Steganografia

origini, tecniche e prospettive

di Roberto Campesato, Andrea Sottoriva

Versione 0.7, 05 Febbraio, 2005

Indice

> Il pericolo di essere scoperti era grande; gli venne in mente un solo modo per far giungere in patria l'avviso: grattar via la cera da un paio di tavolette per scrittura, annotare sul legno sottostante le intenzioni di Serse, e ricoprire il messaggio con cera nuova. In tal modo le tavolette, che sembravano vergini, furono recapitate senza insospettire le guardie. Quando il messaggio giunse a destinazione, mi risulta che nessuno immaginó la sua esistenza, finché Gorgo, moglie di Leonida, ebbe una premonizione e disse che, grattando via la cera, sul legno sarebbe apparsa una scritta. Fu fatto cosí, il messaggio fu trovato e letto, poi riferito agli altri greci.
>
> *Storie*, Erodoto.

1 Introduzione

Percorrendo la storia dell'umanitá sono moltissimi gli episodi in cui le sorti di una vita, o addirittura di un intero popolo, sono dipese da sicurezza e segretezza impiegate nelle comunicazioni. Evitare che informazioni sensibili venissero scoperte o cadessero accidentalmente in mani sbagliate era, ed é tutt'ora, una continua lotta tra chi inventa metodi sempre piú sofisticati per nascondere informazioni e chi, con le sole armi dell'intelligenza, fa di tutto per violarne la segretezza.

Dalle origini ad oggi, l'evoluzione delle tecniche di occultamento delle informazioni non solo é andata di pari passo con le scoperte scientifiche ma é stata al tempo stesso punto di partenza e motore di molti dei risultati ottenuti del progresso tecnologico, accelerandone notevolmente i tempi di sviluppo: basti pensare al chiaro esempio della velocitá con cui si sono diffusi i calcolatori.

In un mondo in cui l'informazione é diventata la materia prima piú preziosa, l'importanza di nasconderene la circolazione o di proteggerne la riservatezza é andata via via aumentando; e mentre un tempo poteva essere considerata una precauzione destinata a pochi casi limite, oggi il bisogno di riservatezza é piú che mai vicino alla vita di tutti. Ogni giorno telefonate, messaggi di posta elettronica o transazioni di qualunque genere attraversano regioni, paesi, continenti, in luoghi potenzialmente esposti al rischio di intercettazione, con inevitabili conseguenze che possono mettere a repentaglio la nostra privacy.

Questo testo si propone in un primo momento di introdurre brevemente le origini storiche che hanno portato allo sviluppo di tecniche crittografiche e in particolar modo steganografiche, per poi approfondire queste ultime in modo rigoroso, citando le piu' comuni implementazioni e analizzandone peculiaritá e punti deboli. Infine sará dato spazio alle relazioni che intercorrono tra crittografa e steganografia che, pur essendo sostanzialmente due tecniche diverse possono trarre beneficio l'una delle caratteristiche dell'altra.

2 Origini

2.1 Le Storie di Erodoto

Alcuni dei piú remoti esempi di steganografia sono contenuti negli aneddoti narrati da Erodoto nelle sue *Storie*, ed in particolare dove si fa riferimento alle guerre combattute dai greci nel V secolo a.C. contro l'impero persiano; non a caso la parola steganografia deriva dal greco **steganós**, coperto, e **gráphein**, scrittura.

2.1.1 L'affronto degli Elleni al Re dei re

In quegli anni le mire espansionistiche di Serse, imperatore di persia, minacciavano libertá e indipendenza delle *póelis* elleniche: durante la costruzione di Persepoli, nuova capitale persiana, tributi e doni giunsero nella cittá da ogni parte dell'impero e dai paesi vicini. Soltanto Sparta e Atene si astennero dal celebrare l'operato degli uomini al servizio di Serse, il quale, da parte sua, prese questa decisione non solo come una mancanza di rispetto nei suoi confronti ma come un vero e proprio affronto alla autoriá che impersonava. Piú che mai deciso a vendicarsi, Serse cominció ad arruolare soldati per organizzare un attacco a sorpresa: il caso volle che durante i preparativi fosse presente Demarato, un esule greco stabilitosi in territorio persiano; nonostante la sua lontananza imposta dalla Grecia, nutriva ancora un certo amor di patria nei confronti del suo paese natale, perció decise di fare il possibile per avvertire spartani e ateniesi dell'attacco imminente.

Per evitare che informazioni riguardanti l'attacco trapelassero oltre il confine, Serse dispose che ogni cosa in transito da o verso la persia fosse controllata scupolosamente dalle sentinelle imperiali; Demarato era intenzionato a inviare un messaggio agli elleni ma per farlo con successo avrebbe dovuto eludere il controllo delle sentinelle. Gli venne un'idea: prese delle tavolette scrittorie, rimosse la cera e incise il messaggio sul legno sottostante che in seguito fece ricoprire con della nuova cera; in questo modo le tavolette, che avevano chiaramente l'aspetto di tavolette vergini non insospettirono le sentinelle al confine, che le lasciarono passare senza problemi in Grecia.

Erodoto racconta anche che il messaggio nascosto nelle tavolette, giunto nelle mani del popolo greco, venne scoperto grazie a una premonizione, che permise loro di investire il ricavato delle miniere d'argento nella costruzione di navi, in vista dell'arrivo della flotta nemica. I Greci che fino a quel momento sarebbero stati del tutto impreparati ad un attacco a sorpresa, sono corsi immediatamente ai ripari e si sono salvati grazie al messaggio segreto di Demarato.

Grazie a Demarato e all'astuzia delle forze elleniche l'armata persiana venne miseramente sconfitta.

2.1.2 La voce della rivoluzione

Un altro curioso episodio in cui la tecnica steganografica é stata usata con successo é riportato da Erodoto nel quinto libro delle *Storie* e si colloca nello stesso periodo storico: Istiéo, cugino di Aristagora di Mileto, era stato allontanato dalla cittá di Mileto dal re persiano Dario e costretto a Susa. Istiéo, desideroso di vendicarsi e di tornare nella Ionia decise di avvertire il cugino Aristagora affinché organizzasse la ribellione contro contro il re persiano.

C'era soltanto un problema: tutte le strade della cittá di Susa erano presidiate da sentinelle e Istiéo non osava inviare una lettera al cugino. Decise quindi di prendere il piú fedele dei suoi servi e gli fece rasare completamente i capelli, tatuó sulla testa di quest'ultimo il messaggio da inviare ad Aristagora; attese che i capelli del servo fossero ricresciuti e lo invió a Mileto dal cugino con l'indicazione che una volta lí avrebbe dovuto chiedere ad Aristagora che gli venissero tagliati i capelli. Arrivato a destinazione fece come era stato istruito: gli furono rasi i capelli e Aristagora lesse il messaggio, lo comunicó ai suoi uomini piú fidati che diedero inizio alla rivolta.

