SECURITY THROUGH OBSCURITY

Dr.K.Duraiswamy , B.E.,M.Sc.,(Engg),Ph.D., MISTE.,MCSI.,SMIEEE.,
Principal,
K.S.R. College Of Technology,
Tiruchengode.

&

Mrs. R.Uma Rani M.C.A., M.Phil., (Ph.D.,)
Lecturer (S.S) in Computer Science,
Sri Sarada College For Women (Autonomous),
Salem-16.
e_mail : r_umarani@yahoo.com

ABSTRACT:

Steganography is the art of hiding information in ways that prevent its detection. Steganography is usually given as a synonym for **cryptography** but it is not normally used in that way. It is not intended to replace cryptography but supplement it. Though steganography is an ancient craft, the onset of computer technology has given it new life. Computer-based steganographic techniques introduce changes to digital covers to embed information foreign to the native covers. Such information may be communicated in the form of text, binary files, or provide additional information about the cover and its owner such as digital watermarks or fingerprints. This paper explains a ***new algorithm*** which describes how **steganography** can be combined with **cryptography** to enhance security in data transfer.

Digital images, audio and video files are composed of collections of bits that are translated by their related software into images, sounds or videos. These files contain unused areas or data that is insignificant and can be overwritten. By using this proposed algorithm, we can hide our file of any format in an image. It will not be obvious that the image also contains a secret data in it. We can then send the image via e-mail attachment or post it on the web site and anyone with knowledge that it contains secret information, and who is in possession of the encryption password, will be able to open the file, extract the secret information and decrypt it.

This **paper** aims to outline a general introduction to ***cryptography and steganography***, explains the differences between these two techniques, elucidates the ***proposed algorithm***, and illustrates how security is enhanced using this ***algorithm.***

Keywords: Cryptography, Steganography, information hiding, digital image, digital watermarking.

1. INTRODUCTION TO CRYPTOGRAPHY

Cryptography is the study of methods of sending messages in disguised form so that only the intended recipients can remove the disguise and read the message. Cryptography, broadly defined, is the science that studies a wide range of issues in the transmission and safeguarding of information.

In cryptographic terms, ***Clear Text*** is the text which is to be encrypted, and ***Cipher Text*** is the
encrypted clear text.

Cryptographic systems are generically classified along three independent dimensions

1. ***The type of operations used for transforming plaintext to cipher text.*** *All encryption algorithms are based on two general principles:* ***substitution****, in which each element in the plaintext is mapped into another element, and* ***transposition****, in which elements in the plaintext are rearranged. The fundamental requirement is that no information be lost.*

2. ***The number of keys used.*** If both sender and receiver use the same key, the system is referred to as **symmetric**, single-key, secret-key, or conventional encryption. If the sender and receiver each uses a different key, the system is referred to as **asymmetric** , two-keys, or public-key encryption.

3. ***The way in which the plaintext is processed:*** A **block cipher** processes the input one block of elements at a time, producing an output block for each input block. A **stream cipher** processes the input elements continuously, producing output one element at a time, as it goes along.

The proposed algorithm uses a **substitution** cipher method. It is a **symmetric key** algorithm using the technique of **block cipher.**

2. INTROUDUCTION TO STEGANOGRAPHY

Steganography literally means covered writing. Its goal is to hide the fact that communication is taking place. This is often achieved by using a (rather large) cover file and embedding the (rather short) secret message into this file. The result is an innocuous looking file (the stego file) that contains the secret message. It has until recently been the poor cousin of cryptography. Now, it is gaining new popularity with the current industry demands for digital watermarking and fingerprinting of audio and video. There are three different aspects in information-hiding systems contend with each other: **capacity, security and robustness**. Capacity refers to the amount of information that can be hidden in the cover medium, security to an eavesdropper's inability to detect hidden information and robustness to the amount of modification the stego medium can withstand before an adversary can destroy the hidden information.

In the field of steganography, some terminology has been developed, as explained below.
The adjectives ***cover, embedded*** **and** ***stego*** were defined at the Information Hiding Workshop held in Cambridge, England. The term **``cover''** is used to describe the original, innocent message, data, audio, still, video and so on. The information to be hidden in the cover data is known as the **``embedded''** data. The **``stego''** data is the data containing both the cover signal and the ``embedded'' information. Logically, the processing of putting the hidden or embedded data, into the cover data, is sometimes known as embedding. Occasionally, especially when referring to image steganography, the cover image is known as the *container*.

