Steganography: is it becoming a double-edged sword in computer security?

Subtitle

Miss K.I. Munro
University of the Witwatersrand

Key words: steganography, cryptography, encryption

Abstract:

The growth of the Internet has stimulated the use and the misuse of Steganography. At its simplest level, Steganography, the art of hiding secret messages within the structure of another media. While legitimate and justifiable applications for steganography exist, criminally-minded people or organisations can also use it for underground, illicit and deliberately secret communication. The objective, similar to cryptography is to make it impossible for those without the key to break the code, however Steganography operates at a more complex level as detection is dependent on recognising the underlying hidden data. This paper introduces the topic of steganography and evaluates the applications, both positive and negative. This paper finds steganography to be both a helpful and a hindering force in the computing milieu. A more thorough investigation is needed to aid a variety of stakeholders: law policy makers, security professionals and the general internet populace.

1. INTRODUCTION

Steganography has become a topical security issue in recent months in the context of seeking explanations for the clear communication success of terrorists cells following the attacks on the United States in September 2001.

Steganography is by no means a recent development though, and is in fact much older than cryptography. Stegano (meaning covered) and graphy (meaning writing) is derived from the Greek language – put together it can be interpreted as follows: the science of concealing messages incorporated into other media. The first recorded occurrence of steganography in practice has been ascribed to the political prisoners of King Darius in the 5th century BC. A secret message was tattooed into the shaven scalp of a fellow inmate who was about to be freed. The carved secret inscription became hidden as the lucky man's hair grew back (Castelluccio, 2001; Johnson and Jajodia, 1998b). There are numerous other occurrences of steganography being used in ancient times. Carvin (2001), Hancock (2001) and Johnson and Jajodia (1998b) describe the Greek historian, Herodotus' account of Demeratus, who was able to notify Sparta that King Xerxes of Persia was about to invade them. By etching the secret message into a tablet of wood, and then covering the wooden surface with wax, it appeared blank and thus was transported to Sparta without a hint suspicion from the sentries on inspection duty.

In more recent times, steganography has also been greatly relied upon during wars and battles. During World War II, the German and allied forces both used it to conceal their private messages (Carvin, 1998; Johnson and Jajodia, 1998b). The famous passage below, used by a particular German spy read:

> *Apparently neutral's protest is thoroughly discounted and ignored. Isman hard it. Blockade issue affects pretext for embargo on byproducts, ejecting suets and vegetable oils.*

This ostensibly innocent message would have most likely been cast aside and ignored, but to the recipient who knew that it was the second letter that should be used for the real communication, a more meaningful message comes through:

Pershing sails from NY June 1.

Thus steganography can be applied to many different media – it is simply a case of disguising a covert message within an overt one for the purposes of concealment (Carvin, 2001). With developments in technology and the

internet, steganography has become possible using various media in the computing world. Images or text can now be stealthily and unrecognisably concealed in graphic (jpeg, bmp or gif files), text or music (mp3) files. To embed the text or image, the least significiant bit of each pixel or wav file is flipped and an additional bit of data can be stored, which does not noticeably affect the appearance of the image or the sound of the audio file.

Any new application of technology, however, requires an assessment of the threats and opportunities it affords. Johnson (2001) points out that "new technological possibilities are not always good or purely good, they need to be evaluated….evaluation can and should take place at each stage of a technology's development, and can and should result in shaping the technology so that its potential good is better realized and negative effects are eliminated or minimised". This paper suggests that threats as well as the opportunities presented by steganography should be highlighted. This brief investigation could form the basis for a more thorough research survey to assist security professionals, law policy makers and other interested parties in determining whether steganography is a feasible and viable security mechanism under the current conditions of globalisation.

2. DEFINING THE NATURE OF THE PROBLEM

Steganography is a high-level type of encryption, and its use results in a mechanism to implement two of the five key pillars of information security, namely confidentiality and integrity. The confidentiality of the hidden message is protected due to it being unrecognisable in its hidden and encrypted form both in the place of storage and during transmission. Any interceptor would not be aware of the secret message. Only authorised people would know of its existence and would be able to decrypt the secret message with the known password. The encrypting of the concealed message protects the integrity of the data. It must be stressed that the unique feature of steganography is largely to be attributed to the potential for use in IT security. Not only is the secret message encrypted, but it is also hidden behind an image, text or music file, making it invisible to ordinary interceptors.

