Global Information Assurance Certification Paper

Table of Contents.....1
Lachlan_McGill_GSEC.doc.....2

Steganography: The Right Way

Name: Lachlan McGill
Date Submitted:
Certification: GSEC version 1.4c

1 Table of Contents

1 Table of Contents 2

2 Abstract 4

3 What is Steganography? 5

3.1 Human Perception 5

3.2 Detection 5

4 The History of Steganography 6

5 How does it work? 8

5.1 Technique 1: Substitution 9

5.2 Technique 2 – Injection 9

5.3 Technique 3 – Generation of New Files 10
5.3.1 The Prisoner's Problem 10
5.3.2 Spam Mimic 10

6 Choice of Carrier 12

6.1 Images 12
6.1.1 Least Significant Bit 12
6.1.2 Masking 12

6.2 Audio 13
6.2.1 Low-Bit Encoding 13
6.2.2 Spread Spectrum 13
6.2.3 Echo Data Hiding 13
6.2.4 Perceptual Masking 14

6.3 Video 14
6.3.1 Discrete Cosine Transform (DCT) 14

7 Steganography vs. Cryptography 16

8 Modern Day Uses 18

8.1 Corporate Espionage 18

8.2 Terrorism 18

8.3 Watermarking 18

9 Detecting the use of Steganography 20

9.1 What is Steganalysis? 20
9.1.1 Active Attack 20
9.1.2 Passive Attack 20

9.2 Is Steganography in widespread use on the Internet? 21

10 Conclusion 23

11 References 25

2 Abstract

Steganography in the last few years has gained a wider audience due in part to the suspicion that the technology may have been used by terrorists to communicate plans for upcoming attacks. While those claims have never been formally substantiated, the technology has certainly been the topic of widespread discussion among the IT community and has provided the benefit of helping more people understand steganography and how it can be used today to conceal information.

This paper discusses the concepts behind steganography by exploring firstly what it is and how it has been used throughout history. This is followed by technical discussions on how it works and what methods are used to embed information in digital carriers. The paper explores the relationship with cryptography and how the two technologies differ. Modern day uses of steganography are then briefly discussed followed by details on how it can be detected through the use of steganalysis.
Finally, the conclusion presents 'The Right Way' to use steganography as a means of concealing information and the pitfalls to be wary of by outlining key points to consider when using steganography.

3 What is Steganography?

Essentially, steganography is the art of concealing private or sensitive information within a carrier that for all intents and purposes, appears innocuous. It comes from the Greek words steganós (covered) and graptos (writing). Simply put, if you were to view the presented information, it would appear to be something that does not warrant further analysis due to the fact that it does not LOOK or SOUND like anything that contains sensitive information. Steganography has been used for hundreds of years as a means of concealing information from prying eyes before ultimately reaching its intended destination. Examples of its use in history are detailed in the following section *The History of Steganography*. It relies on the sender and receiver agreeing upon the method by which the information will be hidden and therefore some means of prior communication is essential for steganography to be of any use.

Steganography is sometimes confused with cryptography. Although the two can co-exist as discussed later in this document, they are not the same. Both are used to **protect** information but steganography is concerned with **concealing** information thereby making it unseen while cryptography is concerned with **encrypting** information thereby making it unreadable.

3.1 Human Perception

Steganography relies on the fact that the human senses are inadequate when compared to analysis performed by machines or even in fact the senses of other animals of the earth. The human eye or the human ear cannot detect very subtle or minute changes in visual or aural presentations making steganography an effective means of concealing private information.

3.2 Detection

One major factor in steganography is that it relies on the fact that a person does not know that a picture or a sound file or a block of text actually contains hidden information. It is a much more effective means of protecting information if the attacker (unintended or unauthorised recipient of information) does not know that the material presented before them actually contains hidden information because once this is known, steganography opens itself up to attack and loses its most potent advantage: innocuousness.

4 The History of Steganography

History has provided countless situations whereby information has had to traverse hostile or enemy territory to reach its destination undetected. People through the ages have used many ingenious methods to conceal information and as time passed these methods would generally improve as older methods and processes were invariably discovered.

Some of these examples are:

- In Ancient Greece, they used a method whereby a person was chosen as a messenger and had their head shaved. The secret text was tattooed onto their bald head and the hair was allowed to grow once again to normal length. The messenger would then proceed to the destination passing any security inspections (they would have appeared to be carrying nothing suspicious) and presented themselves to the receiver of the information who would then shave the head of the messenger to read the secret text. One major drawback to this method was the latency in getting the message to the receiver. One had to wait for the hair to grow back sufficiently to conceal the text before the message could be delivered. Another disadvantage to this method is that the messenger was usually left with a lifelong tattoo upon their head meaning the secret message cannot be destroyed without applying another tattoo over the existing one.

- Another method used in Ancient Greece was wax covered tablets. The wax would be scraped off the tablet, the message written on the wood underneath and the wax re-applied. The receiver of the tablet would then simply scrape off the wax once again to reveal the message.

- A famous Greek, Aeneas the Tactician devised a method whereby holes representing letters of the Greek alphabet were bored into a wooden disk. Yarn was then threaded through the holes in order that they would spell out the message. He also used another method in which he pinned tiny holes above letters in a document to spell out the message. These tiny holes were generally undetectable to someone who was not aware that they existed and was just casually reading the document. This method was still used in the twentieth century and is now called the newspaper code.

