Steganografi

a

L'arte della scrittura nascosta

Graziella

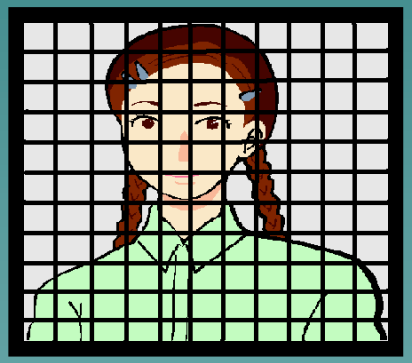
Etimologia

_____ (***stego*, nascondere**) + _____ (*graphein*, scrivere)

Si nasconde non tanto il contenuto (come nel caso della crittografia), quanto l'esistenza stessa della comunicazione agli occhi di un eventuale osservatore, tradizionalmente denominato"nemico".

Origini

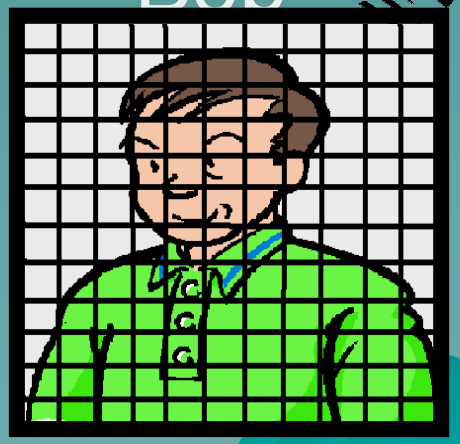
Nel 1983 Simmons formulò il "Problema dei prigionieri".



Alice

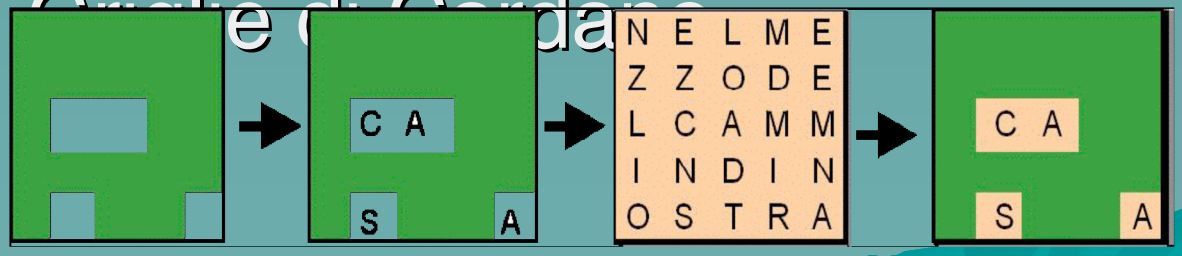
Willie

Bob



Un po’ di storia (1)

- Erodoto racconta…
  1. tavolette di cera
  2. cranio tatuato
- In Cina si usavano delle striscioline di seta sulle quali veniva scritto il messaggio; queste dopo essere state appallottolate e ricoperte di cera, venivano ingoiate dal messaggero
- Griglie di Cardano



Un po' di storia (2)

- Shakespeare VS Bacon
- Durante la seconda guerra mondiale si usò la tecnica delle Cifre Nulle

Esempio

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

Considerando in sequenza la seconda lettera di ogni parola, si ottiene il messaggio:

"pershing sails from NY June 1"

Un po’ di storia (3)

-
- Inchiostri invisibili
- Il direttore dell’F.B.I. inventò la Tecnica dei micropunti
- Le immagini di Al-Queda

Modelli steganografici

Steganografia iniettiva

Modelli steganografici

Steganografia generativa

Un’altra classificazione…(1)

Steganografia sostitutiva _ ci si basa sul fatto che in un qualsiasi canale di comunicazione sono sempre presenti dei rumori. Il messaggio viene nascosto in questi rumori.

Precauzioni

1. non bisogna mai usare file pubblici o facilmente accessibili
2. non bisogna mai usare più volte lo stesso file come contenitore

Svantaggi _ le sostituzioni possono alterare le caratteristiche statistiche del rumore nel media utilizzato.

Un’altra classificazione…(2)

Steganografia selettiva _ ha valore puramente teorico e non viene utilizzato in pratica. Essa si basa sull’idea di procedere per tentativi fino a quando non si verifica una certa condizione

Vantaggi _ l'immagine ottenuta contiene effettivamente il messaggio segreto, ma non è stata modificata.