Applications of steganography are wide ranging, and are indeed valuable if used in the correct manner. However this security technology may be misused and abused, resulting in disastrous consequences.

A New York Times article on October 30th 2001 claims that a French Defence Ministry official corroborated that Jamal Beghal (a terrorist suspect) used the technique of steganography to plan a failed bombing attempt of the US Embassy in Paris earlier in the year (Kolata, 2001). Following the September terrorist attacks in the United States, many reporters, and intelligence agents argued that the detailed planning of these attacks was co-ordinated through steganography (Campbell, 2001; Carvin, 2001; Sieberg, 2001; Kelley, 2001; Cha and Krim, 2001). McAllister (2001) of SfGate wrote that "Bin Laden is rumoured to be fond of concealing his transmissions inside some of the very same 'anit-Islamic' content that prompted the Taliban to ban Internet use in Afghanistan: pornography". It is an intriguing postulation, but as yet, the use of this cryptography tool by terrorists remains unsubstantiated. Declan McCullagh, a journalist for Wired News was one of the first analysts to report on the possible link between terrorist communication and steganography. Although cynical of its role in the recent terrorist attacks, he offers sound advice: "…we should assume for purposes of political debate that terrorists will use cypto and stego, because if they're not now, they eventually will" (Carvin, 2001). Regardless of whether this technique was used by terrorists and resulted in the absence of information prior to the September attacks, one must always focus on its future role in security.

3. DECONSTRUCTING STEGANOGRAPHY

There are many different variations of steganography in the computing realm. Data can be secretly hidden in either text, graphics (jpeg images), video or sound (MP3 audio files) – basically anything that can be represented as bit streams offers a medium for steganography (Yeh and Hwang, 2001). What makes this technique viable to the communicating parties is that these digital media may be slightly altered by incorporating secret data, and yet still look exactly the same to the human eye, or sound identical to the human ear (Kolata, 2001).

Exactly how it works is extraordinary. Johnson and Jajodia (1998b) describe the three different ways in which information can be hidden in digital images. The three mechanisms are least significant bit insertion, masking and filtering and algorithms and transformations. The least significant bit method is the most common method, offering a simple approach to embedding the data. The image is however, somewhat manipulated, although is not noticeable to the human eye. It works by using

the least significant bit of each pixel in an image to encode the message. The secret message can be broken up into bits, and spread around to be concealed separately in each pixel. The technique which is often applied in steganography uses a key to initiate a cyptographically secure random number generator, which then decides on which particular pixels will hold the message. The only person that can decrypt the message has to be in possession of or know the key, which then selects the bits in the right order to produce a meaningful message (Wayner, 2001). Steganography software using this method arranges the palette so that adjacent colours do not contrast prior to inserting the data to be hidden.

What favours the use of steganography is the degree of available space in an image file. One-eighth of the image file can be used to hide messages without being detectable (as the level of distortion is negligible) (Wayner, 2001). Bender *et al* (2000) however, lists the quantity of data to be hidden as a constraint which affects steganography – obviously, hiding reasonable amounts of data can be achieved, but there is a limit.

Schneier (2000, p. 245) discusses the power of steganography in his book "Secrets & Lies". He deems it to offer a degree of privacy which far surpasses the level of privacy offered by ordinary encryption. He goes on to discuss its beneficial qualities of steganography over ordinary encryption. He considers that one of the limitations of encryption is that the third party interceptor or monitor is always aware that a message has been sent, despite the fact that it has been encrypted and cannot be read. The principle appeal of steganography is that it provides a mechanism to communicate in a completely secret manner. By hiding a meaningful message behind an image, two parties can correspond without anyone being aware of the underlying message. Undoubtedly the eavesdropper may intercept the message, and clearly view the image, but will not be aware of the hidden secret information, which cannot be seen.

4. STEGANOGRAPHY – A DOUBLE-EDGED SWORD?

"*One mans meat is another mans poison*" (traditional proverb)

As with any technology, benefits as well as detrimental possibilities for its use exist. It is important to look at both angles and assess the various applications on both sides of the scale. Firstly, the benefits of steganography will be explored, detailing legitimate and useful current applications. The threats of steganography will then be examined, focusing on applications that are harmful or detrimental to society.