- During World War II, invisible inks were used to conceal information in seemingly standard, innocuous memos or letters. Common sources for invisible inks are milk, vinegar, fruit juices and urine. Each one of these substances darkens when heated and was especially effective during this time due to the fact that the sources were always readily available.

- One of the more ingenious methods is by Gaspar Schott and is detailed in his book *Schola Steganographica*. It involves encoding information by matching letters to specific musical notes on a sheet. To glance at, it would appear to be a normal musical piece. If one were to actually play the piece on a musical instrument however, chances are that it would not be pleasurable to the ear. The following diagram shows an example of this method:

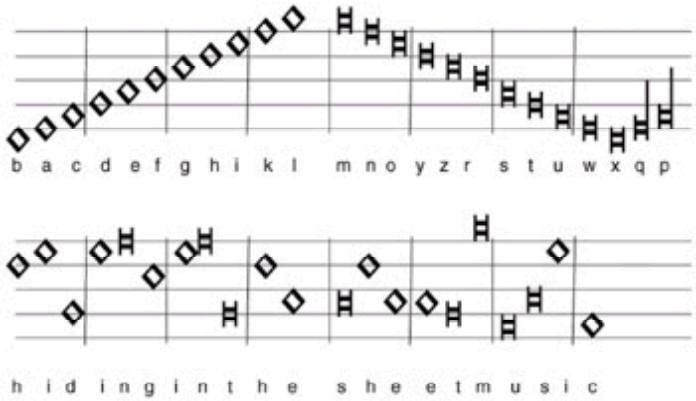
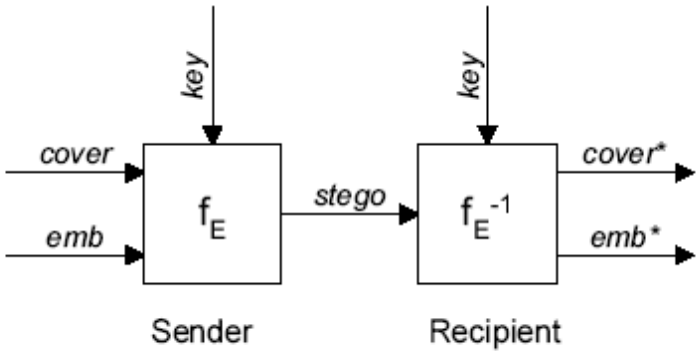


Figure 1 – Steganography in musical notes[1]

[1] Kipper, p.22

5 How does it work?

Modern day steganography mainly deals with hiding information within other files such as music or picture files. These files can "contain perceptually irrelevant or redundant information that can be substituted for hidden messages"[2]. The following diagram has been sourced from a paper presented at the 2nd workshop on Information Hiding in April 1998. It shows the basic method of how digital steganography works:



f_E: steganographic function "embedding"
f_E^{-1}: steganographic function "extracting"
cover: coverdata in which *emb* will be hidden
emb: message to be embedded
key: parameter of f_E
stego: coverdata with embedded message

Figure 2 – The Embedding Model [3]

Cover is the original picture, audio or video file. **Emb** is the embedded secret message. **Key** is the parameter which controls the hiding process of the secret message and **stego** is the resultant file that contains the hidden message. One has to be careful however of how much information they try to conceal within the carrier. "Obviously, the longer the message, the larger the modification of the carrier image and the higher the probability that the modifications can be statistically detected."[4]

There are three common techniques in use today:

- Substitution
- Injection
- Generation of new files

[2] Fridrich, p.1
[3] Zollner, p. 3
[4] Fridrich & Rue, p.2

These are detailed below:

5.1 Technique 1: Substitution

Every file that is created will contain unused or insignificant areas of data. These areas can be replaced without any discernible changes to the visual or aural clarity of the file. This enables one to conceal sensitive information within the file and still have the file appear as though it is the same as the original unmodified version. The Least Significant Bit (LSB) method replaces the last bit in an 8 bit byte. The theory is that simply replacing this bit in each byte will not be noticeable to the human eye or ear depending on the type of file.

In the following discussion, we will use the example of a picture file. If a group of bytes representing a colour in a picture was to look like:

10010110 01101010 11100101

This represents a 24 bit image (3 bytes x 8 bits). Let's suppose we changed the first bit (1) in the first byte. This being the most significant bit would mean that it changing would likely have a significant effect on the picture and be easily seen by the naked eye. However, if we change the last bit (1) in the last byte then chances are that this change would not be noticeable. This last bit is the Least Significant Bit (LSB). Therefore to conceal a message, we can use the LSB's in the picture file to structure a message to conceal within the file.

LSB works best in files that have a lot of 'noise' i.e. Pictures that have many colours and shapes or audio files that have a lot of different sounds and effects such as echoes. This is because LSB changes the value of a byte and in turn that changes the colour or sound. Therefore, the more noise in a file, the harder it will be for a human to notice any minor changes.

Substitution method generally does not increase the size of the file but depending on the size of the hidden message, it can eventually cause a noticeable change from the unmodified version. The LSB technique is commonly used in steganography applications because it is quick and easy to use. One drawback to LSB is that the technique does not take well to the file changing eg. The picture being cropped or rotated as this can destroy the hidden message.

