Tampereen yliopisto

Teemu Löppönen

KATSAUS MODERNIN STEGANOGRAFIAN KÄYTTÖKOHTEISIIN

Informaatioteknologian ja viestinnän tiedekunta
Kandidaattitutkielma
Helmikuu 2020

TIIVISTELMÄ

Teemu Löppönen: Katsaus modernin steganografian käyttökohteisiin
Kandidaattitutkielma
Tampereen yliopisto
Tietojenkäsittelytieteiden tutkinto-ohjelma
Helmikuu 2020

Tässä kirjallisuuskatsauksessa esittelen steganografian historiaa, perusteita, toimintametodeja sekä käyttökohteita. Aloitan kirjallisuuskatsauksen kertomalla steganografian historiasta sekä selostan tarkemmin steganografian perusteet ja vaatimukset. Tämän jälkeen esittelen steganografian suorittamiseen käytettyjen LSB – ja verkkoprotokolla metodien toimintaperiaatteen. Toimintaperiaatteiden esittelyn jälkeen listaan ja esittelen useita erilaisia esimerkkejä steganografian käyttökohteista. Käyttökohteiden esittelyn jälkeen kerron erilaisista keinoista steganografian käytön havaitsemiseen. Kirjallisuuskatsauksen lopussa esittelen lähteet sekä selostan kirjallisuuskatsauksen aikana löydetyt tulokset. Kirjallisuuskatsaukseni tulosten mukaan steganografia on huomaamaton ja joustava tekniikka, joka mahdollistaa datan kätkemisen lähes mihin tahansa peitetasoon.

Avainsanat: Steganografia, toimintametodi, havaitseminen, toimintaperiaate, käyttökohteet

1 Johdanto

Nykyajan nopeatempoisessa ja jatkuvassa muutoksessa elävässä maailmassa fyysistä sekä digitaalista viestintää ja keskustelua pyritään tarkkailemaan ja tallentamaan. Tämän seurauksena yksilön oman tietoturvallisuuden ylläpitämisestä on tullut huomattava haaste. Ratkaisu yksilön kasvaviin vaatimuksiin on steganografia. Steganografian avulla yksilön henkilökohtainen data pystytään kätkemään siten, ettei asiasta tietämätön kykene paikantamaan kätkettyä tietoa. Lyhykäisyydessään steganografia tarkoittaa kätkettävän datan koko olemassaolon salaamista, eräänlaista modernia piilokirjoitusta.

Tämän kirjallisuuskatsauksen tavoitteena on selvittää miten steganografia toimii ja mihin kaikkeen sitä voidaan käyttää. Tarkoituksena on steganografian perusperiaatteiden selkeyttäminen, erilaisten toimintametodien esittely sekä erilaisten käyttökohteiden listaaminen. Lähestyn tutkimusta sellaisen henkilön näkökulmasta, joka ei ole koskaan kuullut steganografiasta. Tutkimuksen tutkimusmenetelmänä toimii kirjallisuuskatsaus. Tutkimuksen tietolähteiden etsimiseen olen käyttänyt Andor, ProQeuest ja Google Scholar tietokantoja. Hakusanoina käytin lyhyitä englanninkielisiä lauseita steganografian eri toiminnoista ja toimintametodeista.

Aloitan tutkimuksen kappaleessa kaksi kertomalla steganografian historiasta ja toimintaperiaatteesta. Tutkimuksen kolmannessa kappaleessa esittelen useita erilaisia steganografian suorittamiseen käytettyjä toimintametodeja. Neljännessä kappaleessa esittelen monia esimerkkejä steganografian erilaisista käyttökohteista. Viidennessä kappaleessa esittelen erilaisia keinoja steganografian käytön havaitsemiseen. Tutkimuksen kuudennessa kappaleessa esittelen työssä tehdyt löydökset, sekä kerron ehdotukseni jatkotutkimuksesta. Tutkimuksen lopusta löytyvät kirjallisuuskatsauksen tekoon käytetyt lähteet.

