IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 10, December 2014.
www.ijiset.com
ISSN 2348 – 7968

An Insight to Steganography

Jayati Bhadra*,A.M. Bojamma*, Prasad .C.N.*, M.N. Nachappa**

*Assistant Professor, Department Of Computer Science, St. Joseph's College (Autonomous), Langford Road, Shanthinagar, Bangalore – 560027, India.
**Associate Professor, Department Of Computer Science, St. Joseph's College (Autonomous), Langford Road, Shanthinagar, Bangalore – 560027, India.

Abstract:

Steganography is a useful tool that allows us to covert transmission of information using certain means or a communications channel. Combining the channel with the encryption methods of substitution is similar to the age old method of cryptography, steganography enables the user to transmit information masked inside a file in plain view. The hidden data is both difficult to detect and when combined with known encryption algorithms, equally difficult to decipher.

Steganography is the art of hiding information and an effort to conceal the existence of the embedded information. It serves as a better way of securing message than cryptography which only conceals the content of the message not the existence of the message. Original message is being hidden within a carrier such that the changes so occurred in the carrier are not observable. In this paper we will discuss how digital images can be used as a carrier to hide messages. This paper also analyses the performance of some of the steganography tools. Steganography is a useful tool that allows covert transmission of information over the communications channel. Combining secret image with the carrier image gives the hidden image. The hidden image is difficult to detect without retrieval.

This paper will take an in-depth look at this technology by introducing the reader to various concepts of Steganography, a brief history of Steganography and a look at some of the Steganographic technique.

Keywords:

Steganography, Steganalysis, Digital watermarking, Stego key, Stego image and Cryptography.

Introduction

With the development of computer and expanding its use in different areas of life and work, the issue of information security has become increasingly important. One of the grounds discussed in information security is the exchange of information through the cover media. To this end, different methods such as cryptography, steganography, coding, etc have been used. The method of steganography is among the methods that have received attention in recent years.

Internet users frequently need to store, send, or receive private information. The most common way to do this is to transform the data into a different form. The resulting data can be understood only by those who know how to return it to its original form[13]. This method of protecting information is known as encryption. A major drawback to encryption is that the existence of data is not hidden. Data that has been encrypted, although unreadable, still exists as data. If given enough time, someone could eventually unencrypt the data. A solution to this problem is steganography[8]. The ancient art of hiding messages so

ISSN 2348 – 7968

that they are not detectable. Steganography's intent is to hide the existence of the message, while cryptography scrambles a message so that it cannot be understood.

Before the invention of digital means, traditional methods were being used for sending or receiving messages. Before phones, before mail, messages were sent on foot. For the messages where privacy was of prime concern, the ways of implementing security were following:

1. Choosing the messenger capable of delivering the message securely.
2. Write the message using such notations that actual meaning of the message was concealed.
3. Hide the message such that even its presence can't be predicted.

The main goal of steganography is to hide information in the other cover media so that other person will not notice the presence of the information[21] . This is a major distinction between this method and the other methods of covert exchange of information because, for example, in cryptography, the individuals notice the information by seeing the coded information but they will not be able to comprehend the information. However, in steganography, the existence of the information in the sources will not be noticed at all.

In steganography, the possible cover carriers are innocent looking carriers (images, audio, video, text, or some other digitally representative code) which will hold the hidden information. A message is the information hidden and may be plaintext, cipher text, images, or anything that can be embedded into a bit stream. Together the cover carrier and the embedded message create a stego-carrier.

Comparison of secret communication techniques.

Secret Communication Techniques	Confidentiality	Integrity	Un removability
Encryption	Yes	No	Yes
Digital Signatures	No	Yes	No
Steganography	Yes/No	Yes/No	Yes

Table 1

Steganography is derived from the Greek for covered writing and essentially means "to hide in plain sight". Steganography is the art of inconspicuously hiding data within data. The main goal of steganography is to hide information well enough such that the unintended recipients do not suspect the steganographic medium of containing hidden data[2]. Simple steganographic techniques have been in use for hundreds of years, but with the increasing use of files in an electronic format new techniques for information hiding have become possible[11].