5.2 Technique 2: Injection

Injection involves embedding the secret message directly into the carrier object. The problem with this approach is that it generally makes the file larger than the original unmodified file. While this is not an issue if an eavesdropper does not have a copy of the original file, it is one drawback of the technique. "Almost all programs today like web browsers or Microsoft

Office programs have methods of placing data in a file that will be ignored or not displayed when the program displays the file to a user"[5]. Allegedly, during the 1980's, British Prime Minister Margaret Thatcher became so irritated at the press leaks of cabinet documents that she ordered the office word processors be re-programmed to inject each user's identity in the word spacing so the press leak culprit could be identified.

5.3 Technique 3: Generation of New Files

This technique involves taking your message and using this to generate a new file from scratch. One advantage of this is that there is never an 'original' file to compare it to which improves the chances of not detecting any hidden data within the carrier.

There are a couple of good examples of this technique: 'The Prisoner's Problem' and the Spam Mimic application.

5.3.1 The Prisoner's Problem

Gus Simmons describes two people Alice and Bob who have been arrested and placed in separate jail cells. Their aim is to communicate with each other about escaping but this must be done through the warden Willie. Willie will not allow anything to be passed on that appears to contain secret information. So, Bob draws a seemingly innocuous picture that contains specific colours and patterns that Alice will instantly recognise as a message and be able to interpret it. Willie the warden will look at the picture and see harmless looking objects and pass the picture on to Alice thinking nothing of it. This also raises the possibilities of attacks by the warden Willie which is known as an active attack where his only concern is to destroy any hidden information rather than reveal its contents. This is explained further in section 9.1.1.

5.3.2 Spam Mimic

Spam Mimic is a web based application that will take your secret message and encode it into a spam message that looks a lot like a lot of other spam messages floating around the Internet. It also has an encryption option whereby you can supply a password and it will encrypt your secret message before encoding. I visited the website at www.spammimic.com and the following is the result:

[5] Hornet

Secret Message:

Visiting the SANS website can make you smarter.

Resultant email with secret message encoded within:

Dear Friend ; Your email address has been submitted to us indicating your interest in our publication . If you no longer wish to receive our publications simply reply with a Subject: of "REMOVE" and you will immediately be removed from our club . This mail is being sent in compliance with Senate bill 2016 , Title 3 , Section 302 . This is a ligitimate business proposal . Why work for somebody else when you can become rich inside 45 days . Have you ever noticed people love convenience and people love convenience . Well, now is your chance
to capitalize on this . We will help you decrease perceived waiting time by 160% & use credit cards on your website ! You are guaranteed to succeed because we take all the risk ! But don't believe us ! Prof Anderson of West Virginia tried us and says "I was skeptical but it worked for me" ! We assure you that we operate within all applicable laws . Because the Internet operates on "Internet time" you must hurry ! Sign up a friend and you'll get a discount of 30% ! Warmest regards
. Dear Friend , This letter was specially selected to be sent to you . This is a one time mailing there is no need to request removal if you won't want any more . This mail is being sent in compliance with Senate bill 1625 ; Title 5 , Section 304 ! This is a ligitimate business proposal ! Why work for somebody else when you can become rich in 99 WEEKS . Have you ever noticed how long the line-ups are at bank machines and the baby boomers are more demanding than their parents ! Well, now is your chance to capitalize on this ! WE will help YOU increase customer response by 140% & deliver goods right to the customer's doorstep ! The best thing about our system is that it is absolutely risk free for you . But don't believe us ! Mrs Simpson who resides in Arkansas tried us and says "Now I'm rich, Rich, RICH" . We are licensed to operate in all states ! DO NOT DELAY - order today ! Sign up a friend and you'll get a discount of 40% ! Thank-you for your serious consideration of our offer ! Dear Web surfer ; You made the right decision when you signed up for our mailing list . If you are not interested in our publications and wish to be removed from our lists, simply do NOT respond and ignore this mail ! This mail is being sent in compliance with Senate bill 1623 ; Title 7 , Section 303 ! This is different than anything else you've seen ! Why work for somebody else when you can become rich in 63 days . Have you ever noticed nearly every commercial on television has a .com on in it and nearly every commercial on television has a .com on in it ! Well, now is your chance to capitalize on this ! WE will help YOU increase customer response by 190% and SELL MORE . You can begin at absolutely no cost to you . But don't believe us . Prof Jones who resides in Kentucky tried us and says "My only problem now is where to park all my cars" . We are licensed to operate in all states ! Do not go to sleep without ordering . Sign up a friend and your friend will be rich too . Warmest regards !
Dear Cybercitizen , You made the right decision when you signed up for our directory ! We will comply with all removal requests ! This mail is being sent in compliance with Senate bill 2616 , Title 3 , Section 309 . Do NOT confuse us with Internet scam artists ! Why work for somebody else when you can become rich in 36 DAYS ! Have you ever noticed nobody is getting any younger and society seems to be moving faster and faster . Well, now is your chance to capitalize on this ! WE will help YOU deliver goods right to the customer's doorstep and use credit cards on your website ! You are guaranteed to succeed because we take all the risk . But don't believe us ! Ms Anderson of Montana tried us and says "Now I'm rich, Rich, RICH" ! We are a BBB member in good standing ! If not for you then for your loved ones - act now . Sign up a friend and you'll get a discount of 80% . Best regards .