4.1 The benefits of steganography

Steganography offers many benefits to society with a large variety of virtuous applications - it enables communication with a high-level of privacy, provides a safe repository for business trade secrets, and scores of applications exist for its use on the internet (it is specifically used for watermarking copyright-protected data).

Ho *et al* (1999) discuss the necessity of digital steganography in various e-commerce applications. Digital watermarking (used for copyright protection), digital signature authentication (for validation of electronic documents) and digital data storage and linkage (for binding digitized photographs with personal attribute information) are all legitimate and valuable uses of this technique.

4.1.1. Digital Watermarking

The internet is a tricky medium for making sure that intellectual property rights are not violated. One mechanism which offers some sort of protection to the copyright holder is digital watermarking. It enables one to embed either a text or image watermark (which identifies ownership) over the digitized data, and make it irremovable and if needs be, invisible. Various digital watermarking software make this possible (Ho *et al,* 1999). StegMark is one that is currently available on the market and used for such applications.

Anderson and Petitcolas (1998) note that the publishing and broadcasting industries have seen the use of this technology as a boon to alleviate the fear of the ease of reproduction and digital distribution over the internet. It

makes the concealment of copyright marks and serial numbers in digital films, audio recordings, books and multimedia products possible.

Bender *et al* (2000) explores the less common legitimate application of anticounterfeiting, made possible by the use of steganography, or to be more specific, digital watermarks. The massive advances in ink-jet printers and scanners have provided a perfect mechanism to reproduce high-quality colour copies of any original document. Criminally minded individuals use such technology to engage in the creation of counterfeit currency or other valuable documents which look like the 'real thing' if not examined by a professional. By embedding a digital signature into a document or currency note, this can be detected by a printer (that is obviously programmed to detect such elements) that can then refuse to complete the print job and provide an appropriate warning to the perpetrator. It thus means that counterfeiters would be discouraged from engaging in this illegal activity.

4.1.2. Digital Signature Authentication

Steganography can be applied to prevent devious interference with private and confidential documents. Emails, letters or company memos are often embedded with a digital signature and a multimedia container password. If the document is tampered with, this will be detected, and the receiver will immediately be notified of the interference (Ho *et al,* 1999). StegSign is one registered brand of software which provides such digital signature authentication.

4.1.3. Digital Linkage and Storage

StegSafe provides a mechanism to link a digital image with attribute text information. Personal information such as medical history, law enforcement records and other details could be linked to digitized copies of ID photos. It is important that the integrity of the data is maintained, and thus vital to know if details have been modified by an intruder. Using steganography to link the image and this personal information allows the database administrator to be notified if any modifications have taken place (Ho *et al,* 1999).

Many researchers believe the use of steganography has been invaluable in electronic commerce, and without such high-level encryption, many believe that electronic commerce would never have taken off like it has (Doogan, 1999).

4.2 The threats of steganography

The use of the technique of steganography, however, presents certain worrying concerns. One major problem that comes to the fore is that criminals could possibly abuse this tool. In making this type of encryption technology available to the general public, it means that criminals too can plot, scheme and plan devious and malicious actions without anyone being aware (Doogan, 1999).

Despite attempts in the US at regulation (discussed later in the paper), the fact which always remains constant is that technology is too pervasive and powerful for governments to simply ban only the criminals from using these types of computerised tools.

Doogan (1999) captures the essence of the problem:

> *"the availability of strong cryptography is a very mixed blessing, on the one hand it can be used in the development of electronic commerce and the maintenance of personal privacy, on the other it does provide a useful tool for the criminally minded"*.

Other security researchers concur with this opinion. They believe that steganography is being used to aid criminal activities the world over. DeQuendre (1998) found that this type of mechanism is being used to an even greater degree in European countries, such as France, Germany and England, where encryption is significantly restricted for common use. Seargent Doyle of the Computer Investigations and Technology department of the New York Police said at a Computer Security Institute conference held in 1998 that "steganography and cryptography are increasingly the methods being used by those with nefarious intentions" (cited in DeQuendre, 1998).

4.2.1. Child pornography distribution, drug trafficking and the transmittal of viruses

Johnson, cited in DeQuendre (1998) described his recent findings at a European conference. He discovered that the use of this technique to hide child pornography and drug trafficking transactions were indeed prolific. Other perilous applications he mentions for this type of technique is its ability to transmit hidden viruses.