2.2 La Scitale spartana

Si tratta di uno dei primi esempi in cui la steganografia viene usata in concomitanza con l'uso di una forma meccanica della crittografia. La scitale spartana era un cilindro di legno su cui veniva arrotolata ad elica una striscia di cuoio, sulla quale poi sarebbe stato scritto il messaggio, seguendo la direzione dell'asse del cilindro.

Una volta scritto il messaggio, la striscia di cuoio veniva srotolata: il risultato ottenuto era una sequenza di caratteri incomprensibile e apparentemente casuale, disposta lungo una delle superfici della stricia. Questa sequenza altro non era che una permutazione delle lettere che compongono il messaggio.

A questo punto per ricavare il testo originale era necessario che il destinatario fosse in possesso di una scitale dello stesso diametro di quella usata dal mittente; arrotolando nuovamente ad elica la striscia di cuoio diventava quindi possibile per il destinatario del messaggio leggerne il contenuto. Eínteressante notare che compare un concetto assolutamente embrionale di chiave crittografica che prende forma e si identifica con la scitale: chiunque in possesso di una scitale uguale per diametro a quella usata dall'autore del messaggio era in grado di intercettarlo; diversamente con scitali di diametro inferiore o superiore non era possibile ottenere il giusto allinamento delle lettere e di conseguenza leggerne il vero significato.

L'uso di questa rudimentale tecnica crittografica veniva spesso associato ad applicazioni di tipo steganografico: quindi a questo punto non solo il comunicazione era nascosta rendendo difficile stabilire che fosse avvenuta, ma anche nel caso in cui venisse scoperta, risultava comunque illeggibile da chi non era in possesso della scitale avente un diametro adeguato a consentire la decodifica.

In molti casi la striscia di cuoio usata per contenere il messaggio veniva cammuffata da cintura o da qualsiasi altro accessorio personale nelle mani del messaggero; questo consentiva una maggiore sicurezza nella comunicazione, perché anche in caso di perquisizione da parte di autorita' di controllo, la presenza del messaggio sarebbe rimasta comunque quasi del tutto inaspettata ed insospettabile.

2.3 Gli inchiostri cosiddetti simpatici

Al giorno d'oggi quando si fa riferimento all'uso di inchiostro simpatico si pensa a qualcosa di buffo e inusuale, un trucco per organizzare improbabili giochi di prestigio, ma nella realtá anche la scrittura simpatica ha giocato un ruolo importante nella storia della steganografia.

Plinio il Vecchio, uno scienziato naturalista del I secolo d.C., fu il primo di cui si hanno testimonianze scritte a raccontare di un inchiostro invisibile che si puó ricavare dal lattice del titimabo e che, una volta esposto al calore assume un colore marroncino, dovuto al degrado termico delle sostenze organiche in esso contenute.

Anche lo scienziato italiano del XVI secolo, Gianbattista Della Porta, spiegó che con una tecnica simile é possibile nascondere dei messaggi nelle uova sode: preparando un inchiostro con trenta grammi di allume e mezzo litro di aceto e scrivendo con questo sul guscio di un uovo il preparato é completamente assorbito dalla superficie porosa del guscio senza lasciare traccia. Soltanto sbucciando l'uovo é possibile risalire al messaggio scritto in precedenza, impresso sulla superficie bianca dell'albume solidificato.

2.4 L'estremo oriente

Nell'arco dei duemila anni che ci separano dalla storia della Grecia cosí come raccontata da Erodoto, innumerevoli altre forme di steganografia sono state sviluppate in tutto il mondo, e non solo: parallelamente all'evoluzione della steganografia che, pur essendo un metodo efficiente per nascondere messaggi ha un punto debole non indifferente nel momento in cui viene scoperto, si assiste alla nascita delle prime forme di crittografia e alla stesura dei primi testi a sostegno dei metodi piu' innovativi in grado di attaccarla.

2.4.1 La Cina

Per questioni politiche e culturali che non saranno trattate in questa sede, la comunicazione tra la Cina e il resto del mondo é sempre stata minima e soltanto negli ultimi anni abbiamo potuto assistere a una radicale svolta; tuttavia la storia riporta delle testimonianze interessanti per quanto riguardano i metodi di comunicazione steganografica applicati in territorio cinese ma anche tra la Cina e l'estero.

La principale tecnica adottata dai messaggeri consisteva nel dipingere il contenuto del messaggio su striscioline di seta microscopiche, appallottolarle e immergerle nella cera fino a formare delle minuscole palline: una volta seccata la cera le palline venivano inghiottite e portate a destinazione. In questo modo il messaggio, protetto dall'attacco degli agenti corrosivi prodotti dallo stomaco di chi lo ospitava, poteva arrivare a destinazione in modo del tutto insospettabile.

Non é escluso che questa tecnica venga usata ancora oggi, avvalendosi di supporti di memorizzazione piú avanzati come microfilm, supporti ottici, magnetici o olografici, a seconda del livello di sicurezza e riservatezza desiderati dall'ambito in cui sono richiesti. Chiaramente al giorno d'oggi i metodi per individuare tecniche steganografiche che che si avvalgono di organismi viventi come mezzo contenitore di informazioni sono soggetti alle innumerevoli tecnologie sviluppate dalla medicina per individuare copri estranei, e quindi potenzialmente semplici da scoprire.

2.4.2 I crittoanalisti arabi

Come accennato all'inizio di questa sezione, il popolo arabo fu il primo ad adottare tecniche di occultamento delle informazioni di tipo crittografico. L'obbiettivo

era custodire in modo sicuro i dati riguardanti l'amministrazione pubblica. In questo tipo di applicazione l'uso della steganografia ha lasciato spazio all'adozione di tecniche di scrittura cifrata.

Oltre a proteggere messaggi contenenti delicate questioni di stato, la stessa crittografia veniva usata per tutti i documenti e gli archivi fiscali in modo sistematico; in questo senso numerosi scritti sono stati rinvenuti, ma non si era ancora arrivati a dimostrare con certezza che la crittografia in ambito amministrativo fosse un'abitudine, finché nel 1987 non venne scoperta l'esistenza di un vero e proprio trattato sull'amministrazione, l'*Adab al-Kutab* (*Il manuale del segretario*), una cui sezione é interamente dedicata alle techiche che dovevano essere adottate dai funzionari statali per crittare ogni genere di atto o documento.

Ma la ragione per cui é importante fare riferimento agli arabi per quanto riguarda la crittografia é un altra: non solo intrudussero nuove tecniche di cifratura, ma contribuirono a renderne obsolete molte altre. Infatti eṕroprio a loro che si deve la nascita della *crittoanalisi*, ovvero la scienza che si occupa di risalire al messaggio originale a partire dal crittogramma, senza avere a disposizione la chiave di codifica o informazioni sull'algoritmo usato per occultare il messaggio.

Le solide basi su cui poggiava la cultura islamica, unite a un diffuso benessere nella societá del tempo e all'insegnamento del Corano, spinsero molti uomini ad abbracciare la strada del sapere, il sapere multidisciplinare che in quel tempo spaziava dall'algebra alla medicina, dall'astronomia alla linguistica, fino ad arrivare alla statistica: ed é proprio qui che gli arabi furono particolarmente astuti e intravidero l'importanza della statistica in campo crittoanalitico.