2 Steganografia

Johnson ja Jajodia (1998) esittelevät tutkimuksessaan tarkemmin steganografian historiaa. Johnson ja Jajodia kertovat, että sana steganografia tulee kreikan kielen sanoista *steganos* ja *graphe,* joka tarkoittaa karkeasti suomennettuna piilotettua kirjoitusta. Steganografialla tarkoitetaan tiedon kätkemistä siten, että se on ihmissilmälle huomaamatonta. Steganografiaa ei tule kuitenkaan sekoittaa kryptografiaan. Kryptografiassa viesti salataan tai sekoitetaan, mutta sitä ei piiloteta. Kryptografialla salattua viestiä ei siis pystytä ymmärtämään ilman toimivaa salausavainta. Kryptografialla salattu viesti herättää huomattavasti enemmän huomiota, kuin steganografialla kätketty viesti, jonka olemassaolosta ei ole mitään todisteita. On mahdollista käyttää steganografiaa ja kryp-

tografiaa samanaikaisesti, esimerkiksi salaamalla kätkettävä tieto kryptografialla ennen varsinaista kätkemistä steganografialla, mutta tässä tutkimuksessa keskitytään pelkästään steganografian ominaisuuksiin ja toimintaan.

2.1 Steganografian toimintaperiaate

Perinteinen steganografia vaatii toimiakseen kaksi asiaa: kätkettävää dataa sekä peitekuvan, johon data kätketään. Käytännössä kätkettävä data voi olla melkein mitä tahansa tekstiä, kuvia tai numeroita. Datan kätkemiseen käytettävänä peitekuvana voi myös toimia lähes mikä tahansa materiaali kaarnasta metalliin.

Yksinkertaistettu esimerkki perinteisen steganografian toiminnasta voisi olla esimerkiksi kirjeen kirjoittaminen sitruunamehulla. Tällöin kirjeeseen kirjoitettu teksti olisi ihmissilmälle huomaamatonta sitruunamehun kemiallisten ominaisuuksien takia, vaikka oikealla tekniikalla eli kirjettä lämmittämällä sitruunamehulla kirjoitettu teksti olisi luettavissa. Tällöin sitruunamehulla kirjoitettua teksti olisi kätketty peitetason sisälle steganografialle ominaisella tavalla.

2.2 Digitaalisen steganografian toimintaperiaate

Digitaalisella steganografialla tarkoitetaan tiedon kätkemistä digitaaliseen mediaan. Myös digitaalinen steganografia vaatii toimiakseen kaksi asiaa: piilotettavaa dataa, esimerkiksi numeroita, tekstiä tai valokuvia. Tämän lisäksi tarvitaan myös jokin peitekuva, johon data kätketään. Peitetasona voi toimia esimerkiksi jokin digitaalinen tiedosto kuten PNG-valokuva tai TXT-tekstitiedosto. Yleisemmin digitaalisen steganografian peitetasolla tarkoitetaan digitaalisia valokuvia ja äänitiedostoja, mutta käytännössä dataa voidaan kätkeä myös tiedonsiirtosignaalin sisälle.

Kaikki tietokoneen data koostuu pohjimmiltaan biteistä, oli kyseessä siten valokuva, tekstitiedosto tai ohjelmisto. Tiedon tallentamiseen tarkoitetulla yhdellä bitillä on yhtensä kaksi mahdollista toisensa pois sulkevaa tilaa, joita tavallisimmin kuvataan ykkösinä ja nollina. Digitaalisessa steganografiassa kätkettävän tiedon data pilkotaan biteiksi ja kätketään peitetasona toimivan tiedoston bittien sekaan.

3 Steganografian toimintametodit

Steganografian perusperiaatteiden selkeyttämisen jälkeen syvennymme tarkemmin erilaisiin toimintametodeihin, joiden avulla dataa voidaan kätkeä steganografian perus-

teiden mukaisesti. Esittelen seuraavaksi kolme erilaista toimintametodia, joita voidaan käyttää datan kätkemiseen erilaisten peitetasojen sisälle.