2.1 How does steganography work?

Digital images, audio and video files are composed of collections of bits that are translated by their related software into images, sounds or videos. These files contain unused areas or data that is insignificant and can be overwritten. By using this proposed algorithm, we can hide our text in an image. It will not be obvious that the image also contains text. We can then send the image via e-mail attachment or post it on the web site and anyone with knowledge that it contains secret information, and who is in possession of the encryption password, will be able to open the

file, extract the secret information and decrypt it.

3. CRYPTOGRAPHY & STEGANOGRAPHY: A COMPARISON

While **cryptography** is about protecting the content of messages (their meaning), **steganography** is about concealing their very existence. It comes from Greek roots, literally means 'covered writing', and is usually interpreted to mean hiding information in other information. Examples include sending a message to a spy by marking certain letters in a newspaper using invisible ink, and adding sub-perceptible echo at certain places in an audio recording. It is often thought that communications may be secured by encrypting the traffic, but this has rarely been adequate in practice. Eneas the Tactician, and other classical writers, concentrated on methods for hiding messages rather than for enciphering them; and although modern cryptographic techniques started to develop during the Renaissance, we find in 1641 that John Wilkins still preferred hiding over ciphering because it arouses less suspicion. This preference persists in many operational contexts to this day. For example, an encrypted email message between a known drug dealer and somebody not yet under suspicion, or between an employee of a defense contractor and the embassy of a hostile power, has obvious implications. A message in ciphertext may arouse suspicion while an *invisible* message will not. In contrast to cryptography, where the "enemy" is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem, the goal of steganography is to hide messages inside other "harmless" messages in a way that does not allow any "enemy" to even detect that there is a second secret message present.

As the purpose of ***steganography*** is having a covert communication between two parties whose existence is unknown to a possible attacker, a successful attack consists in detecting the existence of this communication (e.g., using statistical analysis of images with and without hidden information). **Digital watermarks** are pieces of information added to digital data/audio, video or still images that can be detected or extracted later to make an assertion about the data. These digital watermarks remain intact under transmission/transformation, allowing us to protect our ownership rights in digital form. Technically, watermarking is not a steganographic form. Strictly, steganography conceals data in the image, watermarking extends the image information and becomes an attribute of the cover image, providing license, ownership or copyright details. **Watermarking**, as opposed to steganography, has the (additional) requirement of robustness against possible attacks. In this context, the term 'robustness' is still not very clear; it mainly depends on the application. Copyright marks do not always need to be hidden, as some systems use *visible digital watermarks*, but most of the literature has focused on imperceptible (e.g., invisible, inaudible) digital watermarks which have wider applications. Visible digital watermarks are strongly linked to the original paper watermarks which appeared at the end of the 13^{th} century to differentiate paper makers of that time. Modern visible watermarks may be visual patterns (e.g., a company logo or copyright sign) overlaid on digital images. The intent of use is also different: the payload of a watermark can be perceived as an attribute of the cover-signal (e.g., copyright information, license, ownership, etc.). In most cases the information hidden using steganographic techniques is not related at all to the cover. These differences in goal lead to very different hiding techniques. A watermarking system's primary goal is to achieve a high level of robustness- that is, it should be impossible to remove a watermark without degrading the data object's quality. Steganography, on the other hand , strives for high **security and capacity**, which often entails that the hidden information is fragile. Even trivial modifications to the stego medium can destroy it.

4.***PROPOSED SYSTEM*:**

ENHANCING DATA SECURITY BY COMBINING CRYPTOGRAPHY WITH STEGANOGRAPHY

Ensuring data security is a big challenge for computer users. Businessmen, professionals, and home users all have some important data that they want to secure from others. There are a number of ways for securing data. Encryption is one of them, and here we have the software for data encryption and then embed the cipher text

in an image. Using cryptography, the data is transformed into some other gibberish form and then the encrypted data is transmitted. In steganography, the data is embedded in an image file and the image file is transmitted. But this algorithm combines the effect of these two methods to enhance the security of the data. The proposed algorithm encrypts the data with a crypto algorithm and then embeds the encrypted text in an image file. This algorithm improves the security of the data by embedding the encrypted text and not the plain text in an image.

To **conceal** a message

Plain text -→ encryption → concealment of text

To **extract** a message

Concealed text → decryption → plain text

***4.1. Encryption* :**

The encryption algorithm built in is a **block cipher algorithm.** A block cipher operates on blocks of data. When we give the algorithm a chunk of data, to encrypt/ decrypt, it breaks the plaintext into blocks and operates on each block independently. Unlike other block cipher algorithms, which have a fixed block size of 8/16 bytes, this proposed algorithm provides a variable block size for each message. This algorithm fixes the block size as the length of the password supplied by the user. Hence the block size varies from one message to another sent by the same user but with different passwords.