Relizzato che in linguaggio é formato da un alfabeto, e che a una determinata lingua corrisponde una determinata distribuzione di frequenza con la quale le lettere si ripetono, gli studiosi arabi capirono che per determinate tecniche crittografiche come la *sostituzione monoalfabetica*[1] potevano essere facilmente attaccate da un'analisi di questo tipo. Individuando i simboli piú frequenti nel testo cifrato e in un testo sufficientemente esteso nella lingua con cui si suppone sia stato composto il testo originale, si puó procedere per sostutizione, dal simbolo piú frequente a quello meno frequente, fino ad arrivare a comporre parole parzialmente comprensibili che possono essere facilmente indovinate.

La piú antica descrizione di questo procedimento si deve allo studioso del IX secolo Abu Yusuf ibn Ishaq al-Kindi, noto anche come il Filosofo degli Arabi, che lo descrisse accuratamente nel suo *Sulla decifrazione dei messaggi crittati*, e al quale é stato dato il nome di *Metodo di analisi delle frequenze*; adottato per anni in tutto il mondo é uno dei primi metodi crittoanalitici noti.

2.5 Tempi Moderni

2.5.1 Il Microdot

Usato dagli agenti segreti tedeschi in America Latina nella seconda guerra mondiale, il microdot é una delle piú recenti tecniche steganografiche che non coinvolge la rappresentazione dei messaggi in formato digitale, lo stesso che popola le memorie di massa di ogni calcolatore.

[1] Tecnica crittografica in cui ogni lettera o simbolo del messaggio iniziale viene sostituita con altri simboli appartenenti ad un alfabeto differente, o ordinato in modo differente

Tramite un procedimento fotografico, era possibile stampare su un frammento di pellicola di diametro inferiore al millimetro un'intera pagina di messaggio, per poi nascondere il risultato in un qualsiasi testo dal contenuto banale, ad esempio sul puntino di una i. Pur trattandosi una tecnica potenzialmente infallibile, il microdot rappresenta storicamente uno dei casi in cui non é stato il livello di segretezza a comprometterne il contenuto, bensí l'affidabilitá delle persone in cui era stato riposto il segreto; il primo microdot fu scoperto dall'FBI nel 1941 grazie a una soffiata: qualcuno suggerí agli agenti americani di cercare sulla superficie di una lettera un luccichio che tradiva la presenza di una superficie lucida come quella di una pellicola. Da quel momento in poi gli americani furono in grado di intercettare qualunque comunicazione nemica di origine tedesca proveniente dall'America Latina.

Anche in questo caso l'unione di steganografia e crittografia permise ai tedeschi di rendere se non impossibili, quantomeno difficili le intercettazioni successive: la loro soluzione al problema fu quella di appoggiare i messaggi su microdot dopo averli sottoposti a cifratura, una strategia che impediva agli americani di avere notizie aggiornate ma che permetteva comunque di intercettare e bloccare le comunicazioni.

2.5.2 Gli Acrostici

L'ultima testimonianza steganografica riportata ha uno stretto legame con la letteratura e la filosofia: l'acrostico é un metodo usato molto spesso per nascondere messaggi all'interno di composizioni scritte di senso compiuto, sfruttando regole banali note sia al mittente che al destinatario.

Alcuni esempi di regole possono essere *sequenze di caratteri equidistanti*[2] oppure *la terza lettera di tutti gli aggettivi.*

La comparsa delle prime forme di acrostico compare nell'antichitá della Grecia per mano di Epicarmo di Cos (V secolo a.C.) che usava firmare i suoi drammi servendosi di questo tipo di tecnica steganografica: questo, oltre ad essere la prima testimonianza dell'uso di acrostici nella letteratura é anche il punto di partenza sul quale si é sviluppata una tecnica di garanzia dell'autenticitá di documenti nota con il nome di *watermarking*, della quale si parlerá successivamente in questo testo.

L'acrostico, oltre ad essere usato per rappresentare informazioni rigardanti la provenienza di un testo o l'autore dello stesso, é stato anche un mezzo per diffondere messaggi a grandi quantitá di persone. L'esempio piú famoso e al tempo stesso interessante é quello dello scrittore di racconti dell'orrore, nonché padre fondatore del racconto giallo, Edgar Allan Poe.

In molte delle opere di Poe é stata sfruttata la tecnica dell'acrostico per celare nel testo sinistri messaggi o semplici giochi di parole. Uno tra tutti, la poesia del 1846 *A Valentine*: prendendo la prima lettera del primo verso, la seconda del secondo, la terza del terzo e cosí via, si puó comporre il nome di Mrs. Frances Sargent Osgood, scrittrice di Boston contemporanea e amica di Poe.

[2] Tecnica usata per nascondere parole o frasi che possono essere ricavate raccogliendo, a partire da una parola a da un punto del testo, tutte le lettere che si trovano in posizione multipro della distanza scelta. Molti sostengono che la Bibbia contenga numerosi esempi di questo tipo, addirittura interi discorsi di senso compiuto. Tuttavia é stato piuvolte dimostrato che statisticamente é molto probabile, in testi di grandi dimensioni, incappare in questo tipo di fenomeni, trasformandosi in coincidenze.

3 La steganografia odierna

3.1 Principi

Oggigiorno la steganografia come la crittografia ha avuto un notevole impulso dovuto al progresso tecnologico ed in particolar modo all'invenzione dei calcolatori, il passato che ne relegava l'utilizzo ad episodi saltuari e in ambiti esclusivamente militari ha ceduto il posto all'era dell'informazione che l'ha scaraventata quasi a contatto con la quotidianitá. La steganografia trova oggi spazio nella tutela della privacy, dei diritti intellettuali e alcune volte anche nel mondo dell'informazione di massa. Essa é espressa nella quasi totalitá dei casi con tecniche digitali rimanendo tuttavia concettualmente identica a quella che costituiva gli esempi del passato.
Lo schema logico che sta alla base di una qualsiasi tecnica steganografica presenta tre fondamentali soggetti:

- *Il messaggio segreto* che si desidera trasmettere (si suppone una stringa di bit)
- *Il messaggio contenitore* ovvero un messaggio all'interno del quale nascondere il messaggio segreto
- *L'algoritmo steganografico* utilizzato

L'essenza della steganografia risiede nel nascondere il messaggio segreto all'interno del contenitore tramite l'algoritmo steganografico, in modo quanto piú possibile latente, al fine di rendere praticamente indistinguibile il contenitore originale da un contenitore che presenta informazione nascosta. Prima di addentrarsi nella parte tecnica é necessario chiarire le basi concettuali della materia trattata, in particolare risulta fondamentale far luce sull'esatto fine della steganografia e sui soggetti sopra descritti.