Most steganography jobs have been carried out on different storage cover media like text, image, audio or video. Steganography and encryption are both used to ensure data confidentiality. However the main difference between them is that with encryption anybody can see that both parties are communicating in secret. Steganography hides the existence of a secret message and in the best case nobody can see that both parties are communicating in secret. This makes steganography suitable for some tasks for which encryption aren't, such as copyright marking. Table 1 shows a comparison of different techniques for communicating in secret[2]. Encryption allows secure communication requiring a key to read the information. An attacker cannot remove the encryption but it is relatively easy to modify the file, making it unreadable for the intended recipient.

ISSN 2348 – 7968

Comparison of Steganography and Cryptography

Steganography and cryptography are closely related. Cryptography scrambles messages so it can't be understood. Steganography on the other hand, hide the message so there is no knowledge of the existence of the message. With cryptography, comparison is made between portions of the plaintext and portions of the cipher text.

In steganography, comparisons may be made between the cover-media, the stego-media, and possible portions of the message. The end result in cryptography is the cipher text, while the end result in steganography is the stego-media. The message in steganography may or may not be encrypted. If it is encrypted, then a cryptanalysis technique is applied to extract the message.

Combination of Steganography and Cryptography

Those who seek the ultimate in private communication can combine encryption and steganography. Encrypted data is more difficult to differentiate from naturally occurring phenomena than plain text is in the carrier medium. There are several tools by which we can encrypt data before hiding it in the chosen medium.

In some situations, sending an encrypted message will across suspicion while an invisible message will not do so. Both methods can be combined to produce better protection of the message. In case, when the steganography fails and the message can be detected, it is still of no use as it is encrypted using cryptography techniques[18].

Steganalysis

Steganalysis is "the process of detecting steganography by looking at variances between bit patterns and unusually large file sizes". It is the art of discovering and rendering useless covert messages[13]. The goal of steganalysis is to identify suspected information streams, determine whether or not they have hidden messages encoded into them, and, if possible, recover the hidden information. Unlike cryptanalysis, where it is evident that intercepted encrypted data contains a message.

Steganalysis generally starts with several suspect information streams but uncertainty whether any of these contain hidden message. The steganalyst starts by reducing the set of suspect information streams to a subset of most likely altered information streams. This is usually done with statistical analysis using advanced statistics techniques.

A Brief History of Steganography

The earliest recordings of Steganography were by the Greek historian Herodotus in his chronicles known as "Histories" and date back to around 440 BC. Herodotus recorded two stories of Steganographic techniques during this time in Greece. The first stated that King Darius of Susa shaved the head of one of his prisoners and wrote a secret message on his scalp. When the prisoner's hair grew back, he was sent to the Kings son in law Aristogoras in Miletus undetected. The second story also came from Herodotus, which claims that a soldier named Demeratus needed to send a message to Sparta that Xerxes intended to invade Greece. Back then, the writing medium was text written on wax-covered tablets. Demeratus removed the wax from the tablet, wrote the secret message on the underlying wood, recovered the tablet with wax to make it appear as a blank tablet and finally sent the document without being detected.

ISSN 2348 – 7968

Romans used invisible inks which were based on natural substances such as fruit juices and milk. This was accomplished by heating the hidden text, thus revealing its contents. Invisible inks have become much more advanced and are still in limited use today.

During the 15th and 16th centuries, many writers including Johannes Trithemius (author of Steganographia) and Gaspari Schotti (author or Steganographica) wrote on Steganagraphic techniques such as coding techniques for text, invisible inks, and incorporating hidden messages in music.

Between 1883 and 1907, further development can be attributed to the publications of
Auguste Kerckhoff (author of Cryptographic Militaire) and Charles Briquet (author of Les Filigranes). These books were mostly about Cryptography, but both can be attributed to the foundation of some steganographic systems and more significantly to watermarking[8] techniques.

During the times of WWI and WWII, significant advances in Steganography took place.
Concepts such as null ciphers (taking the 3rd letter from each word in a harmless message to create a hidden message, etc), image substitution and microdot (taking data such as pictures and reducing it to the size of a large period on a piece of paper) were introduced and embraced as great steganographic techniques[14].

In the digital world of today, namely 1992 to present, Steganography is being used all over the world on computer systems. Many tools and technologies have been created that take advantage of old steganographic techniques such as null ciphers, coding in images, audio, video and microdot. With the research this topic is now getting we will see a lot of great applications for Steganography in the near future[14].

