18

From 'Steganographia' to Subliminal Communication

Otto J. Horak
Lecturer and consultant on cryptology
Weidenweg 15, A-2751 Matzendorf-Hölles, Austria

Abstract

After an introducing first section a review on the history and development of steganography concerning its name and its meaning is given in Section 2. Examples of different methods both for information hiding and a trial of an implicit steganographic signature illustrate this review. The last Section 3 is dedicated to steganography of today. This period starts with mass applications of digital computers in the early 1970s. Steganography now appears as covert channel in information processing, storage and communications. Subliminal channels as a special kind of covert channels, its detection and realization in digital signatures are shown as the most recent examples. Questions on future developments conclude the paper.

Keywords

Steganography, null cipher, semagram, implicit signature, covert channel, subliminal communication

1 INTRODUCTION

Looking for a motto characterizing the treated topic it is to find at Karl Ferdinand Gutzkow. Living from 1811 to 1878 in Germany he was working as literary man, publicist and drammatic producer. With his very liberal life-work he did together with colleagues of his time the casting step in literature from the romantic period to the realism. One part of his drama of 1847, 'Uriel Acosta' is Rabbi Ben Akiba who supplies the wanted motto: 'Alles schon dagewesen' (Büchmann, 1955) or as an English version: 'There is nothing new under the sun'. Only names and details change with the years, but adapted to the state of the art in techniques and technologies the heart of the matter remains just as it was in most areas of mankind activities. Steganography is no exception.

2 OLD-FASHIONED STEGANOGRAPHY

The term *Steganographia* (in English *steganography*, in French *stéganographie* and in German *Steganographie*) was introduced 1499 by Trithemius (Tritheim) in the sense of 'cov-

R. Posch (ed.), *Communications and Multimedia Security*

ered writing' (*ars sine secreti latentis suspicione scribendi.*) (Trithemius, 1499). Later G. Schott used this term also with the meaning of 'cryptography' (Schott, 1665). The root of *steganographia* is the Greek word στεγανογραφία [steganographia] built from στεγανός [steganós] = *covered* and γράφειν [grapheïn] = *writing.*

In modern understanding the aim of steganographic methods is just to hide the existence of a message independent of its type and appearance. Two kinds of methods can be distinguished:

1. technical steganography:

   (a) sympathetic (invisible) inks,
   (b) false bottoms,
   (c) micro photography (microdots) etc.

2. linguistic steganography:

   (a) a harmless looking message has another, previously agreed meaning ('open code'),
   (b) only certain elements of a harmless message are carrying meaning:

      i. 'null cipher': just certain letters or words are significant, all others serve as nulls,
      ii. 'semagram' (from σημα [sema] = *sign* and γραμμα [gramma] = *writing*): elements of the concealed message are contained in a harmless writing or drawing in agreed manner.

Kahn shows two 'null cipher' examples from World War I where at all words the first and second letters respectively give twice the same hidden message *Pershing sails from N.Y. June I* (Fig. 1).

PRESIDENT'S EMBARGO RULING SHOULD HAVE IMMEDIATE NOTICE. GRAVE SITUATION AFFECTING INTERNATIONAL LAW. STATEMENT FORESHADOWS RUIN OF MANY NEUTRALS. YELLOW JOURNALS UNIFYING NATIONAL EXCITEMENT IMMENSELY.

APPARENTLY NEUTRAL'S PROTEST IS THOROUGHLY DISCOUNTED AND IGNORED. ISMAN HARD HIT. BLOCKADE ISSUE AFFECTS PRETEXT FOR EMBARGO ON BYPRODUCTS, EJECTING SUETS AND VEGETABLE OILS.

Figure 1 Null Cipher [KAHN67]

Semagrams in form of writings could be built by (perhaps tiny) visible graphic peculiarities like a dot or a prick of a pin below or above the significant letters, by disturbed or misplaced types and so on. A rather recent example for misplacing of types as means for a semagram is contained in a book on combinatorics, edited 1977 in East-Berlin - at this time part of the East-Block - with an anti-soviet message (Halder, 1977). Fig. 2 shows a part of them where the significant characters are marked now with bars below.

8.3 DAS KÖNIGSBERGER BRÜCKENPROBLEM

In Königsberg i. Pr. gabelt sich der Pregel und umfließt eine Insel, die *Kneiphof* heißt. In den dreißiger Jahren des achtzehnten Jahrhunderts wurde das Problem gestellt, ob es wohl möglich wäre, in einem Spaziergang jede der sieben Königsberger Brücken genau einmal zu überschreiten.

Daß ein solcher Spaziergang unmöglich ist, war für L. EULER der Anlaß, mit seiner anno 1735 der Akademie der Wissenschaften in

Figure 2 Writing as Semagram

In drawings as semagrams, i.e. as carrier for concealed messages some special objects can represent encoded letters. A nice example is shown again by Kahn, where short and long blades of grass along the river-banks represent letters in Morse code (Fig. 3).