Svantaggi _ questa soluzione è inaccettabile perché è molto dispendiosa in termini di tempo ed oltretutto permette di nascondere una quantità d'informazione molto modesta.

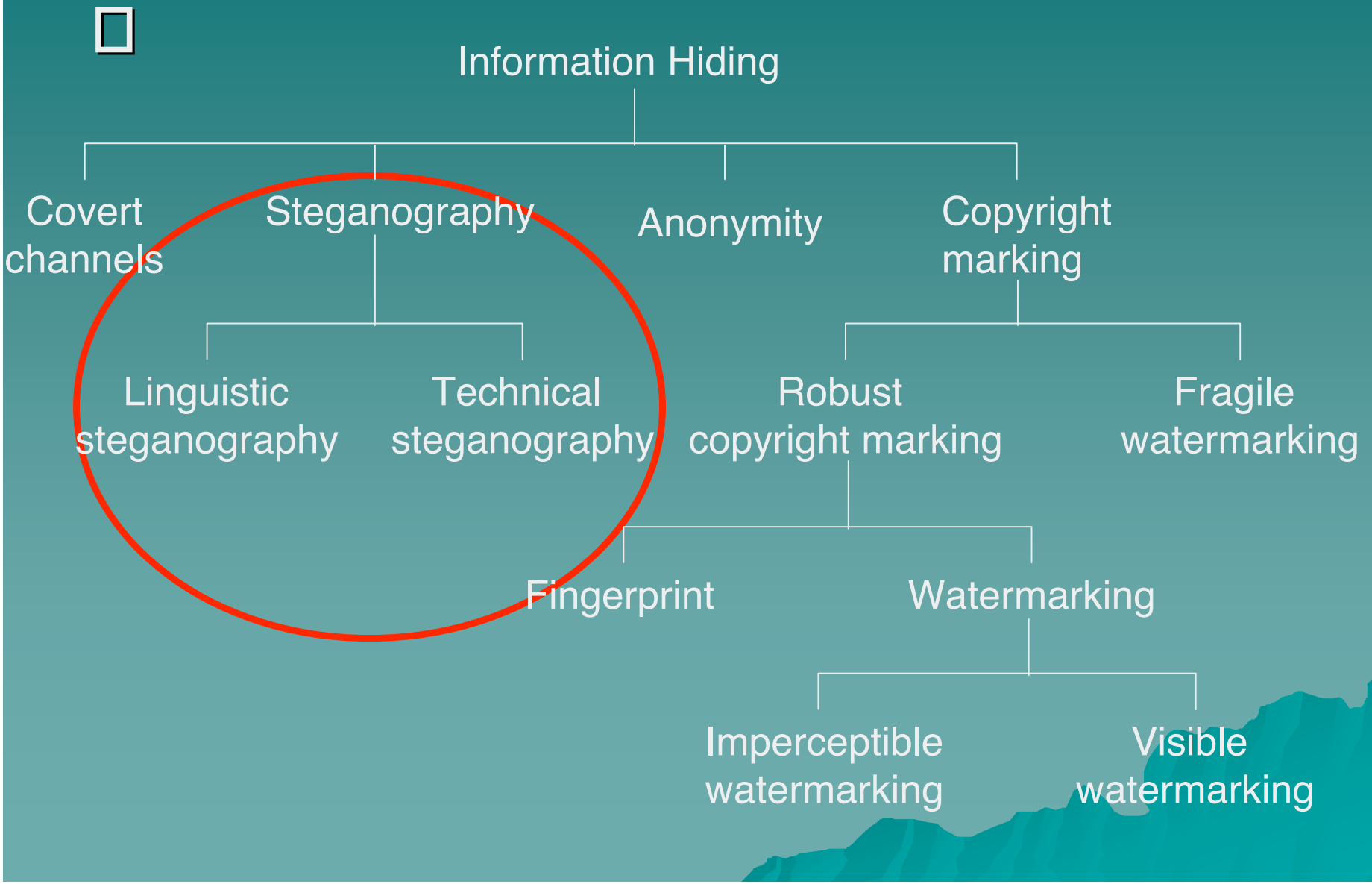
Un’altra classificazione…(3)

Steganografia costruttiva _ nel modificare il file contenitore si tenta di sostituire il rumore presente nel media utilizzato con il messaggio segreto nel rispetto delle caratteristiche statistiche del rumore originale.