Requirements of hiding information digitally

There are many different protocols and embedding techniques that enable us to hide data in a given object[1]. However, all of the protocols and techniques must satisfy a number of requirements so that steganography can be applied correctly.

The following is a list of main requirements that steganography techniques must satisfy:

a) The integrity of the hidden information after it has been embedded inside the stego object must be correct.
b) The stego object must remain unchanged or almost unchanged to the naked eye.
c) In watermarking, changes in the stego object must have no effect on the watermark.
d) Finally, we always assume that the attacker knows that there is hidden information inside the stego object.

Hiding information may require a stego key which is additional secret information, such as a password, required for embedding the information. For example, when a secret message is hidden within a cover image, the resulting product is a stego-image.

ISSN 2348 – 7968

A possible formula of the process may be represented as:
Cover medium + embedded message + stego key = stego-medium

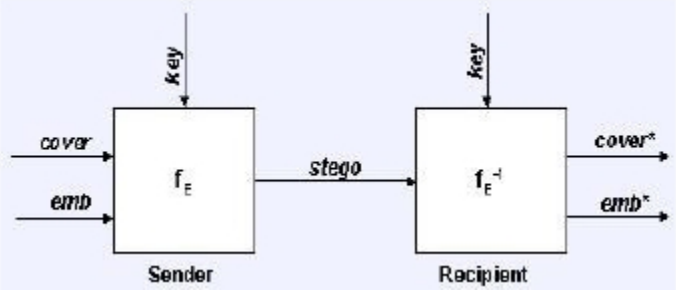


Figure 1.1 Graphical Version of the Steganographic System

Where	f_E :	Steganographic function "embedding"
	f_E^{-1} :	Steganographic function "extracting"
	cover:	Cover data in which emb will be hidden
	emb:	Message to be hidden
	stego:	Cover data with the hidden message

In this example, a secret image is being embedded inside a cover medium to produce the stego medium. The first step in embedding and hiding information is to pass both the secret message and the cover message into the encoder. Inside the encoder, one or several protocols will be implemented to embed the secret information into the cover message[1].

Having produced the stego object, it will then be sent off through some communications channel, such as email, to the intended recipient for extraction. The recipient must extract the stego object in order for them to view the secret information. The extraction process is simply the reverse of the embedding process. It is the extraction of secret data from a stego object. In the extraction process, the stego object is fed in to the system[21].

The stego key that can decode the original key that is used inside the encoding process is also needed so that the secret information can be decoded. After the decoding process is completed, the secret information embedded in the stego object can then be extracted and viewed[21].

Encoding Secret Messages in Text

Encoding secret messages in text can be a very challenging task. This is because text files have a very small amount of redundant data to replace with a secret message. Another drawback is the ease of which text based Steganography can be altered by an unwanted parties by just changing the text itself or reformatting the text to some other form (from .TXT to .PDF, etc.). There are numerous methods by which to accomplish text based Steganography[4]. Wewill introduce a few of the more popular encoding methods below.

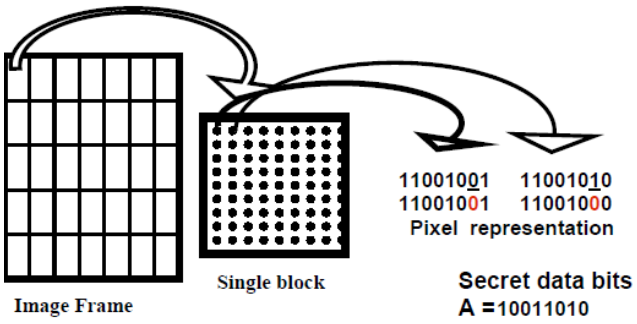
Line-shift encoding involves actually shifting each line of text vertically up or down by as little as 3 centimeters. Depending on whether the line was up or down from the stationary line would equate to a value that would or could be encoded into a secret message[19].

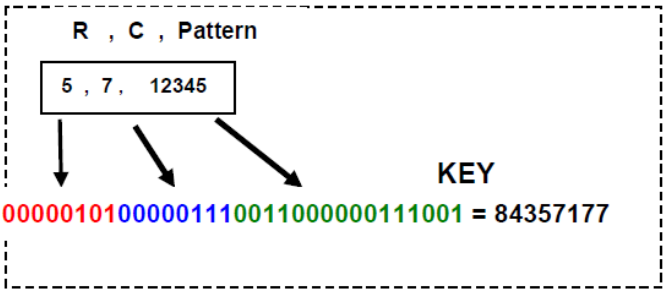
ISSN 2348 – 7968

Word-shift encoding works in much the same way that line-shift encoding works, only we use the horizontal spaces between words to equate a value for the hidden messag[11] e. This method of encoding is less visible than line-shift encoding but requires that the text format support variable spacing.