Spam Mimic is also one example of a Null Cipher. Null Ciphers are a way to hide a message within another message without the use of complicated algorithms.

6 Choice of Carrier

So, what digital format should you choose to conceal your private message? Steganography can be used in just about any type of file. Here we will only discuss in detail methods used in images, audio and video. Some of the discussed methods can be used in all three but I will be concentrating on more common methods in each.

6.1 Images

6.1.1 Least Significant Bit

LSB was discussed in section 5.1 so here we will only specifically discuss its relevance to image files.
"To a computer, an image is an array of numbers that represent light intensities at various points, or pixels"[6]. An image size of 640 by 480 pixels, utilising 256 colours (8 bits per pixel) is fairly common and would contain around 300 kilobits of data. Digital images are usually in either 24-bit or 8-bit per pixel formats. 24-bit images are sometimes known as true colour images.
A 24-bit image is easier to hide messages in due to the extra bytes of information. However, because of these extra bytes, it would also be larger than an 8-bit image and the transferral of large images across the Internet can raise suspicion in certain circumstances. Therefore sometimes 8-bit images are chosen as the carrier object with a preference for grey-scale images because the colour transitions from one to another are barely noticeable i.e. changing the LSB is barely noticeable.

6.1.2 Masking

Image compression can often have an effect on the integrity of the hidden message. There are two types of image compression:

- Lossy – JPEG (Joint Photographic Experts Group) uses this format and offers the highest compression ratio.
- Lossless – BMP (Microsoft Bitmap) and GIF (Graphics Interchange Format) are two formats that provide a higher quality but less compression and therefore are easier carriers to hide messages within.

A simple conversion from a GIF or BMP format to a lossy compression format such as JPEG can destroy the hidden information in the image. Masking or filtering techniques are more effective than LSB when using JPEG images. "By covering, or masking a faint but perceptible signal with another to make the first non-perceptible, we exploit the fact that the human

[6] Sellars, section 7.1

visual system cannot detect slight changes in certain temporal domains of the image"[7]. This quote comes back to the fact that human perception does not notice minute changes in colour. However, this form of message hiding is more closely related to watermarking than steganography although the concept is the same. Watermarking is discussed in more detailed in section 8.3.
Discrete Cosine Transform is a method that suits well to concealing messages in compressed JPEG images. This method will be discussed in section 6.3.

6.2 Audio

The human ear is extremely sensitive to changes in audio patterns but is not so sensitive to differential sounds i.e. loud sounds tend to mask quiet sounds especially those of the same frequency. When concealing a secret message in an audio file, one must consider the transmission medium that the file will travel. Will it be strictly digital? i.e. computer to computer or will it pass over an analogue medium such as a home stereo or even over the air to a microphone? Some methods are more robust to manipulation and noise than others and the transmission medium must be taken into account when choosing a steganographic method. Audio steganography is a classic example of "finding and making use of "natural uncertainty" (e.g. noise)"[8]

6.2.1 Low-Bit Encoding

Data can be stored in audio files in a similar manner to LSB in image files. This is called low bit encoding but is not very immune to manipulation and produces audible noise.

6.2.2 Spread Spectrum

"Spread-spectrum encoding is the method of hiding a small or narrow-band signal, a message, in a larger cover signal"[9]. This method essentially adds seemingly random noise to the signal using a noise generator. The message is hidden within the noise of the carrier and spread across as much of the frequency spectrum as possible.

6.2.3 Echo Data Hiding

This method uses echoes in the audio stream to conceal hidden messages. Echoes when done well can often improve the aural quality of the sound rather than distort it. It works by adding an echo to the signal that varies by initial amplitude, decay rate and offset. When the time delay between the original sound and the echo decreases, it becomes less perceptible to the human ear. The timing of the delay actually signifies whether the bit of digital information is a '1' or a '0' and these delays throughout the audio file will combine together to form the secret message when decoded. "Echo hiding

[7] Bassia
[8] Wohlgemuth
[9] Kipper

was found to work exceptionally well on sound files where there is no additional degradation, such as from line noise or lossy encoding, and where there is no gaps of silence"[10].

6.2.4 Perceptual Masking

I mentioned earlier that the human ear is not so sensitive to differential sounds. Perceptual masking is the concept of hiding a sound behind another louder sound of the same frequency. We have seen this technique used many times in history, for example when someone is concerned that they will be overheard they turn up auxiliary sounds such as the stereo or television to mask their conversation. Well, this technique can be used in the same manner in steganography and is effective because of the weaknesses in the human auditory systems.

6.3 Video

Steganography in video generally uses the Discrete Cosine Transform method of manipulation. A good example for this method could be video conferencing as described by Westfeld and Wolf [14]. Video conferencing requires a high frame rate which often places great stress on digital networks. To overcome this problem, it uses differential lossy compression which means that only the differences in each successive still frame are transmitted across the wire. This method essentially eliminates the issue of image comparison to determine differences which can lead to the discovery of the use of steganography.