The algorithm runs in a **cipher block-chaining** mode. In this mode, we generate the current cipher block from the previous cipher block and the current plain text block. This technique ensures that any duplicate block in the plaintext does not encrypt to the same cipher text block. It also provides the best possible security when different messages are encrypted with the same password. Hence a hacker may not be able to locate any redundant codes in the cipher text, which makes the decryption process complicated, without applying the same algorithm.

Block cipher method:

A block cipher is a type of symmetric key encryption algorithm that transforms a fixed-length block of plaintext data into a block of cipher text data of the same length. This transformation takes places under the action of a user-provided secret key. Applying the reverse transformation to the cipher text block using the same secret key performs decryption. The fixed length is called the block size.

When we use a block cipher to encrypt a message of arbitrary length, we use techniques known as modes of operation for the block cipher. To be useful, a mode must be at least as secure and as efficient as the underlying cipher. One such mode is **cipher block chaining mode**. **CBC** mode is as secure as the underlying block cipher against standard attacks. The speed of encryption is identical to that of the block cipher, but the encryption process cannot be easily parallel zed, although the decryption process can be.

With a block cipher, we can **reuse** keys. The stream cipher is like a one-time pad. "one-time" implies that we should use a pad only once. Similarly we should use a stream cipher key only once. Hence the stream cipher algorithms generate the key by using a random number generator. But when it becomes necessary to encrypt many things using the same key (like file encryption), block cipher proves to be stronger. For file encryption, block cipher method is more suited because we can encrypt each file with the same key and then protect that key.

Cipher block chaining encryption mode:

In cipher block chaining mode, each plain text block is XOR ed with the previous cipher text block and then encrypted. An initialization vector is used as a '**seed'** for the process. **CBC** mode is as secure as the underlying block cipher against standard attacks. In addition, the XOR ing of the previous cipher text block with the current plaintext block conceals any patterns in the plaintext. The plaintext cannot be directly manipulated except by removal of blocks from the beginning or the end of the cipher text. The initialization vector is different for any two messages encrypted with different keys and is preferably randomly chosen. The speed of encryption is identical to that of the block cipher.

Encryption method:

1. Initialization vector is set to the password and is packed into an array.
2. For the first iteration, initialization vector is XOR ed with the current plain text block to generate the cipher text block.

3. For other iterations,
    i. the current plain text block is XOR ed with the previous cipher text block to generate the current cipher text block.
    ii. Initialization vector is set to the current cipher text block.

4.2. Embed data in an image: Image steganography:

Before proceeding into the algorithm, a small note on how images are stored into files. To a computer, an image is an array of numbers that represent light intensities at various points, or pixels. These pixels make up the image's raster data. An image size of 640 x 480 pixels, utilizing 256 colours (8 bits per pixel) is fairly common. Digital images are typically stored in either 24-bit or 8-bit per pixel files. 24-bit images are known as true colour images. Obviously, a 24-bit image provides more space for hiding information; however, a 24-bit images are generally large and not that common. A 24-bit image 1024 pixels wide by 768 pixels high would have a size in excess of 2MB.

Alternatively, 8-bit colour images can be used to hide information. In 8-bit colour images, each pixel is represented as a single byte. Each pixel merely points to a colour index table, or palette, with 256 possible colours. The pixel's value , then, is between 0 and 255. The image software merely needs to paint the indicated colour on the screen at the selected pixel position.

Image compression:

Image compression offers a solution to large image files. Two kinds of image compression are lossless and lossy compression. Both methods save storage space but have differing effects on any uncompressed hidden data in the image.

Lossy compression, as typified by jpeg format files, offers high compression, but may not maintain the original image's integrity. This can impact negatively on any hidden data in the image. This is due to the lossy compression algorithm, which may lose unnecessary image data, providing a close approximation to high quality digital images, but not an exact duplicate. Hence, the term lossy compression. Lossy compression is frequently used on true-colour images, as it offers high compression rates. Lossless compression maintains the original image data exactly: hence it is preferred when the original information must remain intact. It is thus more favoured by steganographic techniques. Unfortunately, lossless compression does not offer such high compression rates as lossy compression. Typical examples of lossless compression formats are GIF, BMP and PCX.