5. AVAILABILITY AND ACCESSIBILITY OF STEGANOGRAPHIC SOFTWARE

Yet another valid concern frequently expressed in the literature deals with the availability of steganographic software. The internet is a prime location where steganographic software appears on freeware and shareware sites. There are a number of sites with various steganographic tools which can be downloaded free of charge. Carvin (2001) mentions the product "Invisible Secrets 3.0" which he used to steganographically alter a photo and place a picture of his cat behind it. (See http://www.benton.org/DigitalBeat/stegdemo.html to view it). Other researchers have attempted to review the steganographic software options available. Johnson and Jajodia (1998b) undertook the evaluation of a number of these tools which run on a variety of platforms, including DOS, Windows, OS/2, Mac and Unix. They are as follows:

- StegoDos (a public domain software)
- White Noise Storm (a steganography application for DOS)
- S-Tools (use for Windows, and deemed the most versatile of all tools tested)

Many researchers concur that the problem is that this software is quick and relatively easy to find and can be downloaded at no cost (DeQuendre, 1998), thus criminals have easy access to these tools. Johnson (cited in Kolata, 2001) reveals the number of steganographic tools available on the internet having doubled in the past two years, currently being close to one hundred and forty, and still increasing.

Johnson sees the availability of this software and information to be quite dangerous for those with devious intentions. He is reported to have said that as he is so worried about the potential of steganography when used by terrorists, that he has stopped publishing research on its use and how to detect it (Kolata, 2001). A common theme expressed by researchers and

security professionals was that information on steganography, and how to use it is so widely available that people with criminal intentions will have access to information about it, and its ease of use.

6. STEGANALYIS :DETECTING MESSAGES WITH STEGANOGRAPHIC CONTENT

Security professionals have also raised concerns about the difficulty of detecting messages in which steganographic content appears. Currently there is the slight possibility that hackers could intercept an encrypted message, and be able to decrypt it and read the plaintext, however being able to spot the communication which contains a secret steganographic text or image is virtually impossible (DeQuendre, 1998).

When steganography is used to hide messages, a certain level of distortion and degradation may occur in the carrier, however, it might not be easily detected by the human eye. Comparing the distortion and degradation and space considerations to a "normal" image, could make possible the detection of whether steganographic content exists or not. What makes steganalysis (the distinguishing and deciphering of messages with steganographic content) very difficult is not knowing which steganographic tool was used, and not knowing the stegokey (or encryption password) (Johnson and Jajodia,1998a).

Johnson and Jajodia (1998) have been researching the possibilities and accuracy of a method they have developed which aims to distinguish the images with underlying content from those without (steganalysis). This detection technology, however, remains in the developmental phases and is currently not one hundred percent reliable (the occurrence of false positives in their studies were quite high).

Provos and Honeyman (2002) discussed the ways in which steganalysis can be undertaken. Using statistical techniques, they test whether the image's statistical properties deviate from the norm. "Stegdetect" can also be used to analyse JPEG images for steganographic content by launching a dictionary attack against the image files. This provides an automated mechanism of trying to guess the password which the stego-content has been encrypted with. They caution that for it to work, the steganographic system must have selected a "weak" password that it a dictionary attack can crack.

The scientific study by Provos and Honeyman (2002) (two researchers from the University of Michigan) challenged the view that terrorists communication relied on steganography. They used steganalysis and various statistical techniques to test well over two million images on e-bay's auction site (*www.ebay.com*). In their very large sample, their research showed that there was no evidence of hidden messages. While some security specialists are sceptical of their statistical techniques, others caution that there may be new and unknown types of steganography which could elude their tests. In light of these findings, a few researchers remain pessimistic that detection tools are not advanced enough to work properly (Campbell, 2001).

Others believe that steganalysis offers a glimmer of hope to computer security/forensics professionals in containing this otherwise explosive security problem of the future. Steganalysis is still in its infancy stages, although promises to be a reckoning force in the future. One can only hope that steganalysis research is successful, as criminals might then be reluctant to use this technological mechanism for fear of being discovered.

7. REGULATION AND LEGISLATION

A common fear is that regulatory authorities will impose legislation banning steganography for fear of possible criminal elements using this type of technology to society's detriment. Many security professionals believe that there are far greater disastrous consequences in restricting its use altogether and treating it as more of a foe than friend. Castelluccio (2001) discussed privacy considerations and the need for encryption. European internet shoppers and online businesses were reassured that stronger encryption techniques were seen as acceptable to protect credit card numbers and personal information.

