Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 3, March 2015, pg.663 – 674

RESEARCH ARTICLE

Proposed System Mix Cryptography and Steganography to Hide Information

Baydaa Jaffer AL-Khafaji
Computer Science; College of Education; Ibn-AL-Haitham
University of Baghdad

Abstract

Every few years computer security has to re-invent itself. New technologies and applications bring new threats, and force us to invent new protection mechanisms.
Text hiding in image is the proposed system ,this proposed system consists of four stages, pre-processing stage, embedding stage, extracting stage, post-processing stage. Each stage it is as follow, the pre-processing stage consists two phases, the first is converting phase which convert the text and cover into binary form, the second is coding phase which code the embedded data. The embedding stage takes the embedded data which in this proposed steganography system (text file) and the cover-object which is either a bit-map (bmp)image or graphics interchange format(gif) image then divide the binary-cover into N-blocks each block has size [8*8] bits and hide each bit resulted from coding phase in the (1,2,3 and 4) least significant bit positions for each byte of each block in the binary cover (image) to produce the (stego-cover) that represent resulted image. In the extracting stage, takes the (stego-cover) then divide it into N-blocks [8*8] bits and determine the position of (1,2,3 and 4) least significant bits from each byte of block and extract the embedded bit (cipher bit) . At last, post-processing stage consists two phases, the first is decoding phase which decode each bit resulted from extracting stage and store it in new file called (destego),the second is inverse converting phase which convert the binary data that stored in (destego) file to get to the original data as text form

Keywords: Cryptography, Steganography, Stego- image, stego-cover, destego least significant bits, PSNR

Introduction

Cryptography is the study of hiding information and it is used when communicating over an entrusted medium such as internet, where information needs to be protected from other third parties. Modern cryptography focuses on developing cryptographic algorithms that are hard to break by an adversary due to the computational hardness consequently could not be broken by a practical means. In the modern cryptography, there are three types of cryptographic algorithms used called Symmetric key cryptography, Public-key cryptography and hash functions. Symmetric key cryptography includes encryption methods where both the sender and the receiver share the same key used to encrypt the data. In Public-key cryptography, two different but mathematically related keys are used. Hash functions does not use a key, instead they calculate a fixed length hash value from the data. It is unfeasible to recover the length or the original plain text from this hash value.
Steganography deals with composing hidden messages so that only the sender and the receiver know that the message even exists. While nobody excluding the sender and the receiver knows the existence of the message, it does not attract superfluous attention. Steganography was used even in ancient times and these ancient methods are called Physical Steganography. Some examples for these methods are messages hidden in messages body, messages written in secret inks, messages written on envelopes in areas covered by stamps, etc. Modern Steganography methods are called Digital Steganography. These modern methods include hiding messages within noisy images, embedding a message within random data, embedding pictures with the message within video files, etc. Furthermore, Network Steganography is used in telecommunication networks. This includes techniques like Steganophony (hiding a message in Voice-over-IP conversations) and WLAN Steganography (methods for transmitting Steganograms in Wireless Local Area Networks).

What is the difference between Cryptography and Steganography?

Cryptography is the study of hiding information, while Steganography deals with composing hidden messages so that only the sender and the receiver know that the message even exists. In Steganography, only the sender and the receiver know the continuation of the message, while in cryptography the existence of the encrypted message is visible to the world. Owing to this, Steganography removes the superfluous attention coming to the hidden message. Cryptographic methods try to defend the content of a message, while Steganography uses methods that would hide both the message as well as the content. By combining Steganography and Cryptography one can achieve better refuge. [1].