3.2 Steganografia vs Crittografia

In molti casi questi due termini vengono posti in stretta relazione tra loro e in alcuni addirittura confusi, tuttavia esistono enormi differenze sia concettuali che tecniche tra steganografia e crittografia. Sebbene il loro fine appaia analogo esso in realtá non lo é, mentre la crittografia infatti ha come scopo finale il rendere un determinato messaggio incomprensibile a chi non possegga alcune informazioni prestabilite (ad esempio una chiave di decifrazione), la steganografia si pone di nascondere l'esistenza stessa della comunicazione, nel momento in cui un intruso scoprisse una comunicazione steganografata, anche se incapace di carpirne il significato, la steganografia avrebbe fallito.

Come vedremo nei capitoli successivi, risulta tuttavia impossibile non notare una certa povertá di contenuti presente nella steganografia rispetto alla crittografia, essa infatti non ha purtroppo avuto quell'enorme spinta che il modello matematico é riuscito a dare a quest'ultima, in particolare con gli algoritmi crittografici asimmetrici. La mancanza di forti basi matematiche in relazione a qualsivoglia tecnica fanno di questa scienza, o se vogliamo branca della conoscenza, una materia relativamente povera di contenuti brillanti. La maggior parte delle tecniche steganografiche, come in seguito si potrá evincere, si basa su

un approccio *security-by-obscurity* piuttosto che su convincenti teoremi (quello che analogamente avviene ad esempio per DES); gli algoritmi steganografici dunque, per quanto complessi ed ingegnosi non sono in grado da soli di soddisfare il principio di Kerckhoff in modo decisivo, almeno fino ad oggi. Una volta compresi correttamente, i due strumenti se messi assieme ed utilizzati in modo proprio (come vedremo in seguito), riescono a fornire un livello di sicurezza importante e prospettive ancor piú interessanti.

3.3 Il messaggio contenitore

Tutte le tecniche steganografiche come abbiamo detto si avvalgono del *messaggio contenitore* o *cover* nel quale nascondere l'informazione da trasmettere, dal punto di vista del mittente che utilizza la steganografia dunque la scelta di tale contenitore, anche se non esplicitamente prevista da una determinato metodo va affrontata, sia per quanto riguarda l'aspetto tecnico che per quello umano.

Caratteristica principale é il suo significato, esso deve essere il piú possibile disgiunto dal significato dell'informazione segreta da trasmettere, ancora é preferibile che tale messaggio sia di scarsa o nulla rilevanza per coloro che eventualmente possano venirne a conoscienza, come si é detto infatti lo scopo principale della steganografia non é tanto rendere un'informazione illeggibile o indecifrabile da un eventuale intruso, quanto fare in modo che egli non sia nemmeno consapevole dell'esistenza di una qualche rilevante comunicazione. Piú in generale nella scelta del cover esistono due fondamentali obbiettivi, apparentemente opposti che é necessario perseguire:

il contenitore deve essere il piú possibile generico, ovvero deve mescolarsi e confondersi nella massa di messaggi e comunicazioni che il mezzo puó ospitare; contemporaneamente esso non deve essere troppo diffuso, é fondamentale infatti evitare assolutamente che un intruso abbia modo di possedere una copia non alterata del contenitore (ottenuto magari per ragioni di fama o eccessiva diffusione), in tal caso sarebbe semplice verificarne le differenze introdotte con la steganografia. Come per le chiavi nella crittografia é consigliabile non riutilizzare lo stesso contenitore piú volte e soprattutto distruggere quelli giá usati in una passata sessione.

Molta rilevanza ha inoltre l'*entropia di Shannon* del cover, essa ne determina la quantitá di informazione ridondata presente, indicatore principale dell'alterabilitá del contenitore in termini quantitativi e di conseguenza qualitativi, la presenza forte di tale informazione ridondata si traduce in un basso valore di entropia che permette l'inserimento di materiale steganografato con minor impatto. Infine alcune parole devono essere spese per il fattore umano che in questo campo é fondamentale : praticamente tutte le tecniche steganografiche utilizzano un messaggio contenitore destinato ad un utente umano, l'analogicitá dell'uomo infatti lo rende molto vulnerabile alla steganografia la quale trova vita proprio in quel margine di errore presente nel mondo reale e altrimenti non trascurabile nel mondo delle macchine.

In questo campo intervengono una serie di fattori sociologici, culturali e politici riferiti al mezzo e al cover che non discuretemo in questa sede in quanto non di nostra diretta competenza, ma che esistono e vanno tenuti in considerazione.

3.4 Attinenza al principio di Kerckhoff

La steganografia, pur essendo fortemente legata all'algoritmo usato, necessita ad un certo livello l'autoimposizione del *principio di Kerckhoff* che, adottato dalla crittografia afferma che la sicurezza di una determinata tecnica non deve risiedere nell'algoritmo usato (che si suppone addirittura conosciuto nei minimi dettagli da un intruso) bensí nella chiave di decifrazione.

A causa delle discusse problematiche relative a tale principio, parlando di chiavi é necessario ricorrere alla crittografia, la quale in questo caso presenta un punto d'incontro e fusione con le tecniche steganografiche, le variazioni del cover introdotte dalla steganografia infatti, seppur inpercettibili, devono apparentemente risultare (anche ad un'attenta analisi) semplici discrepanze dovute al caso; questo impone che tali modifiche debbano sembrare del tutto randomiche ed incomprensibili.

Per ottenere il suddetto risultato ci si avvale di un algoritmo crittografico codificando il messaggio originale in modo che la sequenza di bit da iniettare nel contenitore appaia del tutto casuale; come é possibile dunque evincere in questo caso tutta la sicurezza della tecnica usata si sposta sulla chiave, un eventuale intruso dovrá (supponendo noti l'algoritmo steganografico e quello crittografico usati) trovare la chiave da applicare al rumore prima di poter anche solo sapere se tali discrepanze sono effettivamente informazioni steganografate o semplici disturbi intrinsechi. Tramite la fusione di steganografia e crittografia si ottiene la congruenza con il principio di Kerckhoff, che puó rendere abbastanza sicure anche tecniche steganografiche semplici come quelle applicate alle bitmap (approfondite piú avanti nel documento).

4 Le tecniche

Come vedremo le tecniche steganografiche si differenziano principalmente in base all'algoritmo utilizzato e alla politica relativa al messaggio contenitore, esse si suddividono in *steganografia sostitutiva*, *steganografia selettiva* e *steganografia costruttiva* presentate in successione qui di seguito.

4.1 Steganografia Sostitutiva

La *steganografia sostitutiva* o *steganografia iniettiva* racchiude in se la maggior parte delle tecniche steganografiche esistenti, essa si pone di inserire l'informazione da trasmettere in un contenitore preesistente e di cui si suppone un determinato livello di bontá steganografica (vedi paragrafo *Il messaggio contenitore*). Tale contenitore viene modificato in modo piú inpercettibile possibile e spedito al destinatario, il quale si suppone abbia le informazioni per ricavare il messaggio originale (siano esse esclusivamente la conoscenza della tecnica steganografica utilizzata oppure, in aggiunta, anche una chiave di decifrazione).