Svantaggi:

1. non è facile costruire un modello del rumore, ed anche se lo si costruisce è possibile che qualcun altro ne abbia costruito uno più accurato e quindi sia in grado di scorgere comunque la presenza di un messaggio segreto.
2. se il modello utilizzato cadesse nelle mani del nemico, egli lo potrebbe analizzare per cercarne i punti deboli. In questo modo si

Data hiding (1)



Data hiding (2)

Occultamento dei dati nei seguenti oggetti:

- File di testo
- Immagini
- File audio

Due tipologie:

- Necessari sia il documento originale che quello modificato
- Non serve l'aiuto del documento originale

Steganografia testuale – Il codice di Trithemius

1462-1516 Johannes Trithemius

1518
Poligraphiae Libri Sex

1499
Steganographia
(inserito nella lista dei libri proibiti nel 1609)

Il codice di Trithemius - Steganographia

Libri I e II _ metodi per nascondere messaggi all'interno di scritture più composite e a volte prive di significato

Esempio

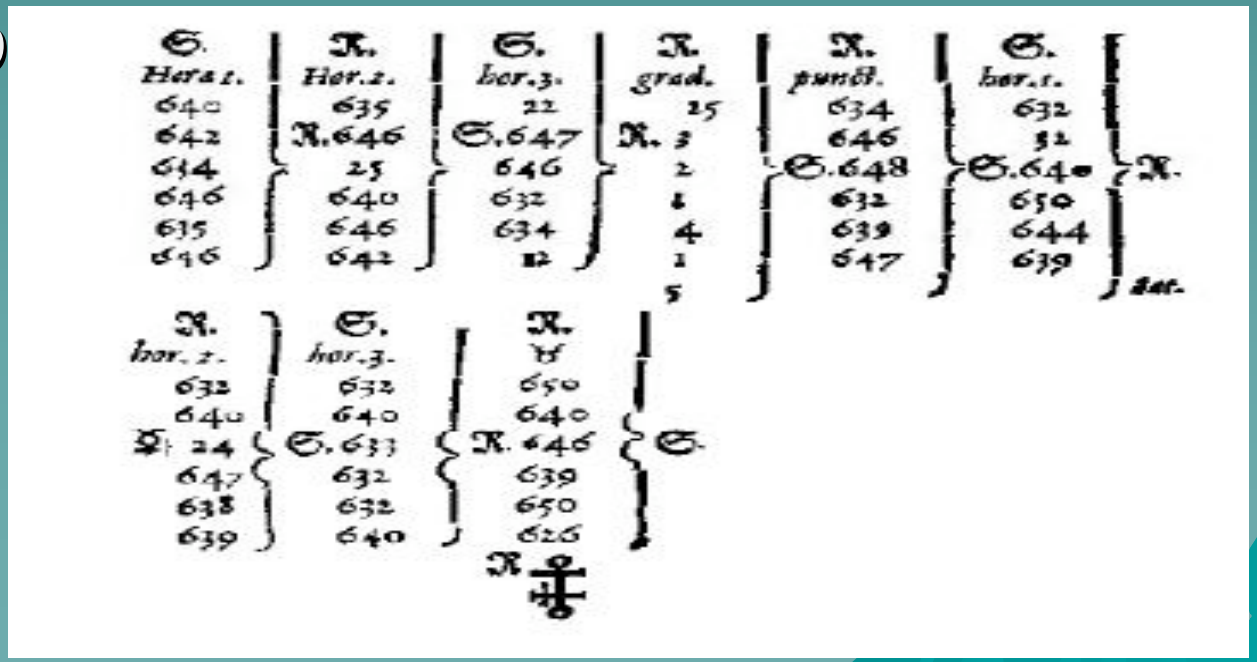
Sistema Crittografico

Leggendo una lettera no e una sì e saltando una

Sum tali cautela ut . . .