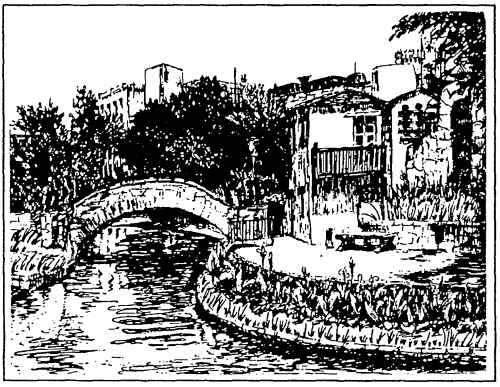

Figure 3 Drawing as Semagram (Kahn, 1967)

Meaning and classification of 'steganography' were not always the same during its existence. Formerly also used in the sense of secret writing, i.e. cryptography, now it is understood just as hiding of information. A. Figl is in between and counts by his

kind of classification linguistic steganography as cipher system (Figl, 1926). Because he distinguishes between visible or physical secret writings (*Geheimschriften*) "which are made by ordinary writing means but with agreed characters or in an agreed manner, generally staying visible" and invisible or chemical secret writings "which are produced with agreed writing means, chemical inks, generally being invisible and become visible only by agreed processing" what concerns technical steganography. Therefore A. Figl's classification is in contradiction to the actual one where linguistic as well as technical steganography is excluded from cryptography.

Steganography cannot be used only for hiding information to keep it secret. Concealed information can also serve as a kind of signature. Following the classification of signatures by J.L. Massey as a means that identifies the writer of a message six types can be distinguished:

1. By creation:

   (a) **implicit**: contained in how the message is written,
   (b) **explicit**: added as an inseparable mark to the message.

2. By the addressee:

   (a) **private:** identifies sender only to someone who shares a secret with the sender (author),
   (b) **public** (or "true"): identifies sender (author) to anyone from public available information.

3. By the revocation possibility:

   (a) **revocable:** sender can later deny he sent (wrote) the message,
   (b) **irrevocable:** recipient can prove that the sender wrote the message.

Among other examples for steganographic signatures a very famous but also very disputed one was assumed to be hidden by F. Bacon in the literary work of W. Shakespeare (1564-1616). In the middle of the 19th century the conjecture arose that Shakepeare is not the real author but Francis Bacon (Baron Verulam, Viscount Saint Albans; 1561-1626). Many 'Baconians', for example I. Donelly (1888), O.W. Owen (1893), E.W. Gallup (1899) tried to prove this by 'deciphering' his hidden signature. Some of their arguments seam very plausible. Donelly for example argued at the beginning of his book that Shakespeare (at his own will spelled 'Shakspeare' without 'e') could not be the author because he was "an untaught, unlearned man" and summarized in Part I, Chapter I, Section V:

> We commence our argument, therefore, with this proposition: The author of the plays, whoever he may have been, was unquestionably a profound scholar and most laborious student. He had read in their own tongues all the great, and some of the obscure writers of antiquity; he was familiar with the language of the principal nations of Europe; his mind had compassed all the learning of his time and of preceding ages; he had pored over the pages of French and Italian novelists; he had read the philosophical utterances

of the great thinkers of Greece and Rome: and he had closely considered the narrations of the explorers who were just laying bare the secrets of new islands and continents. It has been justly said that the plays could not have been written without a library, and connot, to-day, be studied without one. To their proper elucidation the learning of the whole world is necessary. Goethe says of the writer of the plays: "He drew a sponge over the table of human knowledge". We pass, then, to the question, Did William Shakspeare possess such a vast mass of information? - could he have possessed it?

Furthermore F. Bacon had invented a system of steganography called 'bi-literal cipher' transforming the letters of a secret message (the plaintext) in quintuples of two different symbols $\mathcal{A}$ and $\mathcal{B}$, comparable with today's 5-bit codes. In his own example, Fig. 4, Bacon used letters (types) of an a-font and a b-font to type the harmless cover-text.

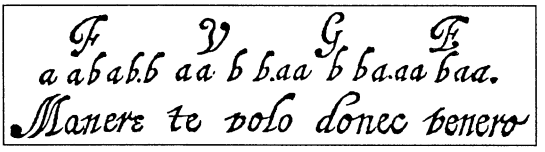

Figure 4 Bacons Bi-Literal Cipher

The cover-text MANERE TE VOLO DONEC VENERO [*Stay till I come to you*] written in this manner will give the cryptogram *aabab baabb aabba aabaa* - which means FUGE [*Flee*] (See also Kahn, 1967, pp. 883-4).