6.3.1 Discrete Cosine Transform (DCT)

Embedding messages in an image is seen as an effective way to hide secret data. However, image compression will destroy the integrity of the hidden message rendering it unrecoverable. The following method explains how some modern programs overcome this issue:

DCT works by using quantization on the least important parts of the image in respect to the human visual capabilities. Quantization means for example the value 5.7489763 can be rounded up to the value 6 and therefore be represented by a lot less number of bits. Of course, doing this to each and every value would produce a noticeable distortion in the image. However, the human eye under normal conditions does not detect high frequencies in images so this allows DCT to make larger modifications to these frequencies with little noticeable image distortion. DCT works by dividing the image up into smaller areas and performing the quantization on the frequencies that humans do not normally detect. This is the lossy compression stage. Any secret message is then injected at this point. The image will then be 'lossless compressed' which will not have any impact on the integrity of the secret message.

[10] Sellars, Section 8.2.4

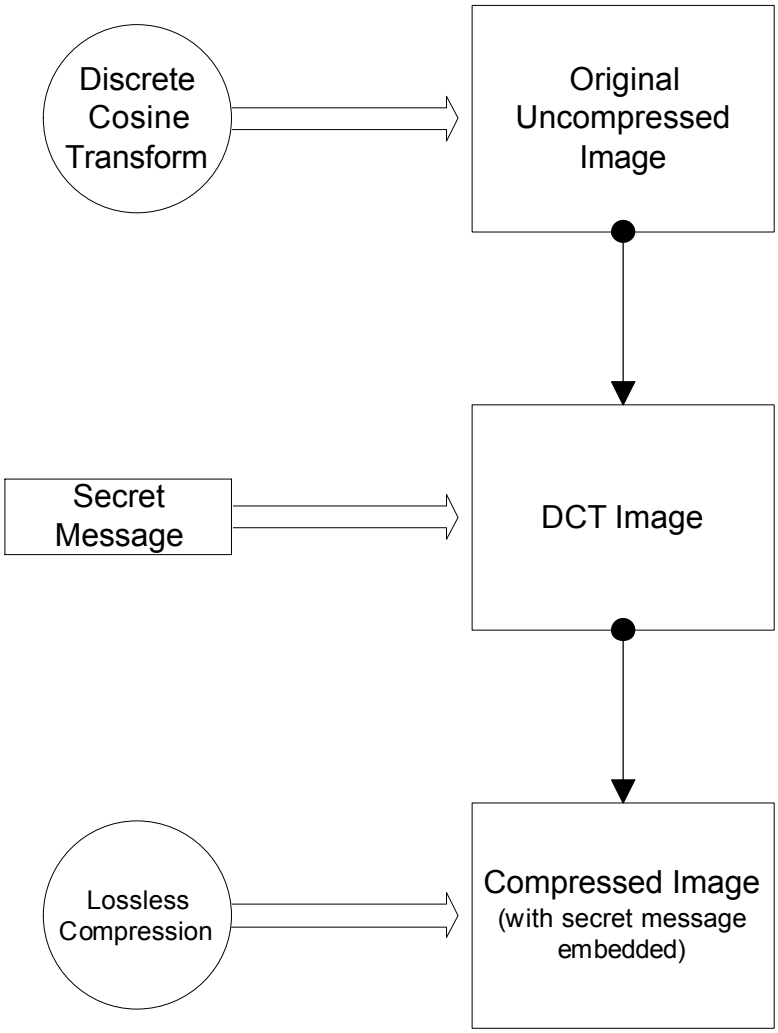


Figure 3 – Hiding a secret message in an image.

7 Steganography vs. Cryptography

Steganography: Hiding messages within carrier objects

Cryptography: Encrypting messages

Steganography has its place in security. It is not intended to replace cryptography but supplement it. Hiding a message with steganography reduces the chance of a message being detected. However, if that message is also encrypted and consequently discovered, it must also be cracked which provides another layer of protection.

One main advantage of steganography is the fact that it doesn't appear to be anything other than what it is eg. A picture or music file. An encrypted file on the other hand cries out *'I contain sensitive information!!!'* If an encrypted file were intercepted in transit or discovered in storage, it does tend to indicate that its contents are intentionally hidden and this may entice someone to attempt to decipher its contents.

To illustrate what a secret message will look like in transit, let's look at two examples. The first is a message that is concealing a secret message within a short article using the steganography program 'Snow'. The second is the same secret message encrypted with PGP v8.1 using cryptography. The secret message is: 'Meet me at The Bridge Hotel at 6pm'.

Steganography:

Victoria's mothers are getting even older. Women in Victoria are now more likely to have babies in their 40s than in their teens, leading a demographic revolution that has ended the slump in Australia's fertility.

The Bureau of Statistics reports that after sliding for years, Australia's fertility rate - the number of children women on average would bear in their lifetime at current birth rates - has levelled off at 1.75 babies per women.

Demographer Rebecca Kippen, of the Australian National University, hailed the trend as "the rise of the older women". She said women who devoted their 20s to establishing their careers and partnerships are now turning to motherhood in their 30s and 40s.

Dr Kippen said the flattening out of fertility rates challenged assumptions of a further decline ahead, which underpinned gloomy estimates this week by the Productivity Commission that an ageing population could cost Australia $2200 billion over the next 40 years.