Il codice di Trithemius - Steganographia

Libro III _ apparentemente è un libro di astrologia occulta: è composto da colonne di numeri sovrastati da simboli zodiacali e planetari; molti hanno concluso che fosse solo un manuale di o

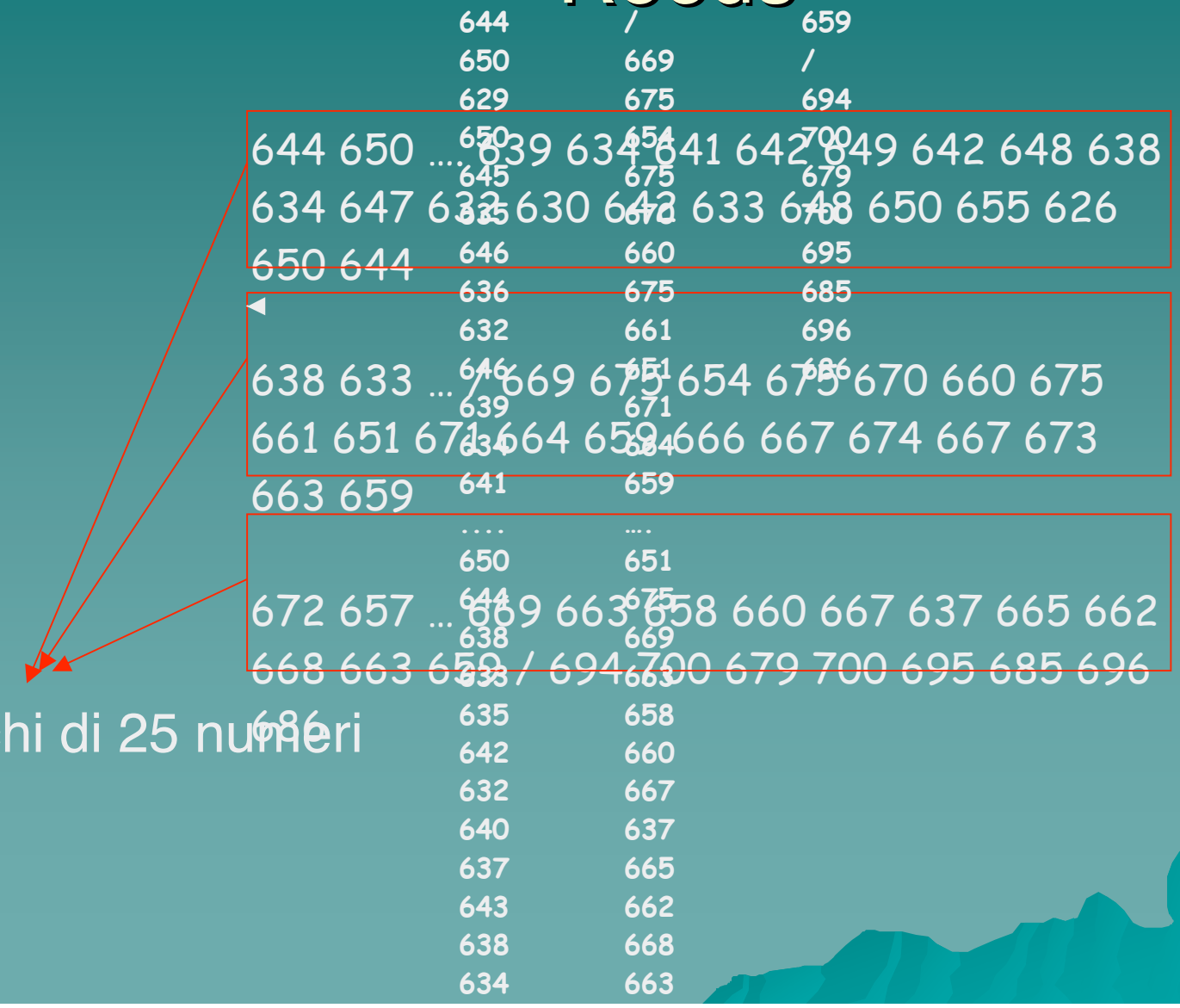


Il codice di Trithemius – Steganographia

1996 Thomas Ernst pubblica un articolo che risolve il mistero ma non suscita interesse

Ma la vera svolta l'abbiamo con il matematico crittoanalista Jim Reeds…

Il codice di Trithemius – Steganographia… la soluzione di Reeds



Blocchi di 25 numeri

Il codice di Trithemius – Steganographia… la soluzione di Reeds

644 650 …. 639 634 641 642 649 642 648 638 634 647 632 630
642 633 648 650 655 626 650 644 638 633 … / 669 675 654 675
670 660 675 661 651 671 664 659 666 667 674 667 673 663 659
672 657 … 669 663 658 660 667 637 665 662 668 663 659 / 694
700 679 700 695 685 696 686 686 632 696 … / 719 725 704 725
720 710 721 711 707 721 …

Primi 160 numeri

Il codice di Trithemius – Steganographia… la soluzione di Reeds

4 blocchi da 40 numeri

644 650 629 650 645 635 646 636 632 646 . . .

