkohë që në rastin auto nuk ekziston asnjëlloj ndryshimi.

Nga ana tjetër në rastin e fshehjes së një imazhi problemi është më i gjerë .Fillimisht duhet që imazhi cover i zgjedhur të ketë hapësirë të mjaftueshme për të fshehur imazhin (mesazhin sekret) e më pas kalojmë te aplikimi i teknikave. Në rastin e kriptimit auto vumë re që ndryshimi nuk është i dallueshëm me sy të lirë deri në momentin që ndryshojmë bitet te LSB e ndryshimi që ndodh te imazhi stego vihet re lehtësisht. E njëjta situatë na shfaqet dhe në rastin e kriptimit me çelës pas ndryshimit të numrit të biteve të përdorura për zëvendësim.

Çka duhet të kihet parasysh është fakti që ndryshimi i numrit të biteve te teknika LSB është bërë me qëllimin e paraqitjes të ndryshimit që ndodh në imazhin stego e për të treguar rëndësinë që kanë bitet në këtë teknikë .Në realitet dikush që ka për qëllim fshehjen e një mesazhi në një imazh do ta shmangte këtë ndryshim sepse do ishte si t'i dhuroje mesazhin sekret personave të paautorizuar.

Referenca

1). R.Anderson and F. Petitcolas, ”On the limits of steganography” IEEE Journal of Selected Areas in Communications, Vol. 16, No. 4, May 1998.
2). Niels Provos, Peter Honeyman, ”Hide and Seek: An Introduction to Steganography,” IEEE computer society,2003.
3). K B Raja, Venugopal K R and L M Patnaik, ”A Secure Stegonographic Algorithm using LSB, DCT and Image Compression on Raw Images”,Technical Report, Department of Computer Science and Engineering, University Visvesvaraya College of Engineering,Bangalore University, December 2004.
4). An overview of image steganography by T. Morkel , J.H.P. Eloff, M.S. Olivier. Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science University of Pretoria, 0002, Pretoria, South Africa.
5). Johnson, N.F. Jajodia, S., ”Exploring Steganography: Seeing the Unseen”, Computer Journal, February 1998.
6). ”A Tutorial Review on Steganography” by Samir K Bandyopadhyay, Debnath Bhattacharyya1, Debashis Ganguly1, Swarnendu Mukherjee1 and Poulami Das, Heritage Institute of Technology.
7). International Journal of Computer Science Engineering Technology (IJCSET) ”Modern Steganographic technique: A Survey” by Pratap Chandra Mandal Asst. Prof., Department of Computer Application B.P.Poddar Institute of Management Technology .
8). A. Cheddad, J. Condell, K. Curran and P.M. Kevitt. (2010). ”Digital image steganography: survey and analysis of current methods.” Signal Processing Journal.
9). A Review of Data Hiding in Digital Images by E Lin, E Delp Center for Education and Research Information Assurance and Security Purdue University, West Lafayette, IN 47907-2086.
10). W Bender, D. Gruhl, N. Morimoto, and A. Lu, ”Techniques for data hiding,” IBM Systems Journal, Vol. 35, No. 3 and 4.
11). Steganography and Steganalysis by J.R. Krenn January 2004.
12). Data hiding Algorithm for Bitmap Images using Steganography by Mamta Juneja Department of computer science and Engineering,RBIEBT,Sahuran
13). Hiding data in images by simple LSB substitution by Chi-Kwong Chan, L.M. Cheng Department of Computer Engineering and Information Technology, City University of Hong Kong, Hong Kong Received 17 May 2002.
14). Fabio(2013), Steg 1.0.0.2 [Computer Software] .Shkarkuar nga: http://www.fabionet.org/