Il concetto su cui si basano questo tipo di tecniche é legato al fatto che le informazioni che circolano nei normali mezzi di comunicazione come telefono, televisione o nel nostro caso reti informatiche contengono per ragioni intrinseche una qualche forma di *rumore di fondo*. Il rumore, come un disturbo di sottofondo di un telefono o gli inpercettibili difetti di un'immagine, altro non é che una quantitá di informazione inutile e molte volte fastidiosa che risulta difficile o in certi casi addirittura impossibile eliminare del tutto, essa si sovrappone al

messaggio originale alterandone le caratteristiche ed é proprio su questo rumore che agisce la steganografia, nascondendovi informazioni.

Esistono innumerevoli tecniche steganografiche piú o meno documentate applicabili a file audio, video, documenti e immagini, in particolare illustreremo qui di seguito alcuni esempi di steganografia sostitutiva applicata a queste ultime; in questo caso le tecniche utilizzate si differenziano soprattutto in relazione all'algoritmo di compressione adottato dal formato, esistono infatti dalla definizione di Kurak and McHugh[3] due fondamentali tipologie di compressione digitale: i metodi *lossless* che comprimono senza alcuna perdita d'informazione e che permettono quindi la ricostruzione perfetta dell'immagine originale (es. GIF e Bitmap) e i metodi *lossy* che invece, sebbene molto piú efficenti in termini di fattore di compressione, introducono perdita di informazione (es. JPEG).

4.1.1 Bitmap

Un modo molto semplice di nascondere informazioni in un'immagine é quello di utilizzare una bitmap. Si supponga di utilizzare un'immagine bitmap a 24bit come contenitore: ogni pixel sará codificato con 3 byte, rispettivamente i valori di Rosso, Verde e Blu (RGB), é possibile alterare i bit meno significativi di ogni valore cromatico inserendovi un determinato messaggio S. Scambiando ad esempio solamente l'ultimo bit di ogni byte e sostituendolo con i bit del messaggio da steganografare si otterrá una variazione di al piú una unitá per valore cromatico, qui visualizzata in un esempio con 2 pixel e un messaggio di 6 bit da steganografarvi:

Messaggio [101001]

$$\left\{\begin{array}{l} r = 10101100 \\ g = 11110010 \\ b = 10011001 \\ \hline\hline \\ r = 11100100 \\ g = 01000111 \\ b = 10000101 \end{array}\right\} \Longrightarrow \left\{\begin{array}{l} r = 1010110\,\mathbf{1} \\ g = 1111001\,\mathbf{0} \\ b = 1001100\,\mathbf{1} \\ \hline\hline \\ r = 1110010\,\mathbf{0} \\ g = 0100011\,\mathbf{0} \\ b = 1000010\,\mathbf{1} \end{array}\right\}$$

l'alterazione creata non modificherá in modo rilevante la percezione complessiva dell'immagine variandola di pochissimo rispetto all'originale; prendendo come esempio una bitmap con risoluzione 800x600 sará possibile nascondervi 800*600*3 bit, ovvero 180 KB di messaggio.
Per rafforzare la tecnica é possibile diradare l'alterazione in modo piú o meno pesante secondo una sequenza prestabilita tanto da rendere le variazioni cromatiche meno evidenti (si potrebbe ad esempio pensare di introdurre variazioni ogni n pixel oppure ogni $f(n)$ con f arbitraria).

La vulnerabilitá di questa tecnica rimane ovviamente la sua estrema semplicitá nonché l'oramai bassissima diffusione di tali formati di immagine in rete e la loro relegazione a formato di supporto in ambienti applicativi ristretti (photo

[3] [Kurak92]

editing ecc...), queste caratteristiche ne fanno una tecnica steganografica quasi esclusivamente didattica.

4.1.2 GIF e formati indexed

Esistono formati di memorizzazione di immagini molto comuni che si basano sull'utilizzo di *palette* o tavolozze, in questi casi non viene memorizzata l'immagine punto per punto, bensí essa associa ad ogni pixel un indirizzo di un valore cromatico posto in una tavola di colori prestabilita, supponendo quindi una palette di 256 colori, saranno sufficenti 8 bit per pixel per la memorizzazione. Questa tecnica presa singolarmente non offre possibilitá di risparmio in termini di dimensioni, tuttavia é stata ampiamente usata in passato a causa del supporto in hardware delle tavolozze nelle vecchie schede video e rimane tutt'oggi ampiamente usata. Un esempio di utilizzo di tale tecnica é il formato *GIF (Graphic Interghange Format)* che memorizza immagini attraverso palette a cui viene aggiunta una compressione con LZW (Lempel-Ziv-Welch, un algoritmo che preserva completamente l'informazione o *lossless*).

Le opportunitá steganografiche offerte da una GIF sono interessanti, supponendo infatti di alterare la tavolozza diminuendone la quantitá effettiva di colori presenti e sostituendoli con colori il piú possibile simili ma non identici ad altri rimanenti si crea una ridondanza nell'immagine che da l'opportunitá alla steganografia di intervenire, in questo caso infatti abbiamo una possibilitá di scelta per quanto riguarda gli indirizzi, che in una tavolozza ipoteticamente ridotta da 256 a 128 colori si traduce nell'avere due valori di colore simili con cui rappresentare la stessa informazione; a questo punto basterá associare il valore 0 e 1 ai rispettivi colori simili per steganografare un messaggio. Supponiamo di ridurre un'ipotetica palette da 16 a 8 colori:

$$\left\{\begin{array}{cccc} (&0&0&0&) \\ (&255&0&0&) \\ (&0&255&0&) \\ (&0&0&255&) \\ (&128&0&0&) \\ (&0&128&0&) \\ (&0&0&128&) \\ (&128&0&128&) \end{array}\right. \left.\begin{array}{cccc} (&128&128&0&) \\ (&128&0&32&) \\ (&64&128&64&) \\ (&64&32&0&) \\ (&128&0&80&) \\ (&255&32&128&) \\ (&32&32&8&) \\ (&255&255&255&) \end{array}\right\} \Rightarrow \left\{\begin{array}{cccc} (&0&0&0&) \\ (&255&0&0&) \\ (&0&255&0&) \\ (&\mathbf{0}&\mathbf{0}&\mathbf{129}&) \\ (&\mathbf{128}&\mathbf{0}&\mathbf{31}&) \\ (&\mathbf{0}&\mathbf{254}&\mathbf{0}&) \\ (&0&0&128&) \\ (&128&0&128&) \end{array}\right. \left.\begin{array}{cccc} (&\mathbf{253}&\mathbf{1}&\mathbf{0}&) \\ (&\mathbf{128}&\mathbf{0}&\mathbf{127}&) \\ (&\mathbf{1}&\mathbf{255}&\mathbf{1}&) \\ (&64&32&0&) \\ (&128&0&80&) \\ (&\mathbf{255}&\mathbf{254}&\mathbf{254}&) \\ (&\mathbf{0}&\mathbf{1}&\mathbf{0}&) \\ (&255&255&255&) \end{array}\right\}$$

Ora i colori reali sono solamente 8 a causa dei colori ridontati introdotti al posto di quelli persi, mentre quelli nella palette rimangono 16 permettendo l'utilizzo della steganografia.