Carvin (2001), discusses one of Provos' concerns, being that online civil libertarians are fearful that these unsubstantiated claims of terrorists using steganography will provide politicians with evidence to lay down further restrictions regarding steganography and encryption. Provos thinks that despite their findings, "the terrorist attacks are being used by some politicians as a reason to pass legislation that they could not pass

before…..there is no indication that any encryption technology has been used".

Legislators in the Netherlands have already succeeded in regulating the publics use of strong encryption on the internet. Currently, the US has no specific law regarding the use of steganography, however many see that such legislation is on the horizon. Carvin(2001) deems that as claims of terrorists using this technology have abounded, and that they are closely related to the goals of many, namely strengthening national security and minimising pornography on the internet, leglislators could limit access to steganography and restrict or ban the development and access to steganographic software in the not too distant future.

Legislation is often seen to be the only answer to such a problem. Many researchers, however, have indicated that this probably will not have any affect on its use by terrorists or the criminally minded. The question which arises is that would anti-steganography leglislation serve the purpose for which it is intended, or would it merely further limit the privacy of law-abiding individuals.

8. STEGANOGRAPHY – FRIEND OR FOE?

Despite the potential uses of steganography to aid criminals in their communication, it also has many useful applications which are necessary in the growing digitized and electronic world in which we operate. While some security professionals foresee doom and gloom with regards to steganography in the future, others see it as merely a phase of technology.

Erbschloe (2001) considers that the future of steganography will be a function of the evolution and limitations of imaging technology. He argues that "steganography won't evolve very much as it has reached its plateau" (Erbschloe, 2001). As steganography consumes images to the fullest, he believes that hiding minimal amounts of information is useless.

9. THE FUTURE ROLE OF STEGANOGRAPHY IN IT SECURITY

Schneier (2000) believes though that steganography is not the ultimate security solution– he views interceptors as intelligent beings who are trained to unearth any irregularities and peculiar occurrences. Two people who wish to communicate secretly and hide it behind images are asking to be viewed in a surreptitious light – the interceptor must question why a particular image (if it bears no prior meaning to their relationship) is being sent and conclude that something untoward is happening. For steganography to be successful, it must fit into the existing communication pattern; it cannot suddenly be incorporated for it not to be viewed with any kind of suspicion.

I believe that although it is a powerful mechanism of hiding information, if traffic analysis evolves and is correctly managed, the power of steganography to conceal information is in jeopardy. Some argue that traffic analysis will not have any effect of intercepting messages with steganographic content. Through the medium of the internet, one can post a message behind a picture on some arbitrary site. As long as the recipient knows where to look for the image and has the key to decrypt the steganographic content, they can see it or read the hidden message. Consequently, there need not be any electronic mail sent or any communication transmission between two parties. In this instance, traffic analysis would be futile.

A final thought (although not mentioned in the literature), I see vast possibilities for the use of steganography in industrial espionage – getting information out of organisations without anyone being aware. This, however is yet to be seen or reported.

10. CONCLUSION

The emerging mainstream view in IT is that steganography provides yet another mechanism of cryptography.

Before the recent horrendous terrorist attacks, steganography was viewed in a favourable light – it merely provided an additional mechanism to safeguard

business secrets, watermark copyrighted data and demonstrate technological prowess. It was just yet another technology which became part of the growing internet culture (Carvin, 2001).

However a contrary perspective on encryption was presented by Freeh, a US politician, who commented to the Senate Judiciary committee in September 1998 that "we are very concerned, as this committee is, about the encryption situation, particularly as it relates to fighting crime and fighting terrorism…..we believe that an unrestricted proliferation of products without any kind of court access and law enforcement access, will harm us, and make the fight much more difficult" (cited in Hancock, 2001). He did not however mention steganography, but viewed encryption as harmful due to its potential uses by terrorists.

To return to the commentary on the use of steganography in the planning of September terrorist attacks, it would appear that there is no hard evidence of the use of steganography by terrorists. Until such evidence is produced, one should be wary of an exaggerated response. Nonetheless, it is imperative that the mechanism of steganography be properly assessed and evaluated before any regulatory authorities ban its use – there is often a knee-jerk reaction to quickly draft legislation, which on the whole causes more harm than good.