Bearing in mind these two facts - arguments against Shakespeare's insufficient education and Bacon's bi-literal cipher - it seemed not out of place to search for bi-literal messages of Bacon in the Shakespeare plays and verify the conjecture that F. Bacon is the real author. Provided that such a signature would exist, by the classification of J.L. Massey it would be an implicit and irrevocable one. As long as only one or some Baconians would have found the key it would be private for them but by making the decipherment public it changes to a public (or "true") signature. Apart from the question if Shakespeare principally was able to write this literary work, W.F. Friedman, who introduced modern cryptanalysis, and his wife E.S. Friedman have investigated the 'decipherment' of different Baconians but could not verify their 'proofs' (Friedman, 1957).

3 STEGANOGRAPHY OF TODAY

Not only the term steganography changed its meaning, cryptography does it too and expanded from the former "secret writing" corresponding to its strong translation and includes additionally now means for authentication and signatures together with related areas and applications. By this expansion a modern form of steganography, represented by

covert and subliminal communication and storage channels became parts of cryptography contrary to its definition mentioned earlier.

The digital computer was the vehicle carrying such new steganographic means into the cryptographic area. First and second generation computers installed about from 1959-1960-1965 opened a new epoch of mass data handling and difficult computation solving in business and science. The IBM System/360 inaugurated the third generation of computers in 1965-1970 introducing three major design innovations:

1. Base-register addressing for data location,
2. Microprogramming to achieve compatibility,
3. Input-output channels.

Parallel to these large-scale machines in the middle of the 1960s minicomputers arose. Since 1974 and in coarse numbers since the 1980s personal computers (PC) became available. All of them need peripheral storage means, displays, printers etc., each connected to the process by a 'channel', i.e. an information transfer path within the computer system. When the first computer euphoria has faded away not only the advantages have been seen and willingly accepted but also computer vulnerabilities became obvious. W.H. Ware (1970) had aroused attention to this problem area with his landmark report on security controls for computer systems and had alerted the US Department of Defense (DoD). Some years later B.W. Lampson (1973) and S.B. Lipner (1975) showed a special vulnerability: 'covert channels', i.e. the use of processes of a system in numerous ways that are not normally used for communication and are not normally protected by mandatory controls. Based on such related studies the US DoD included them already in an early version of the "Orange Book" with the following definitions (DoD-CSC, 1983):

Covert Channel: A communication channel that allows a process to transfer information in a manner that violates the system's security policy. See also: Covert Storage Channel, Covert Timing Channel.

Covert Storage Channel: A covert channel that involves the direct or indirect writing of a storage location by one process and the direct or indirect reading of the storage location by another process. Covert storage channels typically involve a finite resource (e.g., sectors on a disk) that is shared by two subjects at different security levels.

Covert Timing Channel: A covert channel in which one process signals information to another by modulating its own use of system resources (e.g., CPU time) in such a way that this manipulation affects the real response time observed by the second process.

In the introduction of his recent paper G.J. Simmons shows now the close connection between covert channels and that method formerly called steganography (Simmons, 1994):

> Covert channels and covert communications are well known to communications engineers and historians, and more recently, to computer scientists who have come to appreciate just how difficult it is to prevent leakage of information in systems designed to control information access. A classical example of a covert channel was the scheme used by some American prisoners of war during WW II to conceal information from enemy censors by causing the sequence of dots to the letter "i" and crosses to the letter "t" in their letters to be encoded in Morse code of a covert message.

A more recent example would be the use of some previously determined least significant bits of digitized voice, sound or video signals e.g. in ISDN or multimedia communications. Principally this method is not unknown to communications engineers as channels for signalling, control etc. What would be new – as it is reported – is a proposal from German scientists to use them as covert channel for undetectable and therefore secret information exchange.

In 1983 G.J. Simmons showed the existence of a special type of covert channels which he called 'subliminal channels'. Further he demonstrated that message authentication systems without secrecy could provide them (Simmons, 1983). The difference he explained in his recent paper (Simmons, 1994):

> ... covert channels are typically 'open' if only the monitor knows what to look for. Subliminal channels are also covert but are different in the important respect that even if the monitor knows what to look for, he can't discover either the message or the usage of the channel. ...

He illustrates his very detailed explanations with two types of subliminal channels easily producible also in the Digital Signature Standard DSS (NIST, 1994). Concluding his paper Simmons asks: "Given that subliminal channels of both types exist and that they are easy to implement, especially in the DSS, a natural question is: Do they have practical applications?" His answer is principally YES and it looks rather negative for the owner of documents officially signed by DSS. Information – not recognizable for the owner – subliminally (and perhaps illegally) transported within the signature may be of such kind the owner is not interested on a passing-on. This may be a very pessimistic view of subliminal channels and subliminal communications but could be possibly near reality for some cases. But, on the other hand, a question may be asked if there exist also an optimistic view of these things: Perhaps implicit signatures applied to information like that conjectured in Shakespeare plays which could become necessary in the era of the 'Information-Highway' giving an author additional security for protection of his rights apart a public signature (which could be disturbed or forged). Will other positive applications be found? Furthermore it could be asked if there are means other than message authentication without secrecy and signature schemes not known at present providing subliminal channels. May be future investigations will give answers.