Feature specific encoding involves encoding secret messages into formatted text by changing certain text attributes such as vertical/horizontal length of letters such as b, d, T, etc. This is by far the hardest text encoding method to intercept as each type of formatted text has a large amount of features that can be used for encoding the secret message[4].

All three of these text based encoding methods require either the original file or the knowledge of the original files formatting to be able to decode the secret message.





Encoding Secret Messages in Images

Coding secret messages in digital images is by far the most widely used of all methods in the digital world of today. This is because it can take advantage of the limited power of the human visual system (HVS). Almost any plain text, cipher text, image and any other media that can be encoded into a bit stream can be hidden in a digital image.

With the continued growth of strong graphics power in computers and the research being put into image based Steganography, this field will continue to grow at a very rapid pace.

Before diving into coding techniques for digital images, a brief explanation of digital image architecture and digital image compression techniques should be explained.
As Duncan Sellars [7] explains "To a computer, an image is an array of numbers that represent light intensities at various points, or pixels. These pixels make up the images raster data." When dealing with digital images for use with Steganography, 8-bit and 24-bit per pixel image files are typical. Both have advantages and disadvantages, as we will explain below.

ISSN 2348 – 7968

8-bit images are a great format to use because of their relatively small size. The drawback is that only 256 possible colors can be used which can be a potential problem during encoding. Usually a gray scale color palette is used when dealing with 8-bit images such as (.GIF) because its gradual change in color will be harder to detect after the image has been encoded with the secret message. 24-bit images offer much more flexibility when used for Steganography. The large numbers of colors (over 16 million) that can be used go well beyond the human visual system (HVS), which makes it very hard to detect once a secret message, has been encoded. The other benefit is that a much larger amount of hidden data can be encoded into a 24-bit digital image as opposed to an 8-bit digital image. The one major drawback to 24-bit digital images is their large size (usually in MB) makes them more suspect than the much smaller 8-bit digital images (usually in KB) when sent over an open system such as the Internet[3]..

Digital image compression is a good solution to large digital images such as the 24-bit images mentioned earlier. There are two types of compression used in digital images, lossy and lossless. Lossy compression such as (.JPEG) greatly reduces the size of a digital image by removing excess image data and calculating a close approximation of the original image.

Lossy compression is usually used with 24-bit digital images to reduce its size, but it does carry one major drawback. Lossy compression techniques increase the possibility that the uncompressed secret message will lose parts of its contents because of the fact that lossy compression removes what it sees as excess image data. Lossless compression techniques, as the name suggests, keeps the original digital image in tact without the chance of loss. It is for this reason that it is the compression technique of choice for steganographic uses. Examples of lossless compression techniques are (.GIF and .BMP). The only drawback to lossless image compression is that it doesn't do a very good job at compressing the size of the image data.

We will now discuss a couple of the more popular digital image encoding techniques used today. They are least significant bit (LSB) encoding and masking and filtering techniques[3].

Least significant bit (LSB) encoding is by far the most popular of the coding techniques used for digital images. By using the LSB of each byte (8 bits) in an image for a secret message, you can store 3 bits of data in each pixel for 24-bit images and 1 bit in each pixel for 8-bit images. As you can see, much more information can be stored in a 24-bit image file.

Depending on the color palette used for the cover image (i.e., all gray), it is possible to take 2 LSB's from one byte without the human visual system (HVS) being able to tell the difference. The only problem with this technique is that it is very vulnerable to attacks such as image changes and formatting (i.e., changing from .GIF to .JPEG).

Masking and filtering techniques for digital image encoding such as Digital Watermarking (i.e.- integrating a companies logo on there web content) are more popular with lossy compression techniques such as (.JPEG). This technique actually extends an images data by masking the secret data over the original data as opposed to hiding information inside of the data. Some experts argue that this is definitely a form of Information Hiding, but not technically Steganography[3]. The beauty of Masking and Filtering techniques are that they are immune to image manipulation which makes there possible uses very robust.