3.1 LSB – metodi

LSB eli Least Significant Bit, tarkoittaa karkeasti suomennettuna vähiten merkitsevää bittiä. Krennin (2004) sekä Johnsonin ja Jajodia (1998) kertovat tutkimuksissaan, että LSB-metodi on suhteellisen yksinkertainen ja suoraviivainen tapa piilottaa dataa. LSB-metodissa käytetään hyväksi digitaalisten valokuvien pikseleiden väriarvojen vähiten merkitseviä bittejä datan kätkemiseen. Piilotettavaa dataa voidaan kätkeä LSB-metodin avulla myös videoihin tai musiikkitiedostoihin. LSB-metodissa kätkettävä data pilkotaan biteiksi, jonka jälkeen pilkotun tiedon biteillä korvataan kätkemiseen käytetyn peitetason valokuvan pikselien väriarvojen vähiten merkitsevät bitit.

Tässä lyhyt esimerkki kätkettävän datan pilkkomisesta sekä kätkemisestä digitaaliseen valokuvaan. Esimerkissä piilotettavana tietona toimii kirjain ”A”, jonka pituus on 1 tavu eli 8 bittiä tai tarkemmin totuusarvomuuttujana ilmaistuna 01000001. Kirjain ”A” piilotetaan peitetasona toimivaan digitaaliseen 24 bittiseen valokuvaan X, jonka leveys on 3 pikseliä ja korkeus on 1 pikseli.

Aloitetaan avaamalla peitetason ensimmäisen pikselin punainen, vihreä sekä sinisen värikanava. Tämän jälkeen punaisen väriarvon vähiten merkitsevä bitti korvataan kätkettävän tiedon ensimmäisellä bitillä 0. Tätä jatketaan korvaamalla peitetason ensimmäisen pikselin vihreän väriarvon vähiten merkitsevä bitti piilotettavan tiedon toisella bitillä 1. Viimeiseksi korvataan peitetason ensimmäisen pikselin sinisen väriarvon vähiten merkitsevä bitti piilotettavan tiedon kolmannella bitillä 0.

Tätä korvausoperaatiota jatketaan peitetasona toimivan digitaalisen valokuvan jokaiseen pikseliin, kunnes piilotettavan tiedon jokainen bitti on saatu kätkettyä. Tässä esimerkissä piilotettavan tiedon pituus oli 8 bittiä, josta jokaista pikseliä kohti piilotettiin kolme bittiä. Yhden kirjaimen piilottaminen käyttäen ainoastaan peitetason yhtä vähiten merkitsevää bittiä tarvitaan siis vähintään kolme pikseliä.

Johnsonin ja Jajodia (1998) kertovat tutkimuksessaan, että korvaamalla digitaalisen valokuvan värikanavien vähiten merkittävä bitti kätkettävällä datalla menetetään karkeasti noin 0.4 % alkuperäisen peitetason yksityiskohdista. Korvaamalla kaksi vähiten merkitsevää bittiä menetettäisiin 1.2 % alkuperäisen peitetason yksityiskohdista. Korvaamalla kolme vähiten merkitsevää bittiä menetettäisiin noin 2.75 % alkuperäisen peitetason yksityiskohdista. Seitsemän vähiten merkitsevän bitin korvaamisella menetettäisiin 49,8 % yksityiskohdista. Seitsemän vähiten merkitsevän bitin korvaaminen aiheuttaisi valtavia häiriöitä ja poikkeuksia valokuvaan. Johnsonin mukaan yhden vähiten merkitsevän bitin arvon muuttaminen vaikuttaa peitetasoon kuitenkin niin vähän, ettei

ihmissilmä kykene huomaamaan eroa. Tämä tekee LSB-metodista tehokkaan, mutta jokseenkin yksinkertaisen tavan piilottaa dataa. LSB-metodia voidaan helposti tehostaa hajauttamalla kätkettävä data ympäri peitetasona toimivaa digitaalista valokuvaa sekä salaamalla data kryptografialla ennen kätkemistä.