Cryptography:

-----BEGIN PGP MESSAGE-----
Version: PGP 8.1 - not licensed for commercial use: www.pgp.com

qANQR1DBwU4DEa8FCLO4UlkQCADQb/KndQlNYArz/k3x0uAg/vVfp1YfWBkJrRhZ
NOX0TriQEvMJRpF09Kyi2NphlExuZxlOuP7D7rbX+3gdWyxwSPU8vldmLl3KpN/V
eF9dLvq5zt65avp+x2Xr8+h8A4jenoWm0STRUFYg0Oa2lXPDMV8C2qaXBHhCeAX9
ymw3MB7eaD1amnc/jyMqgqR6/S8V0cVJQ9DkvQvru5wN5K4Y7tf9RkpnS+m7Rd54
pnRaNUAPEEzeL4Y3Tr9kTMvyUpAKMluMIM2J9bd/U23T4ynL89VPQQo+4qi+E1sT

```
6sndW/p6bEUutagCfa71L91cXcbf9q079c5XhEFfEDWd+J/QB/9fTAv7wdbwhdEX
E6jKZuP+O1nxeH4E3EJE7R+vlic8lO2HKCh9fdPuTdWpemy8oSwYzczWl/fqBH4v
H7/4W2vvG+a7o3gtzgl9j0i3jl5ROXbYRN/lCOoC17bNRNPXOlTr8p/LNlkul+sw
qEsRTLmdNsg4RjfLDVSsh/T9k9T3ice7vx6lg+6b1e6D7jARL4GnXB9KaUzfGljY
WUM2n3yTawUadg7yxjzu/fAykcO4vB3bQ0minQmg7YC7jlp+AfWTJKZ9ODxWGpfh
NNR6ct/pIbzD48BFrakxOhoH+PG9+ELFi65yXIwpQFifjdVSilQfqIjjpyfHxbRF
Cz/itbh/0lYBSYm8UFYrTzr0sR/ie7RqhalHXiHV3DPCLBnQnqgGW/aWvPySyRJF
0j0ap4QAtFPezxGZywzBYvOFyiJldMkOGt8kSK6A9jXDSukemvwjuhvNDA9/tw==
=S8dp
-----END PGP MESSAGE-----
```

As one can see, to the human observer, the cryptographic message would instantly ring alarm bells and alert the observer to the fact that the communication is potentially confidential or sensitive. An encrypted file will also indicate that there may be more sensitive information travelling along this path in the future and that this connection should be monitored for the long term to try and determine patterns in the traffic to help decipher the data.

For example: “The detection of enciphered message traffic between a military soldier and a hostile government, or between a known smuggler and someone not yet under suspicion, has obvious implications”[11].

The point of all this is that if one were to monitor traffic travelling along the wire, then encrypted information would be much easier to spot than information that is concealed within another file unencrypted.
For example, most encryption applications use a header to tell the receiving application what to do with the file when decrypting it. An application could be developed to look for these headers and voila! you have your encrypted transmission and the sending and receiving headers. Alternatively the very randomness in the encrypted text can be detected to determine that a private transmission is occurring.

Eric Cole states: “In certain countries where the mere use of encryption is illegal or deemed highly suspicious, just the fact that a message or file is encrypted could raise enough suspicion to get those involved in sending and receiving it into trouble”[12] Steganography has the added benefit in that it is not subject to international law that restricts its use to the same scale as cryptography is.

[11] Anderson, p.474
[12] Cole, p3.

8 Modern Day Uses

8.1 Corporate Espionage

Trade secrets in the corporate world are an extremely valuable asset. They can reveal information which could be potentially extremely damaging to a company's profitability and sustainability. Corporate espionage is a threat to any business whose livelihood depends on information.
For example, certain company employees with appropriate privileges may be offered incentives by competitors to disclose information that could possibly give a distinct advantage to the competitor. Hence companies will go to lengths to protect their information by implementing measures such as monitoring digital networks, monitoring incoming and outgoing goods, auditing information storage practices and other general security precautions. This is why steganography has been used in the past to hide secret information in innocuous carriers and therefore bypass these protections to transfer the information to the competitor.

8.2 Terrorism

It has been suspected for some time that people have been using some form of steganography to conduct information transfer pertaining to terrorist activities. The widespread paranoia was perhaps fuelled in the first instance by the article on USA Today by Jack Kelley "Terror groups hide behind Web encryption" published on 5th Feb 2001 in which he alleges Osama Bin Laden and others have been using steganography to communicate via the Internet. However, no official proof of these covert communications has ever been produced for public examination.

8.3 Watermarking

Digital watermarking is not strictly a form of steganography for these key reasons:

- Not all watermarks are hidden
- It is not the primary purpose of a watermark to conceal its existence
- A successful attack against watermarking is not detecting its presence, it is rendering it ineffective.

However, digital watermarking does hold its place in the arena of information hiding. Digital watermarks are mainly used today as a form of copyright protection. With the digital age, came a realisation that picture, music, video, books and other forms of copyright material could be cloned perfectly and distributed many times over to multiple recipients without the original author

or artist receiving monies or recognition. This has brought about a flurry of topics, discussion and rulings between consumers, media corporations and law officials.

Digital watermarking is seen as one way to prevent people from illegally copying or modifying copyright material. Digital watermarks are also used as a means of preventing modification. Often they are placed in the most perceptually significant parts of the file so that if the file is modified it will render it useless or at the least provide significant evidence that the file has been tampered with. Another form of watermarking is the device control code which has been used in DVD's whereby the player will identify the hidden watermark on the disc which will identify to the player whether the disc is allowed to be copied once, copied many times or not to be copied at all.