ISSN 2348 – 7968

As a side note, there are many other techniques that are not covered in this paper that should be researched by anyone interested in using digital images for steganographic purposes[3]. Techniques that use complex
algorithms, image transformation techniques and image encryption techniques are still relatively new, but show promise to be more secure and robust ways to use digital images in Steganography.

Original Image

Stego Image

Encoding Messages in Audio

Encoding secret messages in audio is the most challenging technique to use when dealing with Steganography. This is because the human auditory system (HAS) has such a dynamic range that it can listen over. To put this in perspective, the (HAS) perceives over a range of power greater than one million to one and a range of frequencies greater than one thousand to one making it extremely hard to add or remove data from the original data structure.

The only weakness in the (HAS) comes at trying to differentiate sounds (loud sounds drown out quiet sounds) and this is what must be exploited to encode secret messages in audio without being detected[6].

There are two concepts to consider before choosing an encoding technique for audio. They are the digital format of the audio and the transmission medium of the audio.
There are three main digital audio formats typically in use. They are Sample Quantization, Temporal Sampling Rate and Perceptual Sampling.

Sample Quantization which is a 16-bit linear sampling architecture used by popular audio formats such as (.WAV and. AIFF). Temporal Sampling Rate uses selectable frequencies (in the KHz) to sample the audio. Generally, the higher the sampling rate is, the higher the usable data space gets. The last audio format is Perceptual Sampling. This format changes the statistics of the audio drastically by encoding only the parts the listener perceives, thus maintaining the sound but changing the signal. This format is used by the most popular digital audio on the Internet today in ISO MPEG (MP3) [9].

Transmission medium (path the audio takes from sender to receiver) must also be considered when encoding secret messages in audio. W. Bender [8] introduces four possible transmission mediums:

1. Digital end to end - from machine to machine without modification.
2. Increased/decreased resampling - the sample rate is modified but remains digital.
3. Analog and resampled - signal is changed to analog and resampled at a different rate.
4. Over the air - signal is transmitted into radio frequencies and resampled from a microphone.

We will now look at three of the more popular encoding methods for hiding data inside of audio. They are low-bit encoding, phase-coding and spread spectrum. Low-bit encoding embeds secret data into the least

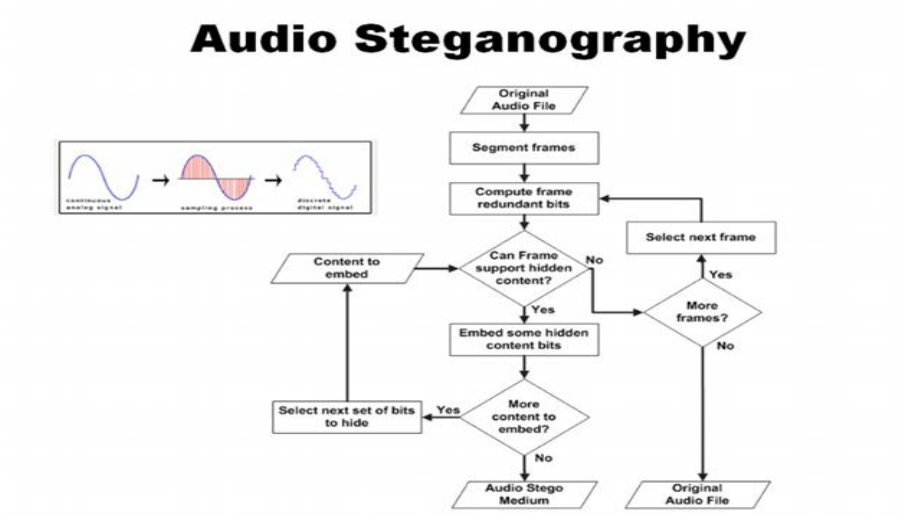
ISSN 2348 – 7968

significant bit (LSB) of the audio file. The channel capacity is 1KB per second per kilohertz (44 kbps for a 44 KHz sampled sequence). This method is easy to incorporate but is very susceptible to data loss due to channel noise and resampling.

Phase coding substitutes the phase of an initial audio segment with a reference phase that represents the hidden dat[9] a. This can be thought of, as sort of an encryption for the audio signal by using what is known as Discrete Fourier Transform (DFT), which is nothing more than a transformation algorithm for the audio signal.