3.2 Verkkoprotokollaan pohjautuva steganografia

Lubacz (2012) ja Das (2011) todistivat tutkimuksessaan, että verkkoliikenteen sisälle pystytään kätkemään dataa steganografian avulla. Verkkoprotokollaan pohjautuvassa steganografiassa käytetään hyväksi verkkoliikenteessä jatkuvasti toistuvaa dataa, jonka vähäinen muokkaaminen ei haittaa verkkoliikenteen tavallista toimintaa. Lubaczin ja Dasin mukaan verkkoliikennettä hyväksikäyttävässä steganografiassa kätkettävä data pilkotaan biteiksi, jonka jälkeen se kätketään verkkoprotokollien kuten TCP, UDP ja IP sisälle. Verkkoprotokollan sisälle steganografialla kätkettävä data piilotetaan ylätunnisteen käyttämättömien bittien sisälle. Lubaczin ja Dasin mukaan datan kätkemiseen parhaiten soveltuvia tarpeettomia ylätunnisteen kenttiä ovat esimerkiksi tunniste- ja lippukentät. Verkkoliikenteeseen pohjautuva steganografia mahdollistaa kätketyn tiedon hitaan ja hallitun lähettämisen ja vastaanottamisen. Verkkoprotokollaan pohjautuvan steganografian huonona puolena kätketyn datan vastaanottajan tulee olla tietoinen hänelle lähetettävästä verkkoliikenteeseen piilotetusta viestistä, jotta hän kykenee valmistautumaan vastaanottamaan kätketyn datan.

3.3 Äänitiedostoihin pohjautuva steganografia

Gopolan (2003) todistaa tutkimuksessaan, että steganografiaa voidaan käyttää datan kätkemiseen äänitiedostoihin. Gopolan mukaan äänitiedostoihin voidaan kätkeä dataa muokkaamalla hienovaraisesti äänen määrittelevien taajuuksia bittejä. Äänitiedostojen suuremman tiedostokoon takia niihin pystytään kätkemään huomattavasti enemmän dataa kuin esimerkiksi tekstitiedostoihin tai valokuviin. Äänitiedoston muokkaus on hyvin samankaltainen prosessi kuin LSB-metodissa esitetty. Gopolan mukaan äänitiedoston muokkaaminen steganografialla ei ole kuitenkaan yhtä suoraviivaista tai täysin ongelmatonta. Gopolan tutkimuksen mukaan suurin ongelma äänitiedostoihin pohjautuvassa steganografiassa on ihmiskorva. Ihmiskorva kykenee havaitsemaan pienetkin steganografian aiheuttamat poikkeukset ja muutokset taajuudessa, jonka seurauksena steganografian avulla muokattu äänitiedosto saattaa kuulostaa luonnottomalta tai se saattaa sisältää jatkuvaa kohinaa. Ihmiskorvan tarkkuuden takia tulee kiinnittää äärimmäistä huomiota mitä taajuuksia muokataan. Gobolan tutkimuksen tulosten mukaan kätkemisen seurauksena aiheutunutta häiriötä voidaan minimoida kätkemällä dataa vain korke-

ampia ja matalimpia ääniä määrittelevien taajuuksien sekaan. Tällöin ihmiskorvan on huomattavasti vaikeampi, mutta ei kuitenkaan mahdotonta kuulla muutosta manipuloidussa äänitiedostossa, koska muokatut äänitaajuudet ovat ihmiskorvan kuuloalueen äärireunoilla.

4 Steganografian käyttökohteet

Steganografian käyttämisen vahvuuksia on ehdottomasti sen huomaamattomuus sekä joustavuus. Steganografian avulla on siis mahdollista kätkeä mitä tahansa informaatiota lähes minkä tahansa peitetason sisälle siten, ettei paljas ihmissilmä kykene havaitsemaan kätkettyä tietoa. Seuraavaksi esittelen useita esimerkkejä steganografiaa hyödyntävistä käyttökohteista.