+ 25

669 675 654 675 670 660 675 661 651 671 . . .

694 700 679 700 695 685 696 686 632 696 . . .

719 725 704 725 720 710 721 711 707 721 . . .

Il codice di Trithemius – Steganographia… la soluzione di Reeds

1 626	X 631	Q 636	L 641	E 646
O 627	V 632	P 637	J 642	D 647
U 628	T 633	C 638	H 643	Z 648
I 629	S 634	N 639	G 644	B 649
Y 630	R 635	M 640	F 645	A 650

Il codice di Trithemius – Steganographia… la soluzione di Reeds

644 650 629 650 645 635 646 636 632 646 639 634
G A Z A F R E Q U E N S

641 642 649 642 648 638 634 647 632 630 642 633
L I B I C O S D U Y I T

648 650 635 626 650 644 638 650 633 635 642 632
C A R _ A G O A T R I U

640 637 643 638 634
M P H O S

Il codice di Trithemius – Steganographia… la soluzione di Reeds

Una serie di fortuite coincidenze e intuizioni lo spinsero nella giusta direzione

641 650 629 650 645 635 646 636 632 646 639 634
G A Z A F R E Q U E N S

- _ _ insieme “sch”

641 642 649 642 648 638 634 647 632 630 642 633
L I B I C O S D U X I T

- quella che lui credeva una “x” in realtà era la “w”

648 650 635 626 650 644 638 650 633 635 642 632
C A R TH A G O A T R I U

- _ _ digramma “tz”

640 637 643 638 634
M P H O S

- _ _ digramma “th”

- quella che nell’alfabeto cifrato era la “y” in realtà era una “x”

Il codice di Trithemius – Steganographia… la soluzione di Reeds

Th	Sch	Tz	Z	X	W	U	T	S	R	Q	P
01	02	03	04	05	06	07	08	09	10	11	12
26	27	28	29	30	31	32	33	34	35	36	37
51	52	53	54	55	56	57	58	59	60	61	62
76	77	78	79	80	81	82	83	84	85	86	87

O	N	M	L	I	H	G	F	E	D	C	B	A
13	14	15	16	17	18	19	20	21	22	23	24	25
38	39	40	41	42	43	44	45	46	47	48	49	50
63	64	65	66	67	68	69	70	71	72	73	74	75
88	89	90	91	92	93	94	95	96	97	98	99	00

Il codice di Trithemius – Ma vediamolo in pratica…

Supponiamo di voler avvertire un nostro amico Tizio di fidarsi di un certo Caio…
…usando la Steganografia scriviamo…

**"Nelle ore notturne feroci illusioni di antichi riti tramandati
in dimenticate isole ci assalgono, ivi ora . . ."**

Tizio per leggere il nostro messaggio non deve far altr
Leggere tutte le iniziali delle parole e comporre il mess
nascosto

"**Non fidarti di caio**"

Il codice di Trithemius – Ma vediamolo in pratica…

Quello di prima era uno degli esempi più semplici…Trithemius infatti utilizzò anche dei dischi rotanti basati sulla sostituzione monoalfabetica di Cesare

Scriviamo quindi il seguente messaggio…

“*MioΨ**z**ioΨ Ψ**a**ndatoΨaΨ**Z**urigoΨnonΨ**p**erΨunΨ**s**empliceΨincontroΨ**n**otturnoΨdiΨ**k**arate,Ψquindi **d**omaniΨsiΨ**f**ar ΨilΨ**s**olitoΨgirettoΨ**n**elΨcentroΨ**s**torico.ΨDovrebbeΨ**m**andarmiΨunΨ**k**imonoΨper **s**abato,ΨeΨ**a**llora. ..*”

Usando però la trasposizione che muta la “a” in “z” [illegible] ottengo la seguente frase…

“**zaZpsnkdfsnsmksa**” “[illegible]”

La steganografia ai giorni nostri

Le parole cifrate vengono nascoste all'interno del docur
modificandone alcune caratteristiche.

Metodi di codifica:

- Codifica line – shift
- Codifica word – shift
- Codifica feature

Codifica Line - Shift

Le righe di testo vengono spostate verticalmente di pochi millim
in su o in giù.