Questa tecnica seppur non trascurabile presenta parecchi problemi legati al fatto che risulta semplice analizzare tramite un programma la palette di un' immagine che si suppone steganografata per individuarne associazioni di colori simili ed eventuali anomalie annesse, questo problema la rende una tecnica parecchio vulnerabile seppur relativamente ingegnosa e la relaga all'utilizzo esclusivamente per immagini in scala di grigi.

Un'altro aspetto legato all'utilizzo di palette é la loro permutabilitá, ovvero la possibilitá di variare l'ordine dei colori modificando contamporaneamente i puntatori in modo da ottenere una stessa immagine finale; con questo meccanismo si ha la possibilitá avere, in una palette di 256 colori ad esempio, 256! possibili permutazioni ovvero 256! messaggi potenzialmente steganografabili,

se ne decuce che risulta possibile nascondere log(256!) bit (210 byte) in una gif in modo totalmente indipendente dalla risoluzione (anche in un'icona 16x16 ad esempio), offrendo un'enorme rapporto informazione-contenitore in termini quantitativi.

Le tecniche appena illustrate sono tra le piú usate e diffuse e, se in congiunto con la crittografia, si possono considerare metodi steganografici abbastanza affidabili, tuttavia risulta facile che anomalie della palette (colori in disordine o simili tra loro) vengano notate con facilitá provocando il fallimento della steganografia.

Da notare infine che tutte le tecniche sopra elencate sono applicabili solamente a formati che utilizzano algoritmi di compressione lossless come appunto LZW nelle GIF.

4.1.3 JPEG

Il formato *JPEG (Joint Photographic Experts Group)* necessita di tecniche steganografiche completamente diverse da quelle utilizzate per le GIF e formati bitmap semplici in quanto adotta vari livelli di compressione dell'immagine ma soprattutto utilizza un algoritmo di compressione *lossy* quale *DCT (Discrete Cosine Transform)* che introduce una perdita di informazione a causa di varie approssimazioni esplicitamente volute dal formato, e che impediscono l'introduzione di informazione stegangrafata precedentemente o successivamente.

La principale tecnica consiste nel modificare i coefficenti dei coseni ottenuti dalla trasformata con una tecnica molto simile a quella applicata sulle bitmap. Vediamo in particolare di cosa si tratta illustrando innanzitutto l'algoritmo di compressione e di conseguenza le tecniche steganografiche annesse. Il formato JPEG si basa su un concetto fondamentale (dimostrato a livello medico/scientifico):

> *l'occhio umano risulta molto piú sensibile alla luminositá che al colore, le informazioni relative ad esso possono essere quindi in buona parte trascurate.*

La compressione dell'immagine prevede vari step che analizzeremo di seguito, alcuni di essi, non essendo argomento trattato in questa sede, sono stati volontariamente trascurati e verranno semplicemente accennati. Vediamo i vari passaggi:

- *Conversione da RGB a YCbCr*

  suppendo di avere in ingresso un'immagine in RGB a 24bit, essa viene ricodificata nel formato YCbCr ovvero per ogni terna di valori cromatici viene calcolato il coefficente di luminositá Y e i coefficenti cromatici Cb (Blu/Giallo) e Cr (Rosso/Verde). Nel caso in cui si desideri un'immagine in scala di grigi sará sufficente lavorare esclusivamente sul fattore Y.

- *Subsampling cromatico*

  si fondono i valori cromatici di ogni quattro pixel successivi prendendone la loro media (é possibile farlo di conseguenza al principio sopra espresso), in questo modo vengono eliminati i 2/3 di

ogni pixel per 3/4 dei pixel totali, ovvero l'immagine si riduce esattamente di metá in termini di dimensioni. A questo punto i fattori cromatici vengono ulteriormente subcampionati di un fattore 8 (da notare anche qui l'apparente eccessiva approssimazione). Questo porta ad avere i due canali cromatici con una granularitá di 8x8 pixel che, presi singolarmente risultano estremamente degradati mentre il fattore luminositá percorre i suddetti passi inalterato.

- *DCT - Discrete Cosine Transform*

  all'immagine viene ora applicata una trasformata coseno discreta 8x8 blocchi per volta per ogni canale, trasformando i valori dal dominio cromatico/luminoso al dominio delle frequenze, il concetto é quello analogo alla trasformata di Fourier utilizzata per i domini del tempo. Si supponga l'immagine A costituita da NxM pixel, per ogni locazione k_1, k_2 si ottiene il rispettivo coefficente :

$$B_{k_1,k_2} = \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} 4 \cdot A(i,j) \cos\left[\frac{\pi \cdot k_1}{2 \cdot N}(2i+1)\right] \cos\left[\frac{\pi \cdot k_2}{2 \cdot M}(2j+1)\right]$$

  I 64 coefficenti ricavati dai 64 valori indicano, tangibilmente parlando, la variazione nell'ambito spaziale del colore o dell'intensitá luminosa dell'immagine, tali valori sono disposti in ordine crescente rispetto alla frequenza a cui fanno riferimento partendo dall'angolo in alto a sinistra, un coefficente grande indica che la variazione é concentrata prevalentemente su quella frequenza, ad esempio un coefficente grande per una frequenza bassa indica che il colore varia in modo prevalentemente lento rispetto al piano dell'immagine, un coefficente grande in corrispondenza di una frequenza alta indica che l'immagine presenta forti variazioni di colore su spazi ridotti. Ecco come risulta possibile passare dalla matrice di valori a quella di coefficenti DCT:

$$\left\{\begin{array}{cccccccc} 139 & 144 & 149 & 153 & 155 & 155 & 155 & 155 \\ 144 & 151 & 153 & 156 & 159 & 156 & 156 & 156 \\ 150 & 155 & 160 & 163 & 158 & 156 & 156 & 156 \\ 150 & 161 & 162 & 160 & 160 & 159 & 159 & 159 \\ 159 & 160 & 161 & 162 & 162 & 155 & 155 & 155 \\ 161 & 161 & 161 & 161 & 160 & 157 & 157 & 157 \\ 162 & 162 & 161 & 163 & 162 & 157 & 157 & 157 \\ 162 & 162 & 161 & 161 & 163 & 158 & 158 & 158 \end{array}\right\} \Rightarrow \left\{\begin{array}{cccccccc} 1260 & -1 & -12 & -5 & 2 & -2 & -3 & 1 \\ -23 & -17 & -6 & -3 & -3 & 0 & 0 & 1 \\ -11 & -9 & -2 & 2 & 0 & -1 & -1 & 0 \\ -7 & -2 & 0 & 1 & 1 & 0 & 0 & 0 \\ -1 & -1 & 1 & 2 & 0 & -1 & 1 & 1 \\ 2 & 0 & 2 & 0 & -1 & 1 & 1 & -1 \\ -1 & 0 & 0 & -1 & 0 & 2 & 1 & -1 \\ -3 & 2 & -4 & -2 & 2 & 1 & -1 & 0 \end{array}\right\}$$

  L'esempio mostrato evidenzia come in questo caso in corrispondenza di alte frquenze (in basso a destra) i coefficenti siano molto ridotti o addirittura tendenti a zero, caratteristiche tipiche di un'immagine reale come puó essere una fotografia; questo rispecchia un po' il lento ed uniforme flusso di colori presente in natura che caratterizza il mondo che ci circonda. Quest'ultima operazione, previo approssimazioni numeriche é reversibile

(con IDCT - Inverse Discrete Cosine Transform, usata per decomprimere) ma é proprio qui che si concentra la compressione principale del JPEG che introduce perdita di informazione.