However, digital watermarking is not the be-all and end-all of protecting copyright material. The research paper "Information Hiding – A Survey"[6] talks about limitations of watermarks in copyrighted software. It discusses the use of the application called StirMark[13] which "introduces random bilinear geometric distortions to de-synchronise watermarking algorithms"[14] to remove the digital watermark. This is known as an active attack in which the only goal is to remove the hidden data, not decipher it.
A technique called 'fingerprinting' is very similar to watermarking in that it embeds something within the carrier object that cannot be seen. However, fingerprinting differs in that it does not prevent copying. A serial number or copyright sign can be transparently hidden within a picture, movie, sound file, etc. in order for the originating manufacturer or artist to prove that a piece of work is legitimately theirs.

[13] Petitcolas, p1069
[14] Petitcolas, URL.

9 Detecting the use of Steganography

As mentioned previously, steganography strength lies in an eavesdropper's unawareness that a message is hidden in the carrier object. Once an object is discovered to be carrying a hidden message, then steganography has essentially lost its usefulness and the protection of the message will generally rely on the strength of the encryption process if indeed one has been used. However, encryption of the message is a cryptographic technique. The hiding of the message is a steganographic technique. Therefore, discovering the presence of a hidden message does essentially mean that you have defeated the process of steganography through steganalysis.

9.1 What is Steganalysis?

"Steganalysis is identifying the existence of a message"[15]. It does not deal with extracting the message as this encompasses in most modern day scenarios, cryptography. It is essentially a passive attack on steganography. There are two types of attacks: Active and Passive.

9.1.1 Active Attack

This involves destroying the hidden message and is more prevalent in such technologies as digital watermarking where the main purpose is to remove the mark or render it useless. Active attacks are also useful in situations where steganography is suspected to be in use but discovering the hidden message is unimportant. It works in that all objects are modified in such a manner that the object still appears to be the same but any hidden bits of information will be void. A good example is with images whereby a certain digital effect can be applied to the image without any human noticeable change but will change the bits of the embedded secret message and render it unrecoverable.

9.1.2 Passive Attack

A passive attack involves detecting the use of steganography and is a prelude to actually deciphering the hidden message.

Methods of steganalysis include:

- Viewing the file
- Listening to the file
- Performing comparisons on a file (if you have the original)
- Statistical Attack – this involves detecting changes in the patterns of pixels of Least Significant Bits.
- Signature

[15] SpyHunter – slide 16

Obviously the first two methods of analysis will not often yield accurate results. The purpose of steganography is that the changes are well **hidden**. Therefore simply viewing or listening to the file is not meant to reveal anything other than what the file appears to be. The first four methods in fact involve performing comparisons against the original file. While this can often indicate that one file is a carrier and therefore be successful, if steganography is used 'The Right Way', (see section 10) then an attacker will rarely have access to the original unmodified file. If a person is intending to use steganography to hide a secret message, it would be foolish to use a well known or readily available image or sound file to conceal the message in. Sensibility suggests that one would use a file preferably never before seen by anyone else or at the very least, chosen from an inconspicuous location on the Internet.

Steganalysis however has come in leaps and bounds in recent years and programs have been developed that are able to perform analysis on a single file and determine whether that file contains a hidden message and in some cases even identify the software application used to perform the function. This is done by identifying signatures within a file left by the particular application when performing the steganographic procedure. For example, if I were to hide a message within a file using a certain software application and then examine that file with a hex editor, I may find a specific character or group of characters that would be identical in every file I hid a message in using the same application. This group of characters is the 'signature' and steganalysis programs use this to determine the existence of a hidden message. As was mentioned before, once the existence of a message is known, the steganography has been defeated.

The authors of the research paper "Information Hiding – A Survey" propose four properties of a robust information hiding system:

1. "Marks should not degrade the perceived quality of the work"[16]
2. "Detecting the presence and/or value of a mark should require knowledge of a secret"
3. "If multiple marks are inserted in a single object, then they should not interfere with each other"
4. "The mark should survive all attacks that do not degrade the work's perceived quality"

9.2 Is Steganography in widespread use on the Internet?

There is no doubt that with the enormity and widespread usage of the Internet, that steganography will be in use in many forms for many purposes. However, an interesting study was performed by Niels Provos and Peter Honeyman from the University of Michigan to try and determine whether popular steganography applications were in fact in use on the Internet. The

[16] Petitcolas, p1073

results are detailed on their paper “Hide and Seek: An Introduction to Steganography”. During the course of their research, they downloaded approximately two million images from eBay and 1 million from Usenet with the belief that these two websites were two of the more popular for the storage of images. They used the steganalysis application ‘Stegdetect’ which detects the use of steganography in images processed by the popular applications ‘JSteg’, ‘JPHide’ and ‘OutGuess v0.13b’. A quote from the paper reads:

“For the more than two million images Crawl downloaded from eBay auctions, Stegdetect indicated that about 17,000 seemed to have steganographic content. We observed a similar detection rate for the one million images that we obtained from the Usenet archives”[17]

However, when dictionary attacks were run against these suspected steganographic images, not one single hidden message was found even though the word dictionary contained some 850,000 different words. To prove the process, they ran the attack against known steganographic images and they were shown to contain hidden data.

This study, while by no means conclusive, does encourage more discussion on the topic of steganography usage and may suggest that perhaps it is not as widespread as we thought.