4.1 Käteisvaluutta

Ensimmäinen steganografiaa hyödyntävä käyttökohde on käteisvaluutta. Käteisvaluutta sisältää useita erilaisia uniikkeja ihmissilmälle näkyviä ja näkymättömiä merkintöjä, materiaaleja sekä vesileimoja, jotta sen aitouden fyysinen ja digitaalinen tunnistaminen olisi mahdollisimman helppoa. Tällaisten merkintöjen ja vesileimojen tarkoituksena on myös vaikeuttaa käteisvaluutan kopioimista ja väärentämisestä. Erään tällaisen käteisvaluuttaan steganografian avulla kätketyn merkinnän nimi on EURion. EURionin olemassaolo paljastui vuonna 2002, kun saksalaisen tutkijan Marcus Kuhnin väritulostin ei suostunut tulostamaan valokuvaa setelistä.

Nieves (2010) kertoi tutkimuksessaan tarkemmin käteisvaluuttaan piilotetusta EURion kuviosta. Nieves todisti tutkimuksessaan, että useiden eri valtioiden käteisvaluuttaan on kätketty useita keltaisia, vihreitä ja oransseja renkaita, joiden muodostamaa kuviota kutsutaan EURioniksi. Nievesin mukaan renkaiden muodostamaa kuviota käytetään setelin fyysisen ja digitaalisen aitouden tunnistamiseen. Nievesin mukaan EURionia voidaan käyttää myös käteisvaluutan väärentämisen vaikeuttamiseen. Mikäli väärentämiseen käytetty skanneri, tulostin tai kuvankäsittelyyn erikoistunut ohjelmisto havaitsee edes yhden kokonaisen EURion kuvion, se estää setelin skannaamisen, muokkaamisen sekä tulostamisen, vaikeuttaen väärentämisprosessia.

4.2 Kommunikointi

Toinen vähemmän tunnettu esimerkki steganografian käytöstä on kommunikointi. Cox (2007) todisti että steganografiaa voidaan käyttää kahden tai useamman organisaa-

tion välisen kommunikaation kätkemiseen esimerkiksi valtioissa, joissa ”poliittisesti eriäviä mielipiteitä ei sallita”. Tällaisessa ympäristössä toimivien organisaatioiden tulee käyttää äärimmäistä huolellisuutta kommunikoidessaan keskenään. Cox (2007) esittää tutkimuksessaan että, steganografian avulla kätketty keskustelu olisi yksi turvallisimmista, kun keskustelun eri osapuolet tietävät olevansa jatkuvan kolmannen osapuolen tarkkailun alaisia.

Schmurr (2003) todisti tutkimuksessaan, että steganografiaan pohjautuvaa viestintää on käytetty myös erilaisten terroristi- ja rikollisjärjestöjen väliseen kommunikointiin. Schmurr kertoo tutkimuksessaan, että erilaisia steganografiaan pohjautuvia sovelluksia opetetaan käyttämään hyväksi esimerkiksi Afganistanin ja Sudanin ääriryhmien koulutusleireillä. Steganografiaan pohjautuvalla kommunikoinnilla on myös todistetusti ollut osallisuutta vähintään kolmeen eri terrori-iskuun. Nämä iskut ovat Kenialaisen sekä Tansanialaisen lähetystön pommittaminen vuonna 1998 sekä WTC-iskujen suunnittelu ja toteuttaminen vuonna 2001.