- *Quantizzazione*

  A questo punto abbiamo ottenuto il nostro blocco 8x8 di valori nel dominio della frequenza, é ora possibile agire sui coefficenti delle alte frequenze tramite un metodo di divisione-approssimazione di tali valori: una volta scelta una matrice detta *tavola di quantizzazione* con valori piú alti in corrispondenza delle frequenze che si vogliono eliminare si procede con la divisione e l'arrotondamento dei coefficenti (la matrice scelta varia in base al fattore di compressione desiderato e di conseguenza alla qualitá dell'immagine voluta, espressa in genere in percentuale) come di seguito:

$$Coefficenti: \begin{Bmatrix} 1260 & -1 & -12 & -5 & 2 & -2 & -3 & 1 \\ -23 & -17 & -6 & -3 & -3 & 0 & 0 & 1 \\ -11 & -9 & -2 & 2 & 0 & -1 & -1 & 0 \\ -7 & -2 & 0 & 1 & 1 & 0 & 0 & 0 \\ -1 & -1 & 1 & 2 & 0 & -1 & 1 & 1 \\ 2 & 0 & 2 & 0 & -1 & 1 & 1 & -1 \\ -1 & 0 & 0 & -1 & 0 & 2 & 1 & -1 \\ -3 & 2 & -4 & -2 & 2 & 1 & -1 & 0 \end{Bmatrix}$$

$$Tavola\ di\ quantizzazione: \begin{Bmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{Bmatrix}$$

$$Coefficenti\ quantizzati: \begin{Bmatrix} 79 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ -2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{Bmatrix}$$

  In questo modo si va ad eliminare l'influsso delle alte frequenze sull'immagine, si pensi di levigare matematicamente un'onda di forma sinusoidale ricoperta di increspature rendendola piú liscia ed armoniosa. É proprio questo punto che presenta la parte lossy dell'algoritmo, qui vengono irrimediabilmente perse informazioni ed é solo da qui in poi che é possibile agire con la steganografia.

- *Riordino a ZIG-ZAG*

  La matrice di valori viene riorganizzata seguendo un'ordine a zig-zag partendo dall'angolo in alto a sinistra per il semplice fatto di accumulare gli zeri verso la fine in modo da ottimizzare i successivi processi di compressione questa volta *lossless*.

- *Lossless compression*

  A questo punto si utilizzano alcuni algoritmi lossless che in questa sede ci limiteremo ad accennare in quanto non rilevanti per la steganografia; si tratta di una compressione iniziale con RLE (Run-Length Encoding) indirizzata soprattutto ai coefficenti di bassa frequenza, seguita da un applicazione di DPCM (Differential Pulse Code Modulation) atta a comprimere i primi coefficenti delle frequenze piú alte, per finire con un classico codice Huffman il cui albero viene memorizzato all'inizio del file JPEG.

Vediamo ora una tecnica per steganografare informazioni all'interno di un'immagine compressa con questo algoritmo. Come abbiamo detto in precedenza lo stadio chiave per la steganografia é la quantizzazione successiva al DCT, é possibile qui inserire informazioni nei primi coefficenti (purché maggiori di 1) con il metodo del *Least Significant Bit* illustrato parlando delle bitmap. Questa tecnica é utilizzata da parecchi famosi programmi di steganografia, primo tra tutti *JSTEG*[4], il quale inserisce nell'ultimo bit dei primi 5 coefficenti la *dimensione [A] del valore che indica la lunghezza in bit del testo steganografato*, quindi nei successivi *[A]* bit indicati memorizza la dimensione del messaggio presente *[N]*, infine nei seguenti *[N]* bit viene steganografato il messaggio effettivo come illustrato nello schema qui di seguito:

$$
\begin{aligned}
A &= a_0a_1a_2a_3a_4 \\
N &= n_0n_1n_2n_3n_4 \ldots n_{A-1} \\
M &= m_0m_1m_2m_3m_4 \ldots m_{N-1}
\end{aligned}
$$

$$
\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & \ldots & A-1(+5) & A(+5) & A+1(+5) & A+2(+5) & A+3(+5) & \ldots & N-1+(A+5) \\ a_0 & a_1 & a_2 & a_3 & a_4 & n_0 & n_1 & n_2 & n_3 & n_4 & \cdots & n_{A-1} & m_0 & m_1 & m_2 & m_3 & \cdots & m_{N-1} \end{pmatrix}
$$

Come é possibile vedere il numero A formato dai primi 5 bit codificati determina di quanti bit é formato il valore N di grandezza del messaggio, questo a sua volta rappresenta la grandezza effettiva dell'informazione steganografata, memorizzata di seguito.

[4] http://www.theargon.com/archives/steganography/DOS/jsteg.zip

4.2 Steganografia selettiva

Questo tipo di approccio alla steganografia si basa, invece che sull'attivitá di modifica del messaggio contenitore, sulla *selezione* dello stesso effettuata in base allo specifico messaggio segreto che si desidera steganografare. In pratica tale tecnica consiste in una ricerca esaustiva di un cover che presenti una steganografia naturale nell'esatto modo voluto, ad esempio con gli ultimi bit dei byte che rappresentano giá il messaggio segreto; per fare questo si utilizzano delle funzioni ausiliare che verificano la bontá di una serie di contenitori presi in esame, indicando in output il contenitore che soddisfa i requisiti richiesti; a questo punto la modifica non é necessaria e il messaggio contenitore si presenta del tutto intoccato rendendo inefficaci le tecniche di analisi delle anomalie.

Tale tecnica risulta per ovvi motivi molto valida dal punto di vista della sicurezza, non é possibile affermare altrettanto invece per l'efficenza, la ricerca esaustiva e potenzialmente infinita ne fa una tecnica eccessivamente dispendiosa ed utilizzabile solo per steganografare messaggi molto brevi (che aumentano la probabilitá di trovare il contenitore opportuno). Tutti questi svantaggi la relegano a tecnica il piú delle volte esclusivamente teorica.