This algorithm hides the encrypted file into a carrier medium.(The image file which carries the encrypted data),using the **least significant bit insertion** technique. The stego medium may be any image file compressed with lossless compression. The message is hidden into the LSBs of the image file. This algorithm handles the carrier file in a much careful way, since a very small change in the stego file, which is noticeable, will reveal the fact that it contains some data.

Least significant bit insertion:

The least significant bit insertion method is probably the most well known image steganography technique. It is a common, simple approach to embed information in a graphical image file. Unfortunately, it is extremely vulnerable to attacks, such as image manipulation. 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. When applying LSB techniques to each bytes of a 8-bit image, one bit can be encoded to each pixel. Any changes in the pixel bits will be indiscernible to the human eye. The main advantage of LSB insertion is that data can be hidden in the least and second to least bits and still the human eye would be unable to notice it. Care needs to be taken in the selection of the cover image, so that changes to the data will not be visible in the stego-image.

***4.3.M*ulti-level securities proposed in the algorithm:**

i.. To hide a text into the image:

1. *Apply encryption algorithm. This algorithm encrypts the text with a strong block cipher mechanism by applying the cipher block-chaining mode. It also provides the password protection.*
2. *The cipher text file is embedded into the stego medium*

ii.To extract a text from the image:

1. *By extracting the LSBs from the stego image, a file containing cipher text is obtained.*
2. This file is decrypted using the encryption algorithm to get the original file.

5.HOW SECURITY IS ENFORCED IN THE PROPOSED ALGORITHM?

The stego image file along with the message embedded into it is available to the hacker. The stego file does not reveal any difference in attributes like size, content etc., from that of the original file. Hence it is difficult for a hacker to find out that this image contains a message.

Even if he doubts so, he has to apply the same algorithm to retrieve the embedded file. Unfortunately if he finds out the algorithm by which the text has been embedded into the medium, he could get back only the cipher text file. In the retrieved file, he could see nothing but the junk characterts. This provides an **extra layer** of protection. To get the original message, this junk file has to be decrypted with the encryption algorithm with the **correct password**. This also adds an **extra layer** of protection. If the algorithm is found out, he must supply the correct password to get the correct message. Even if one character is altered in the password the original message can't be obtained.

Hence a hacker must know the following in order to extract the embedded message from the image file.

1. Algorithm to extract the message from the image. (stego algorithm)
2. Ecryption algorithm.
3. Correct password for algorithm.

With these increased levels of protection using encryption algorithm, the proposed system for steganography is more strong from attacks than any other existing system.

6.CONCLUSION AND COMMENTS

Until recently, information hiding techniques received very much less attention from the research community and from industry than cryptography. Steganography has its place in security. It is not intended to replace cryptography but supplement it. Hiding a message with steganography methods reduces the chance of a message being detected. However, if that message is also encrypted, if discovered, it must also be cracked (yet another layer of protection). There are an infinite number of steganography applications. This paper explores a tiny fraction of the art of steganography. It goes well beyond simply embedding text in an image. Steganography does not only pertain to digital images but also to other media (files such as voice, other text and binaries; other media such as communication channels, the list can go on and on).

References:

1. Herbert S. Zim, *Codes and Secret Writing*, William Marrow and Company. New York, NY, 1948.
2. J. Brassil, S. Low, N. Maxemchuk, L. O'Goram, "Hiding Information in Document Images," *CISS95*
3. Tuomas Aura, "Invisible Communication," *IEEE* 1995,
4. J. Brassil, S. Low, N. Maxemchuk, L. O'Goram, "Electronic Marking and Identification Techniques to Discourage Document Copying," *Infocom94*,
5. Neil F. Johnson, Zoran Duric, Sushil Jajodia, *Information Hiding: Steganography and Watermarking - Attacks and Countermeasures* Kluwer Academic Press, Norwrll, MA, New York, The Hague, London, 2000.
6. J. Brassil, S. Low, N. Maxemchuk, L. O'Goram, "Document Marking and Identification using Both Line and Word Shifting," *Infocom95*,
7. C. Kurak, J. McHugh, "A Cautionary Note On Image Downgrading," *IEEE Eighth Annual Computer Security Applications Conference*, 1992. pp. 153-159.
8. Diffie,W. "The first ten year of cryptography".

9. Stinsown,D. "Cryptography:Theory and practice"
10. Uyless black "Internet security protocols"
11. Ankit Fadia "Network Security"

WEB Sites Resources:

12. http://www.research.att.com/.
13. http://nsi.org/Library/Library.html.
14. http://www.trcone.com/t_links.html
15. www.cryptography.com