4.3 Värilasertulostimet

Embar (2014) todisti tutkimuksessaan, että modernit värilasertulostimet piilottavat tulosteisiin yksilöiviä ihmissilmälle näkymättömiä vesileimoja. Embarin mukaan värilasertulostimet merkitsevät jokaiseen tulosteeseen vesileiman pienten keltaisten pallojen muodossa. Tulostimien kätkemät vesileimat sisältävät Embarin tutkimuksen mukaan ainakin tulostimen yksilöivän sarjanumeron sekä tulostamisen päivänmäärän sekä kellonajan minuutin tarkkuudella. Embarin tutkimuksen mukaan piilotetut vesileimat ovat ihmissilmälle nähtävissä vain tehokkaalla sinisellä valolla sekä ultravioletti LED-valolla. Embarin mukaan tulostimen kätkemän vesileiman pystyy paikantamaan myös mikroskoopilla tai voimakkaalla taustavärin muutoksella. Tutkimuksessaan Embar esitteli myös erilaisia tekniikoita, joiden avulla tulostimen yksilöivä vesileima saadaan peitettyä. Tutkimuksessa esitettyihin peittotekniikoihin kuuluu esimerkiksi vesileiman sijoitusalueen peittäminen keltaisella laatikolla tai vaihtoehtoisesti koko paperiarkin täyttäminen pienillä keltaisilla pisteillä. Embarin mukaan yksittäiseen tulosteeseen piilotettua vesileimaa voidaan käyttää tulosteen tulostamiseen käytetyn tulostimen tunnistamiseen ja jäljittämiseen eri toimijoiden toimesta.

4.4 Reaaliaikainen sisällön vesileimaus

Digitaalisen sisällön ja ohjelmiston immateriaalioikeudet ovat yksi suurimmista haasteista internetin aikakaudella. Digitaalisen median suojeluun ja tunnistamiseen on kehitetty useita erilaisia metodeja ja algoritmeja, joissa yksinkertaisimmillaan kätketään

vesileima digitaalisen median sisälle. Reaaliaikaisella sisällön vesileimauksella tarkoitetaan toistettavan median sisällön tekijänoikeuksien dynaamista merkitsemistä. Tämä parantaa digitaalisten materiaalien ja sovellusten tekijänoikeussuojaa.

Piec (2014) esitteli tutkimuksessaan tarkemmin sisällön reaaliaikaista vesileimausta. Piec esittelee tutkimuksessaan reaaliaikaista ihmissilmälle näkymätöntä vesileimausta, jota käytetään World of Warcraft videopelissä. Piecin mukaan jokaiseen pelistä otetun kuvankaappaukseen päälle tallentuu myös ihmissilmälle näkymätön dynaaminen vesileima. Tämä ihmissilmältä piilotettu vesileima sisältää esimerkiksi kuvankaappauksen kellonajan, pelihahmon yksilöivän uniikin numeraalisen tunnuksen, asiakasohjelman versionumeron, pelipalvelimen IP-osoitteen sekä muita yleisiä tietoja. Reaaliaikainen vesileimaus toimii pelin päällä pyörivällä ylimääräisellä tasolla. Tällä tavoin yksilöivä vesileima saadaan toistettua jokaiseen kuvankaappaukseen dynaamisesti. Word of Warcraftin kuvankaappausten dynaaminen vesileimaus lisättiin peliin jo vuonna 2007, mutta paljastui pelaajien tutkimuksen seurauksena vasta vuonna 2012. Piecin mukaan dynaamista vesileimausta voidaan käyttää esimerkiksi immateriaalioikeuksien tarkempaan valvomiseen.

5 Steganografian havaitseminen

Steganografialla on useita erilaisia toimintametodeja ja käyttökohteita, mutta tulee kuitenkin pitää mielessä, ettei steganografia ole täysin huomaamaton kätkemismetodi. Datan kätkeminen digitaalisesti aiheuttaa aina pieniä muutoksia peitetasona käytettyyn mediaan. Pienten muutosten seurauksena peitetasoon saattaa ilmestyä jonkin asteista hajoamista sekä epätavallisia ominaisuuksia. Steganografian tutkimiseen, havaitsemiseen ja paljastamiseen käytetään stegoanalyysiksi kutsuttua tekniikkaa.