4.3 Steganografia costruttiva

Nella steganografia costruttiva l'approccio non é piú quello di *modificare* il rumore del contenitore, bensí quello di *costruire* un modello quanto piú accurato del rumore stesso in modo tale da poterlo generare a proprio piacimento ed inserirlo nel cover. La creazione di un modello di rumore risulta peró parecchio complessa e dispendiosa in termini di risorse. In questo caso tutta la forza della tecnica si sposta sul modello utilizzato ed é proprio qui che si concentrano i problemi di questo approccio: chiunque disponesse di maggiori risorse infatti sarebbe potenzialmente in grado di costruirsi un modello piú accurato del rumore riuscendo a distinguere il messaggio steganografato dal segnale randomico, da qui si evince l'aspetto speculare di questa tecnica, la costruzione di un modello di rumore piú accurato non si limita a portare il fallimento della precedente tecnica, ma introduce essostesso un nuovo metodo per la steganografia e si dimostra quindi un'arma a doppio taglio. La steganografia costruttiva rimane un'ambito tuttoggi ancora prettamente sperimentale.

5 Watermarking

Che il giudizio personale sia positivo o negativo é necessario dire che, soprattutto con l'attuale boom del business su Internet e delle reti peer-to-peer, fondamentale importanza ha per produttori e distributori di software e musica la tutela del copyright.

Per quanto riguarda la steganografia un grosso impulso vi é stato dato negli ultimissimi tempi proprio dalla grande distribuzione di prodotti multimediali, tali soggetti economici infatti hanno adottato tecniche steganografiche per inserire licenze o parti di esse all'interno del software distribuito atte a garantirne l'autencicitá proteggendolo quindi, in modo piú o meno affidabile dalla pirateria. In questi casi non solo questa forma di copyright viene inserita all'interno del media, ma si adottano particolari tecniche che la rendono parte intrinseca del cover su cui viene steganografata, tanto da danneggiarlo o addirittura renderlo inutilizzabile in caso di estrazione.
Questo fenomeno avveniva giá precedentemente con software prettamente steganografico come *MP3Stego* (che in questa sede per modivi di spazio non approfondiremo, vedasi Bibliografia) ma per ragioni prettamente tecniche relative all'algoritmo di compressione; con il Watermarking si tende ad allargare questo comportamento a tutti i formati su cui si necessiti una tutela dei diritti intellettuali.

Nonostante gli sforzi per mantenere la politica del *security-by-obscurity* compiuti dalle *major* tuttavia, esiste parecchio software per la rilevazione ed il benchmark di algoritmi per il watermarking, primo tra tutti *StirMark*[5] di Fabien A. P. Petitcolas che permette di individuare statisticamente la presenza di watermarking in modo assolutamente generico ed indipendente dall'algoritmo.

Per ragioni di dimensioni questo capitolo voleva essere solamente un cenno al Watermarking che potrá eventualmente essere approfondito dal lettore tramite la bibliografia.

[5] http://www.petitcolas.net/fabien/watermarking/stirmark/index.html

6 Conclusioni e prospettive

6.1 Il futuro: dove stiamo andando

Come si é detto i metodi attualmente utilizzati nella steganografia sono fortemente basati su un modello *security-by-onscurity*, le prospettive future riguardano la speranza di un approccio piú matematico alle tecniche steganografiche, come accaduto per la crittografia con gli algoritmi a chiave pubblica, un modello cioé che dia una forte spinta in termini di affidabilitá a tutti gli algoritmi steganografici. Relativamente ad un piú remoto futuro inoltre, le prospettive si spostano soprattutto sui modelli derivati dalla fisica quantistica; tali modelli, giá applicati in modo tangibile con successo per la crittografia sembrano destinati a trovare impiego anche nella steganografia, come a voler sfruttare l'universo stesso e la materia che lo compone come principale soggetto della steganografia.

6.2 Considerazioni personali

Tra le innumerevoli prospettive che, per quanto riguarda questa materia, abbiamo potuto osservare ed immaginare, una di queste ci sembra particolarmente interessante: il concetto risiede nello sfruttare la steganografia come mezzo di arricchimento dell'informazione e non piú come metodo di occultamento. Un esempio potrebbe essere quello di inserire all'interno di materiale multimediale come file audio e video, informazioni aggiuntive di qualsivoglia natura relative ad esempio a *titolo* e *autore* dell'opera e cosí via, non piú informazioni segrete o copyright ma dati utili disponibili all'utente memorizzati in modo estremamente elegante.

Infine alcuni degli errori dattilografici presenti in questo testo non sono dovuti al caso: l'interesse da noi scoperto per la materia trattata ci ha portato ad effettuare alcuni esperimenti relativi a tecniche steganografiche, in particolare abbiamo concepito un piccolo e semplice algoritmo da utilizzare per testo scritto tramite il quale abbiamo steganografato un breve messaggio all'interno di questo stesso documento.

La semplicissima tecnica consiste nel codificare i bit del messaggio nel cover tramite i caratteri *apice*, tale carattere puó essere sostituito da un *apostrofo* molto simile, in modo da rappresentare i due valori binari (nel nostro caso apice per 0 e apostrofo per 1), il termine del messaggio infine viene rappresentato con un carattere (in questo caso volutamente visibile) come la *tilde*. Lasciamo al lettore munito di pazienza la facoltá di scoprire il messaggio nascosto...

7 Bibliografia

- Simon Singh, *Codici e segreti (The Code Book)* - BUR saggi, Febbraio 2002
- Neil F. Johnson and Sushil Jajodia, *Steganography: Seeing the Unseen* - IEEE Computer, February 1998: 26-34.
- Neil F. Johnson and Sushil Jajodia, *Steganalysis of Images Created using Current Steganography Software* - Workshop on Information Hiding Proceedings, Portland, Oregon, USA, 15 - 17 April 1998.
- Charles Kurak, John McHugh, *Cautionary Note On Image Downgrading* - IEEE Eighth Annual Computer Security Applications Conference. 1992.
- Stefan Katzenbeisser and Fabien A. P. Petitcolas, *Information hiding techniques for steganography and digital watermarking* - Artech House Books, ISBN 1-58053-035-4, December 1999.
- Stirmark - strumento generico per test sulla robustezza di algoritmi di watermarking su immagini
  http://www.petitcolas.net/fabien/watermarking/stirmark/index.html
- MP3Stego - software per la steganografia di file in formato MP3
  http://www.petitcolas.net/fabien/steganography/mp3stego/
- The information hiding homepage
  http://www.petitcolas.net/fabien/steganography/
- Analisi dell'algoritmo usato da JSTEG
  http://www.guillermito2.net/stegano/jsteg/
- Stegoarchive
  http://www.stegoarchive.com/
- Bibliografia e articoli
  http://www.jjtc.com/Steganography/
- Statistical steganalisys
  http://niels.xtdnet.nl/stego/
- Panoramica sulla steganografia (in italiano)
  http://www.tonycrypt.com/Crittografia/Stegano.htm
- Watermarking mailing list
  http://www.watermarkingworld.org/ml.html