Spread spectrum encodes the audio over almost the entire frequency spectrum. It then transmits the audio over different frequencies which will vary depending on what spread spectrum method is used. Direct Sequence Spread Spectrum (DSSS) is one such method that spreads the signal by multiplying the source signal by some pseudo random sequence known as a (CHIP). The sampling rate is then used as the chip rate for the audio signal communication.

Spread spectrum encoding techniques are the most secure means by which to send hidden messages in audio, but it can introduce random noise to the audio thus creating the chance of data loss.



Applications for Steganography

There are many applications for Steganography, some good and some bad, which brings us to the closing section of our in-depth look at Steganography in which we will look at Steganalysis. Steganalysis is the art and science of stopping or detecting the use of all steganographic techniques mentioned earlier. In Steganalysis, the goal is to be able to compare the cover-object (cover message), the stego-object (the cover message with the hidden data embedded in it) and any possible portions of the stego-key (encryption method) in an effort to intercept, analyze and/or destroy the secret communication. As Fabien A.P. Petitcolas points out in his book, there are six general protocols used to attack the use of Steganography.

1. Stego only attack - only the stego object is available for analysis
2. Known cover attack - the original cover object and the stego object are available for analysis.
3. Known message attack - the hidden message is available to compare with the stego-object.
4. Chosen stego attack - the stego tool (algorithm) and stego-object are available for analysis.
5. Chosen message attack - takes a chosen message and generates a stego object for future analysis.

ISSN 2348 – 7968

6. Known stego attack - the stego tool (algorithm), the cover message and the stego-objects are available for analysis.

Being that Steganalysis is a broad topic and one that merits a paper on just it, I will close this discussion of Steganalysis by showing the reader one example of how someone could detect the use of steganographic tools that change the least significant bit (LSB) of an image in order to embed secret data inside of it.

Generally, bitmap images (.BMP) have known and predictable characteristics. One such characteristic is the probability of near duplicate colors. Bitmap images get their color from a central color table, which by its nature have little, or no near duplicate colors. When hidden data is embedded into the (LSB) of a bitmap image, it increases the number of near duplicate colors dramatically. Generally speaking, any bitmap image with more than fifty near duplicate colors should raise the suspicion of embedded data being present.

Steganography is applicable to, but not limited to, the following areas.

1. Confidential communication and secret data storing
2. Protection of data alteration
3. Access control system for digital content distribution
4. Media Database systems

The area differs in what feature of the steganography is utilized in each system.

A. Confidential communication and secret data storing

The "secrecy" of the embedded data is essential in this area. Historically, steganography have been approached in this area. Steganography provides us with:

1. Potential capability to hide the existence of confidential data
2. Hardness of detecting the hidden (i.e., embedded) data
3. Strengthening of the secrecy of the encrypted data

In practice, when you use some steganography, you must first select a vessel data according to the size of the embedding data. The vessel should be innocuous. Then, you embed the confidential data by using an embedding program (which is one component of the steganography software) together with some key. When extracting, you (or your party) use an extracting program (another component) to recover the embedded data by the same key ("common key" in terms of cryptography). In this case you need a "key negotiation" before you start communication.

Attaching a stego file to an e-mail message is the simplest example in this application area. But you and your party must do a "sending-and-receiving" action that could be noticed by a third party. So, e-mailing is not a completely secret communication method.

There is an easy method that has no key-negotiation. We have a model of "Anonymous Covert Mailing System." See the reference [7].

There is some other communication method that uses the Internet Webpage. In this method you don't need to send anything to your party, and no one can detect your communication. This method is shown in the other page.

ISSN 2348 – 7968

Each secrecy based application needs an embedding process which leaves the smallest embedding evidence. You may follow the following.

1. Choose a large vessel, larger the better, compared with the embedding data.
2. Discard the original vessel after embedding.

For example, in the case of Qtech Hide & View, it leaves some latent embedding evidence even if the vessel has a very large embedding capacity. You are recommended to embed only 25% or less (for PNG / BMP output) of the maximum capacity, or only 3% of the vessel size (for JPEG output)..

B. Protection of data alteration

We take advantage of the fragility of the embedded data in this application area.