5.1 Steganografian yleinen havaitseminen

Kumar (2010) kuvaa tutkimuksessaan tarkemmin stegoanalyysissä käytettyjä metodeja. Yksinkertaisin keino steganografian havaitsemiseen on alkuperäisen muokkaamattoman peitetason ja tiedon piilottamiseen käytetyn peitetason vertaaminen. Tällöin muokatun peitetason ja muokkaamattoman peitetason eroavaisuudet tulevat selkeimmin esille. Tällöin peitetasoon kätketty data saadaan esille vertaamalla sitä muokkaamattomaan peitetasoon. Valitettavan usein alkuperäistä muokkaamatonta peitetasoa ei ole kuitenkaan saatavilla, jolloin tulee turvautua haastavampiin havaitsemismetodeihin. Kumarin mukaan toinen haastavampi keino steganografian havaitsemiseen on peitetason visuaalinen analysointi. Tällöin muokattua peitetasoa pyritään tutkimaan ulkoisten

muutosten ja epätavallisten ominaisuuksien varalta ihmissilmällä tai koneavusteisesti. Tällöin analysoitavassa peitetasossa ilmenevät poikkeukset, häiriöt tai uniikkien värien lukumäärän poikkeuksellisen äkillinen nousu tai lasku voi paljasta, että peitetasoon on kätketty dataa steganografian avulla.

5.2 Äänitiedostoon pohjautuvan steganografian havaitseminen

Natarajan ja Nayak (2010) kertovat tutkimuksessaan, että äänitiedostoihin pohjautuva steganografia voidaan havaita esimerkiksi äänitiedostossa esiintyvien häiriöiden ja poikkeuksien avulla. Natarajan ja Nayakin mukaan datan ollessa kätketty ihmiskorvan kuuloalueen reunoilla, voidaan kätketyn datan paikantamiseen käyttää tilastomatematiikkaan pohjautuvia algoritmeja. Tällaisessa tilanteessa algoritmi pilkkoo äänitiedoston useaan erilliseen taajuusalueisiin ja vertailee niiden arvoja. Poikkeuksellisen korkeat piikit ja toistuvuudet yksittäisen taajuusalueen sisällä saattavat paljastaa steganografian avulla kätketyn datan olemassaolon.

5.3 LSB-metodiin pohjautuvan steganografian havaitseminen

Fridrich (2001) paneutuu tutkimuksessaan tarkemmin LSB-metodin avulla kätketyn datan paljastamisesta. Fridrichin mukaan LSB-metodin avulla kätkettyä tietoa voidaan pyrkiä paljastamaan purkamalla peitetasona toimivan digitaalisen valokuvan pikselien bitit bittialueisiin. Bittialueita koneavusteisesti analysoimalla voidaan päätellä onko peitetasoon kätketty dataa. Fridrich kertoo tutkimuksen tuloksissaan, että LSB-metodin avulla kätketty data saadaan suurella todennäköisyydellä selvitettyä, mikäli peitetason pikseleistä alle 30 % sisältää uniikkeja värejä. Fridrichin tutkimuksen mukaan LSB-metodin avulla kätketty tieto on todella vaikea paljastaa, mikäli peitetason pikseleistä yli 50 % sisältää uniikkeja värejä.

6 Yhteenveto

Tässä kirjallisuuskatsauksessa olen esitellyt steganografian toimintaperiaatteen sekä useita toimintametodeja. Tämän jälkeen listasin useita steganografian käyttökohteita, sekä esittelen erilaisia keinoja steganografian käytön havaitsemiseen. Kirjallisuuskatsaukseni päätarkoituksena oli selventää steganografian toimintaperiaate ja tuoda esille erilaisia steganografian käyttökohteita. Toin myös esille kuinka steganografia toimii käytännössä ja miten steganografian käyttö pystytään havaitsemaan. Mielestäni kirjallisuuskatsauksen tärkein osuus on kuitenkin steganografian perusperiaatteen selkeyttämi-

nen, sekä erilaisten steganografiaa käyttävien käyttökohteiden listaaminen. Tiedonhaun aikana en löytänyt ainuttakaan tutkimusta, joka olisi selostanut kuinka steganografia toimii käytännössä. En myöskään löytänyt tutkimusta, joka olisi koonnut yhteen useita erilaisia steganografian käyttökohteita.