[17] Provos, p12

10 Conclusion

To conclude, I would like to discuss the appropriateness of steganography as a tool to conceal highly sensitive information. There have been many discussions on whether steganography is the right method for keeping information from other than the intended recipient when other methods such as cryptography are seen as more robust. Here I will discuss the main criteria that should be followed when using steganography. If these steps are adhered to, then the detection of its use will be significantly more difficult by anyone performing steganalysis on the file. Note that most of these points probably apply to people who are perhaps already well known by authorities and are seen as having the potential to send secret information that could damage a government and/or corporation. Your average office worker for example, can probably feel safe in the fact that authorities are not performing active surveillance on every piece of information they transmit (probably).

So, here is 'The Right Way' to those wishing to use steganography to hide sensitive information:

- Anderson & Petitcolas speak about some limitations of steganography in their paper "On the Limits of Steganography". They make an important point: "what makes the case of steganography more difficult than secrecy or authenticity is that we are critically dependent on our model of the covertext"[18] Essentially what this means is that you must carefully choose what object we would like to use to embed the secret message. If chosen correctly, this is a good step towards not having your message revealed by unintended recipients. Choose images that are 'noisy' in their nature i.e. lots of colours and objects or many different sounds, etc.

- If you are a known or potential criminal, terrorist, troublemaker, etc. then suddenly sending pictures, video or audio over the Internet will most likely ring alarm bells if this is not what you commonly send to other people. One must keep within the boundaries of normal traffic patterns to avoid raising suspicion. Either that or develop new boundaries over time.

- If you send a picture containing hidden text to someone, then don't send a picture that depicts something that is completely unrelated to your life or to the text attached. A photo of a gorilla accompanied by a story about your new car will most likely look a little peculiar.

- Use a reputable steganography tool that you know does not leave a well known signature behind in the object.

- If you are concealing a secret message within an image or video then

[18] Anderson, p.477

make sure you are the one who took the photo. This ensures that you know how many copies exist and the whereabouts of all the copies.

- If using an image or video that you took, then securely destroy the original after concealing the message. Use a method that will make sure the original file cannot be recovered by any means. This will ensure that no original file exists to make a comparison to the copy that has embedded information.

- Encrypt the secret message using a well known and robust encryption algorithm.

- Communicate the shared key to your recipient well before transmitting the stego object. Do it by means that are preferably not electronic and therefore not stored digitally anywhere for someone to crack.

11 References

1. Kipper, Greg "Investigator's Guide to Steganography" Auerbach Publications, 2004

2. Fridrich, Goljan, Du. "Reliable Detection of LSB Steganography in Color and Grayscale Images" http://www.ws.binghamton.edu/fridrich/Research/acmwrkshp_version.pdf

3. Zollner, Federrath, Klimant, Pfitzmann, Piotraschke, Westfeld, Wicke, Wolf. "Modelling the security of steganographic systems" Paper presented at the 2nd Workshop on Information Hiding – April 1998, Portland.

4. Cole, Eric. "Book Excerpt: Hiding in Plain Sight" Published on Computerworld August 4th 2003. http://www.computerworld.com/printthis/2003/0,4814,83714,00.html

5. SpyHunter "Steganography & Steganalysis" Presentation made at Infosec 2004 Conference

6. Petitcolas, Fabian Anderson, Ross J Kuhn, Markus. Attacks on copyright marking systems, in David Aucsmith (Ed), "Information Hiding – A Survey", Second International Workshop, IH'98, Portland, Oregon, U.S.A., April 15-17, 1998, Proceedings, LNCS 1525, Springer-Verlag, ISBN 3-540-65386-4, pp. 219-239. and
Fabien A. P. Petitcolas. Watermarking schemes evaluation. I.E.E.E. Signal Processing, vol. 17, no. 5, pp. 58–64, September 2000.

7. Petitcolas, Fabian. "StirMark Benchmark 4.0" URL: http://www.petitcolas.net/fabien/watermarking/stirmark/index.html

8. Jiri Fridrich, Du Rui "Secure Steganographic Methods for Palette Images" http://www.ws.binghamton.edu/ fridrich/Research/ihw99_paper1.dot

9. Sellars, Duncan. "An Introduction to Steganography" URL:http://www.totse.com/en/privacy/encryption/163947.html

10. Simmons, G.J. "The Prisoner's Problem and the Subliminal Channel," Advances in Cryptology: Proceedings of CRYPTO '83, Plenum Press, 1984, pp. 51-67.

11. Hornet, Charles. "Steganography". 9th April 2002. Published on Infosecwriters.com. URL:http://www.infosecwriters.com/texts.php?op=display&id=2

12. Bassia, P and Pitas, I. Robust Audio Watermarking in the Time Domain, IX

European Signal Processing Conference (EUSIPCO'98), Rhodes, Greece, vol. I, pp. 25-28, 8-11 September 1998

13. Wohlgemuth, Sven. "Steganography and Watermarking" January 2002 Lecture to University of Freiburg. URL:http://www.informatik.uni-freiburg.de/~softech/teaching/ws01/itsec/Folien/20020108SteganographyWatermarking.1on1.pdf

14. Westfeld, Andreas Wolf, Gritta. "Steganography in a video conferencing system", IHW'98 - Proc. of the International Information hiding Workshop, April. 1998.

15. Anderson, Ross J & Petitcolas, Fabian. "On The Limits of Steganography" IEEE Journal of Selected Areas in Communications, 16(4):474-481, May 1998.