We asserted in the Home Page that "the embedded data can rather be fragile than be very robust." Actually, embedded data are fragile in most steganography programs. Especially, Qtech Hide & View program embeds data in an extremely fragile manner[20]. We demonstrate this in the other page.

However, this fragility opens a new direction toward an information-alteration protective system such as a "Digital Certificate Document System." The most novel point among others is that "no authentication bureau is needed." If it is implemented, people can send their "digital certificate data" to any place in the world through Internet. No one can forge, alter, nor tamper such certificate data. If forged, altered, or tampered, it is easily detected by the extraction program. Just visit this page and see the reference [9].

C. Access control system for digital content distribution

In this area embedded data is "hidden", but is "explained" to publicize the content.

Today, digital contents are getting more and more commonly distributed over Internet than before. For example, music companies release new albums on their Webpage in a free or charged manner. However, in this case, all the contents are equally distributed to the people who can make access to the page. So, an ordinary Web distribution scheme is not suited for a "case-by-case" and "selective" distribution. Of course it is always possible to attach digital contents to e-mail messages and send them to the customers. But it will takes a lot of cost in time and labor.

If you have some valuable content, which you think it is distributable if someone really needs it, and if it is possible to upload that content on Internet in some covert manner. And if you can issue a special "access key" to extract the content selectively, you will be very happy about it. A steganographic scheme can help realize this type of system.

We have developed a prototype of an "Access Control System" for digital content distribution through Internet. The following steps explain the scheme.

1. A content owner classify his/her digital contents in a folder-by-folder manner, and embed the whole folders in some large vessel according to a steganographic method using folder access keys, and upload the embedded vessel (stego data) on his/her own Webpage.
2. On that Webpage the owner explains the contents in depth and publicize worldwide. The contact information to the owner (post mail address, e-mail address, phone number, etc.) will be posted there.

ISSN 2348 – 7968

3. The owner may receive an access-request from a customer who watched that Webpage. In that case, the owner may (or may not) creates an access key and provide it to the customer (free or charged).

In this mechanism the most important point is, a "selective extraction" is possible or not.

In fact we have already developed such a selective extraction program to implement the system. However, we will not go down to the details about this.

D. Media Database systems

In this application area of steganography secrecy is not important, but unifying two types of data into one is the most important.

Media data (photo picture, movie, music, etc.) have some association with other information. A photo picture, for instance, may have the following.

1. The title of the picture and some physical object information
2. The date and the time when the picture was taken
3. The camera and the photographer's information

Formerly, these are annotated beside the each picture in the album.

Recently, almost all cameras are digitalized. They are cheap in price, easy to use, quick to shoot. They eventually made people feel reluctant to work on annotating each picture. Now, most home PC's are stuck with the huge amount of photo files. In this situation it is very hard to find a specific shot in the piles of pictures. A "photo album software" may help a little. You can sort the pictures and put a couple of annotation words to each photo. When you want to find a specific picture, you can make a search by keywords for the target picture. However, the annotation data in such software are not unified with the target pictures. Each annotation only has a link to the picture. Therefore, when you transfer the pictures to a different album software, all the annotation data are lost.

This problem is technically referred to as "Metadata (e.g., annotation data) in a media database system (a photo album software) are separated from the media data (photo data) in the database managing system (DBMS)." This is a big problem.

Steganography can solve this problem because a steganography program unifies two types of data into one by way of embedding operation. So, metadata can easily be transferred from one system to another without hitch. Specifically, you can embed all your good/bad memory (of your sight-seeing trip) in each snap shot of the digital photo. You can either send the embedded picture to your friend to extract your memory on his/her PC, or you may keep it silent in your own PC to enjoy extracting the memory ten years after. Qtech Hide & View v02 may be a good program for such purposes.

If a "motion picture steganography system" has been developed in the near future, a keyword based movie-scene retrieving system will be implemented. It will be a step to a "semantic movie retrieval system."

ISSN 2348 – 7968

Conclusion and future scope

Steganography transmits secrets through apparently innocuous covers in an effort to conceal the existence of a secret. Digital image steganography and its derivatives are growing in use and application. In areas where cryptography and strong encryption are being outlawed, citizens are looking at steganography to circumvent such policies and pass messages covertly. As with the other great innovations of the digital age: the battle between cryptographers and cryptanalysis, security experts and hackers, record companies and pirates, steganography and Steganalysis will continually develop new techniques to counter each other.