Svantaggi:

- È certamente visibile per un lettore esperto
- Un'operazione di rispaziatura casuale o uniforme delle r
  del testo danneggerebbe ogni successivo tentativo di ril
  la modifica

Vantaggi:

- Se un documento in forma cartacea fosse contrassegna
  tale codifica risulterebbe piuttosto sicuro
- Se il testo in esame fosse una fotocopia sarebbe ancora
  difficile risalire al messaggio dal momento che si potrebb
  incappare anche in macchie o nel tipico effetto pepe - sa
  proprio delle macchine fotocopiatrici.

Codifica Word - Shift

Si trasferiscono le posizioni orizzontali delle parole all'interno de
righe di testo

Svantaggi:

- È applicabile solo a quei documenti in cui lo spazio tra l
  parole è variabile (documenti adattati al testo contenuto
- Può essere scoperto facilmente se si riesce a conoscer
  l'algoritmo di adattamento del documento al testo

Vantaggi:

- Meno visibile del line – shift dato che spesso si modifica
  spazio tra parole adiacenti per avvallare l'adattamento d
  documento al testo.

Codifica Feature

Alcune caratteristiche del testo vengono modificate o lasciate inalterate a seconda della parola cifrata.

Esempio: si possono allungare o accorciare le barrette di lettere quali “h”, “b”, “d” …

Vantaggi:

- La scelta dei caratteri da modificare è casuale in modo evitare un’intuitiva decodifica visiva
- Un file di testo presenta un’incredibile mole di peculiarit che possono essere alterate per cui consente di nascon una notevole quantità di dati
- È difficilmente distinguibile per un lettore medio

Un’altra classificazione

Un’altra classificazione dei metodi di steganografia testu
si opera in base al particolare aspetto del testo che si vu
modificare per nascondere il messaggio.

Metodi di codifica:

- Metodi sintattici
- Metodi semantici

Metodi sintattici

Modificano le contrazioni grammaticali (la lingua ha una sintassi ricca di contrazioni) e/o la punteggiatura.

Esempio: “pane, burro, e latte”

“pane, burro e latte”

Svantaggi:

- È tanto più facilmente individuabile quanto più è lungo il testo

Vantaggi:

- Risulta molto più efficace se combinato con metodi open - space.

Metodi semantici

Si modificano le parole vere e proprie. Si utilizzano i sinonimi come
Classi di equivalenza.

Esempio: “big” _ 1
“large” _ 0

Svantaggi:

- A volte l’utilizzo di un sinonimo piuttosto che un altro stravolge l’intero senso della frase
- Soprattutto quando si usa l’inglese c’è molta differenza tra un documento formale ed uno informale, magari in slang

Vantaggi:

Bibliografia (1)

[1] 1606. Johannes Trithemius. Steganographia.

[2] 1606. Johannes Trithemius. Clavis Steganographiae.

[3] 1624. Johannes Trithemius. Cryptomenytices.

[4] 1997. Peter Wayner. Crittografia Invisibile.

[5] 1999. Simon Singh. Codici e Segreti.

[6] http://members.tripod.com/steganography/stego.html

[7] http://www.cl.cam.ac.uk/ fapp2/steganography/

[8] http://www.jjtc.com/Steganography/

[9] http://www.steganos.com/

[10] Ross Anderson. Stretching the Limits of Steganography.

[11] 1996. Bruce Schneier. Applied Cryptography-Protocols, algorithms and source code in C.

[12] Ivars Peterson. Cracking a medieval code.

[13] Neil F. Johnson, Sushil Jajodia. Steganalysis of images created using current steganography software

Bibliografia (2)

[14] Frank Sinapsi. Steganografia.

[15] http://www-lia.deis.unibo.it/Courses/RetiDiCalcolatori/Progetti00/fortini/project.pdf

[16] 1998. Neil Johnson & Sushil Jajodia. Exploring Steganography: Seeing the Unseen.

[17] 1998. Christian Cachin. An Information-Theoretic Model for Steganography.

[18] 1998. Ross Anderson & Fabien Petitcolas. On The Limits of Steganography.

[19] 1998. Andreas Westfeld & Andreas Pfitzmann. Attacks on Steganographic Systems.

[20] http://www.cs.uct.ac.za/courses/CS400W/NIS/papers99/dsellars/stego.htm

[21] 1998. Lisa Marvel & Charles Boncelet & Charles Retter. Reliable Blind Information Hiding for Images.

[22] www.Stegoarchive.com