Tulevaisuudessa steganografiaan pohjautuvat jatkotutkimukset voitaisiin kohdentaa esimerkiksi äänitiedoston steganografian käytön havaitsevan algoritmin tutkimiseen ja kehittämiseen. Vaihtoehtoisesti jatkotutkimuksen resurssit voitaisiin kohdistaa toimivan prototyyppiohjelmiston tuottamiseen. Ohjelmisto voisi pilkkoa kätkettävän datan biteiksi, jonka jälkeen ohjelmisto hajauttaisi kätkettävän datan ympäri peitetasoa steganografialle ominaisella tavalla. Ohjelmiston tulisi kiinnittää erityisesti huomiota uniikkien värien suuren lukumäärän ylläpitämiseen. Tällöin steganografian käytön havaitseminen olisi huomattavasti haastavampaa. Ohjelmisto voisi käyttää myös kryptografiaa kätkettävän tiedon salaamiseen ennen peitetasoon kätkemistä. Suorituksen lopussa ohjelmisto voisi tulostaa käyttäjälle raportin. Raportissa kerrottaisiin yksityiskohtaisesti suorituksen tiedot, esimerkiksi montako prosenttia yksityiskohdista menetettiin käyttäen annettua peitetasoa, sekä kuinka monta prosenttia peitetason väreistä on uniikkeja.

7 Viiteluettelo

Kaliappan Gopolan (2003). Audio steganography using bit modification. International Conference on Multimedia and Expo. Sivut 629-632 DOI: 10.1109/ICME.2003.1220996

Schmurr, A., Crawley, W. (2003). Cybercrime in the United States criminal justice system: Cryptography and steganography as tools of terrorism. Journal of Security Administration, 26(2), Sivut 51-75.

Ingemar Cox, Matthew Miller, Jeffrey Bloom, Jessica Fridrich & Ton Kalker (2007). Digital Watermarking and Steganography. Sivut 427-434. ISBN: 978-0-12-372585-1.

Neil F. Johnson & Sushil Jajodia (1998). Exploring steganography: Seeing the unseen. Computer, volume 31, issue 2 (1998). Sivut 26-34 DOI: 10.1109/MC.1998.4655281

Maya Embar, Louis F. McHugh & William R. Wesselman (2014). Printer Watermark Obfuscation. SIGITE/RIIT Proceedings of the 3rd annual conference on Research in information technology (2014) Sivut 15-20. ISBN: 978-1-4503-2711-4.

Józef Lubacz, Wojciech Mazurczyk & Krzysztof Szczypiorski (2012). Principles and Overview of Network Steganography. IEEE Communications Magazine vol. 52. DOI: 10.1109/MCOM.2014.6815916

Javier Nieves, Igor Ruiz-Agundez & Pablo G. Bringas (2010). Recognizing Banknote Patterns for Protecting Economic Transactions. Workshops on Database and Expert Systems Applications (2010). ISBN: 978-1-4244-8049-4.

Maciej Piec & Andreas Rauber (2014). Real-time screen watermarking using overlaying layer. Ninth International Conference on Availability, Reliability and Security (2014). ISBN: 978-1-4799-4223-7

Jessica Fridrich, Miroslav Goljan & Rui Du (2001) Reliable Detection of LSB Steganography in Color and Grayscale Images. MM&Sec '01: Proceedings of the 2001 workshop on Multimedia and security: new challenges, Lokakuu 2001 Sivut 27–30 DOI: 10.1145/1232454.1232466

Arvind Kumar & Km. Pooja (2010). Steganography- A Data Hiding Technique. International Journal of Computer Applications, volume 9, issue 7. DOI: 10.5120/1398-1887

Meghanathan Natarajan, and Lopamudra Nayak (2010). "Steganalysis algorithms for detecting the hidden information in image, audio and video cover media." International Journal of Network Security & Its Application. Sivut 43-55.

Krenn Robert (2004). "Steganography and steganalysis". Itsenäisesti julkaistu tutkimus vuodelta (2004).

Soumyendu Das, Subhendu Das & Sugata Sanyal (2011). Steganography and Steganalysis: Different Approaches. International Journal of Computers, Information Technology and Engineering Vol. 2 No. 1.