4 REFERENCES

Büchmann, G. (1955) Geflügelte Worte und Zitatenschatz. Licence Edition for Bertelsmann-Lesering. Johannes Asmus Verlag, Stuttgart.

DoD-CSC (DoD-Computer Security Center, 1983) Department of Defense Trusted Computer System Evaluation Criteria. Document CSC-STD-001-83.

Donelly, I. (1888) The great cryptogram: Francis Bacon's cipher in the so-called Shakespeare plays. R.S. Peale & Co, Chicago.

Figl, A. (1926) Systeme des Chiffrierens. Verlag Moser, Graz.

Friedman, W.F. and Friedman E.W. (1957) The Shakespearean ciphers examined. An analysis of cryptographic systems used as evidence that some author other than William Shakespeare wrote the plays commonly attributed to him. University Press, Cambridge.

Galland, J.S. (1945) An historical and analytical bibliography of the literture of cryptology. Northwestern University, Evanstone.

Gallup, E.W. (1899) The bi-literal cypher of Sir Francis Bacon discovered in his works and deciphered by Elizabeth Wells Gallup. Howard Publication Co., Detroit, Mich.; Gay & Bird, London.

Halder, H.-R. and Heise W. (1977) Einführung in die Kombinatorik, 118-9. Akademie-Verlag, Berlin.

Kahn, D. (1967) The Codebreakers - The story of secret writing. MacMillan Publishing Co., Inc, New York.

Lampson, B.W. (1973) A note on the confinement problem. *Communications of the ACM*, **16**, 613-5.

Lipner, St.B. (1975) A comment on the confinement problem. *ACM Operating Systems Review*, **9**,192-6.

Meister, A. (1906) Die Geheimschrift im Dienste der Päpstlichen Kurie von ihren Anfängen bis zum Ende des XVI. Jahrhunderts. *Quellen und Forschungen aus dem Gebiet der Geschichte*, **XI**. Edited by Görres-Gesellschaft. F. Schöningh, Paderborn.

NIST (US National Institute of Standards and Technology, 1994) Digital Signature Standard (DSS). Federal Information Processing Standard (FIPS) No. 186.

Owen, O.W. (1893) Sir Francis bacon's cipher story discovered and deciphered (5 Volumes, 1893-1895). Howard Publication Co., Detroit, Mich.

Schott, G. (P. Gasparis Schotti, 1665) Schola steganographica, in classes octo distributa .... Nürnberg.

Simmons, G.J. (1983) The prisoner's problem and the subliminal channel, in *Advances in cryptology (Ed. by D. Chaum, 1984). Proceedings of CRYPTO '83*, 51-67. Plenum Publishing Corporation, New York.

Simmons, G.J. (1994) Subliminal channels; past and present, in *European Transactions on Telecommunications (ETT)*, **5**, 45/459-59/473.

Trithemius, I. (Johannes Tritheim, 1499) Steganographia: hoc est: Ars per ocvltam scriptvram animi svi volvntatem absentibus aperienda certa.
According to Kahn (1967): Manuscript of a volume which he planned in 1499 and intended to comprise eight books and which he called 'Steganographia'. Meister (1906) states that four books were planned and that Tritheim finished the first, March 27, 1500, the second, April 20 of the same year. According to Galland (1945) publication of "Stenographia" followed only long after the death of Tritheim († 1512), whereby 1531 and 1551 as earliest dates are mentioned amongst many others. A last reprint appeared 1721.

Ware, W.H. (1970) Security controls for computer systems: Report of Defense Science Board Task Force on Computer Security. *Report R-609-1*. Rand Corporation, Santa Monica, Cal. (Reissued October 1979).

BIOGRAPHY

Born in Vienna in 1928, Otto J. Horak was working after completion of polytechnic education for five years as electronic engineer. In 1954 he started a military career and entered the Theresian Military Academy. Upon graduation in 1957 and engaged as an instructor for radar and electronics he began in autumn 1960 studies in communications

and electronics at the Technical University, Vienna. After completion in 1967 he began an engagement at the Austrian Ministry of Defense with responsibility for planning of electronics including cryptology. In 1976 he was appointed Head of the MoD Department for Informatics, Communications and Electronics. Eight years later he became Head of the Armed Forces Data Processing Agency and promoted Major-General. Also in 1984 followed his appointment as sworn expert witness on cryptology. He retired in 1989 and lectures since 1990 at the Technical University, Vienna on 'Introduction to Cryptology'. Additionally he works as consultant in this area.