In the near future, the most important use of steganographic techniques will probably be lying in the field of digital watermarking. Content providers are eager to protect their copyrighted works against illegal distribution and digital watermarks provide a way of tracking the owners of these materials. Steganography might also become limited under laws, since governments already claimed that criminals use these techniques to communicate.

The possible use of steganography technique is as following:

- Hiding data on the network in case of a breach.
- Peer-to-peer private communications.
- Posting secret communications on the Web to avoid transmission.
- Embedding corrective audio or image data in case corrosion occurs from a poor connection or transmission.

References

[1] Ahsan K., and Kundur D., “Practical Internet Steganography: Data Hiding in IP” found online at http://www.ece.tamu.edu/~deepa/pdf/txsecwrksh03.pdf.
[2] Anderson R.J. and Petitcolas F.A.P., “On the Limits of steganography,” J. Selected Areas in Comm., vol. 16, no.4, 1998, pp. 474–481.
[3] Bailey, K. and Curran, K. “An evaluation of image-based steganography methods”. International Journal of Digital Evidence, Fall 2003.
[4] Chapman, M. Davida G, and Rennhard M.. “A Practical and Effective Approach to Large-Scale Automated Linguistic Steganography” found online at http://www.nicetext.com/doc/isc01.pdf
[5] Dai Y., Liu G., and WangBreaking Z., “Predictive-Coding- Based Steganography and Modification for Enhanced Security”, IJCSNS International Journal of Computer Science and Network Security, vol.6 no. 3b, March 2006.
[6] Chin-Chen Chang , Iuan-Chang Lin, and Yaun-Hui YU, “ A new Steganographic method for color and gray scale image hiding”, Computer Vision and Image Understanding, 20 December 2006.
[7] Shareza Shirali, M.H, “Anew Approach to persain/Arabic Text Stegraphy”, Computer and Information Science, 2006, ICISCOMSAR 2006, 5th IEEE/ACIS International Conference, 10-12 July 2006 pp 310-315.
[8] Fabien A.P., and Petitcolas, “Information Hiding: Techniques for Steganography and Digital Watermarking.”, 2000.
[9] National Academy of Sciences, How do Wavelets work? National Academy of Sciences, http://www.beyonddiscovery.org/content/view.page.asp?I=1956, 2003 .
[10] Digital Watermarking for Digital Media, Information Science Publishing.
[11] Hiding in Plain Sight: Steganography and the Art of Covert Communication Cole, Eric.
[12] Information Hiding: Steganography and Watermarking Attacks and Countermeasures (Advances in Information Security, Volume 1) Johnson, Neil F. / Doric, Zoran / Jajodia.
[13] Computerworld. Steganography: Hidden Data. Quick study by Deborah Radcliff. [Online] 2002.

ISSN 2348 – 7968

http://www.computerworld.com/securitytopics/security/story/0,10801,71726,00. html.
[14] SANS Security Essentials, (volume 1.4, chapter 4) Encryption and Exploits, 2001.
[15] Petitcolas, Fabien A.P., "Information Hiding: Techniques for Steganography and Digital Watermarking.", 2000.
[16] StegoArchive, "Steganography Information, Software and News to enhance your Privacy", 2001, URL: www.StegoArchive.com
[17] Petitcolas, Fabien A.P., "The Information Hiding Homepage: Digital Watermarking and Steganography", URL: http://www.cl.cam.ac.uk/~fapp2/steganography/
[18] Johnson, Neil F., "Steganography", 2000, URL: http://www.jjtc.com/stegdoc/index2.html
[19] The WEPIN Store, "Steganography (Hidden Writing)", 1995, URL: http://www.wepin.com/pgp/stego.html
[20] Sellars, D., "An Introduction to Steganography", URL: http://www.cs.uct.ac.za/courses/CS400W/NIS/papers99/dsellars/stego.html
[21] Bender, W., "Techniques for Data Hiding", IBM Systems Journal, Vol. 35, Nos 3+4, Pgs 313-336, 1996

References not directly used in this paper

[22] Krinn, J., "Introduction to Steganography", 2000, URL: http://rr.sans.org/covertchannels/steganography.php
[23] Noto, M., "MP3Stego: Hiding Text in MP3 files", 2001, URL: http://rr.sans.org/covertchannels/mp3stego.php