Clearly the use of steganography is largely an American concern at present. It does however pose a potential international problem as the internet operates on a global level. The proliferation of freely available steganographic software and its detrimental applications do send warning signals in the uncertain and criminally-active climate in which we operate today. It becomes clear that it is not a security mechanism to be ignored or avoided – its use could result in serious ramifications and it desperately needs to be considered by all stakeholders from every angle.

11. REFERENCES

Anderson, R.J. and Petitcolas, F.A.P. (1998) "On the limits of Steganography", *IEEE Journal of Selected Areas in Communications,* Vol. 16, No. 4, pp. 474 – 481.

Bender, W., Butera, W., Gruhl, D., Hwang, R., Paiz, F.J. and Pogreb, S. (2000) "Applications for Data Hiding", *IBM Systems Journal,* vol. 39, issue 3/4, p. 547.

Campbell, D. (2001) "Are terrorists using hidden messages", *Telepolis,* available online at http://www.heise.de/tp/english/inhalt/te/11004/1.html

Carvin, A. (2001) "When a Picture is Worth a Thousand Secrets: The Debate Over Online Steganography", *Interesting people message,* available online at http://www.interesting-people.org/archives/interesting-people/200111/msg00003.html

Castelluccio, M. (2001) "Hidden Writing and National Security", *Strategic Finance,* November, vol. 83, issue 5, p59.

Cha, A.E. and Krim, J. (2001) "Terrorists' Online Methods Elusive: US Agencies seek experts' help in tracing encrypted messages", washtech.com, available online at

DeQuendre, N. (1998) "A picture hides a thousand words", *Security Management,* February, vol. 42, no. 2, pp. 17-18.

Doogan, S. (1999) "Criminals using Cryptography, Reasonable Precaution or Convenient Smokescreen?", *Proceedings to the 14th BILETA Conference: "CYBERSPACE 1999: Crime, Criminal Justice and the Internet",* March 29-30, York, England.

Erbschloe, M. (2001) "Future of Steganography", *New Straits Times,* November 8.

Hancock, B. (2001) "Terrorism and Steganography: Shaken, Not Stirred", *Computers and Security,* vol. 20, no. 2, pp 110 – 111.

Ho, A., Tam, S-C, Tan, S-C., Yap, L-T., Neo,K.B. and Thia, S-P. (1999) "Digital Steganography for Information Security", available online at http://www.datamark-tech.com/publications/steganography.pdf

Johnson, D.G. (2001) "*Computer Ethics",* 3rd edition, Prentice-Hall: New Jersey.

Johnson, N.F. and Jajodia, S. (1998a) "Steganalysis: The Investigation of Hidden Information", *Proceedings of the 1998 IEEE Information Technology Conference,* Syracuse, New York, USA, September 1-3.

Johnson, N.F. and Jajodia, S. (1998b) "Exploring Steganography: Seeing the Unseen", *IEEE Compute Magaziner,* Vol. 31, No. 2, pp. 26 –34.

Kelly, J. (2001) "Terror Group hide behind Web Encryption", *USA Today.* Available online at http://www.usatoday.com/life/cyber/tech/2001-02-05-binladen.htm.

Kolata, G. (2001) "Veiled Messages of Terrorists May Lurk in Cyberspace", *The New York Times,* October 30, available online at http://www.nytimes.com/2001/10/30

McAllister, N. (2001) "No Scorched Internet Policy Attacking Technology Will Only Add to the Toll", *SFGate,* Available online at http://www.sfgate.com/cgi-bin/article.cgi?file=/gate/archive/2001/09/20/sigintell.DTL

Provos, N. and Honeyman, P. (2002) "Detecting Steganographic Content on the Internet", to appear at the , ISOC NDSS'02 conference, San Diego, CA, February 2002, available online at http://www.citi.umich.edu/u/provos/stego/

Schneier, B. (2000) *"Secrets & Lies: Digital Security in a Networked World",* Wiley & Sons : New York.

Sieberg, D. (2001) "Bin Laden exploits technology to suit his needs", CNN.com/US. Available online at http://www.cnn.com/2001/US/09/20/inv.terrorist.search/.

Wayner, P (2001) "Steganography", *Interesting people message,* available online at http://www.interesting-people.org/archives/interesting-people/200111/msg00023.html

Yeh, W-H and Hwang, J-J. (2001) "Hiding Digital Information Using a Novel System Scheme", *Computers and Security,* vol. 20, no. 6, pp. 533-538.