Every few years computer security has to re-invent itself. New technologies and applications bring new threats, and force us to invent new protection mechanisms. Cryptography became important when business started to build networked computer systems; virus epidemics started once large numbers of pc users were swapping programs, and when the internet took off , the firewall industry was one of the first to benefit[1]. One of the hot spots in security research is information hiding. It is driven by two of the biggest policy issues of information age copyright protection (watermarking) and state

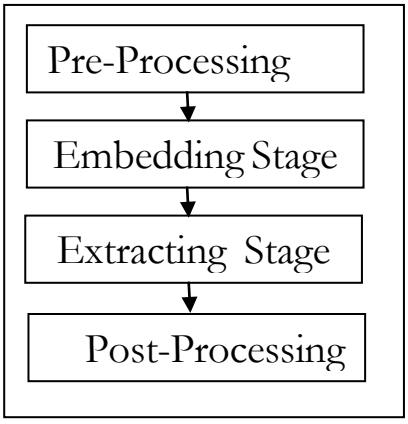
surveillance (steganography). Steganography's intent is to hide the existence of a hidden message, the goal of steganography is to hide message inside other harmless message in a way that does not allow any enemy to even detect that there is a second secret message present. While watermarking and fingerprinting are used to protect authors, artist, software and things have copyrights. Placing a hidden trademark in products is watermarking, and hiding a serial number or a set of characteristics that distinguishes an object from a similar object is fingerprinting. They are both used to fight piracy, to detect and prosecute any violators [2].

Steganography is very old method of passing a message in secret. This method of message sending goes back to the ancient Greeks. The historian Herodotus wrote about how an agent wrote a message of an invasion on the wood part of a wax tablet. Since message was normally inscribed in the wax and not the wood, the tablet appeared blank to a common observer[3]. Another famous example of a classical system is that of the roman general who shaved the head of a slave and tattooed a hidden message on it . After the hair had grown back, the slave was sent to deliver the message. While such a system might work once, the moment that it is known, it is simple to shave the heads of all people passing by to check for hidden message[4]. Another common form of invisible writing is through the use of invisible inks. Such inks were used with much success in both World War I and World War II [5].

A proposed technique

The proposed steganography system consists of four stages as illustrated in the following block diagram, these stages are :

1. **Re-Processing Stage.**
2. **Embedding Stage.**
3. **Extracting Stage.**
4. **Post-Processing Stage.**



Pre-Processing Stage

This stage represent the first stage in the proposed system and it consists of two phases are :

1- Converting phase.

In this phase, Select cover image, this selection is performed by choosing a image from a group of images. This image represents a cover, then select the text file to be hidden (which can be selected from a list of stored file or a new one).

After that converting operation into the binary form is performed on the selected cover (image file) and data file to ready them to the next phase

2- Coding phase.

In this phase, the coding operation is performed on each bit of embedded data, the coding operation deals with readed bit from embedded data as decimal value. The readed bit from embedded data called (plain-bit), this means the bit before coding opration. The bit after coding operation called (cod). The coding and decoding operations uses the same key that called (cod-k), this means, symmetric key. The symmetric key equals one in decimal system in both operations. The coding operation is shown in the figure (3.2).The coding operation uses the following equations:

IF (plain bit=0) Then [cod=(plain bit)+(cod-k)] …….equation(1)
IF(plain bit=1) Then [cod =((plain bit)+(cod-k)) mod 1].. equation(2)

Embedding Stage

This stage represents the second stage in the proposed system, in this stage will embedd an encrypted binary data which resulted from the coding phase in the binary cover (image file) by using the steps in the embedding algorithm,
The embedding algorithm of the proposed system can be described as following:

Input : Cover File and Embedded Data File.
Output : Stego-Cover.

1. **Read cover (bmp file or gif file) and splitting it into header and body.**
2. **Read embedded data, then converting it into binary.**
3. **Divide the cover into N-blocks, each block consists of [8*8] bits.**
4. **Read one block of bit, then converting it into binary.**
5. **Read one byte from the binary block and determine least significant bit position of (1,2,3 and 4) least significant bits for each bit of block.**
6. **Read one bit from the binary embedded data file, then go to the coding phase to obtain encrypted bit (cipher bit).**
7. **Embedding the cipher bit in the least significant bit position of (1,2,3 and 4) least significant bits and store it in new file.**
8. **Go to step 5 until the end of the binary block of [8*8] bits.**
9. **Go to step 4 until the end of the cover.**
10. **End.**

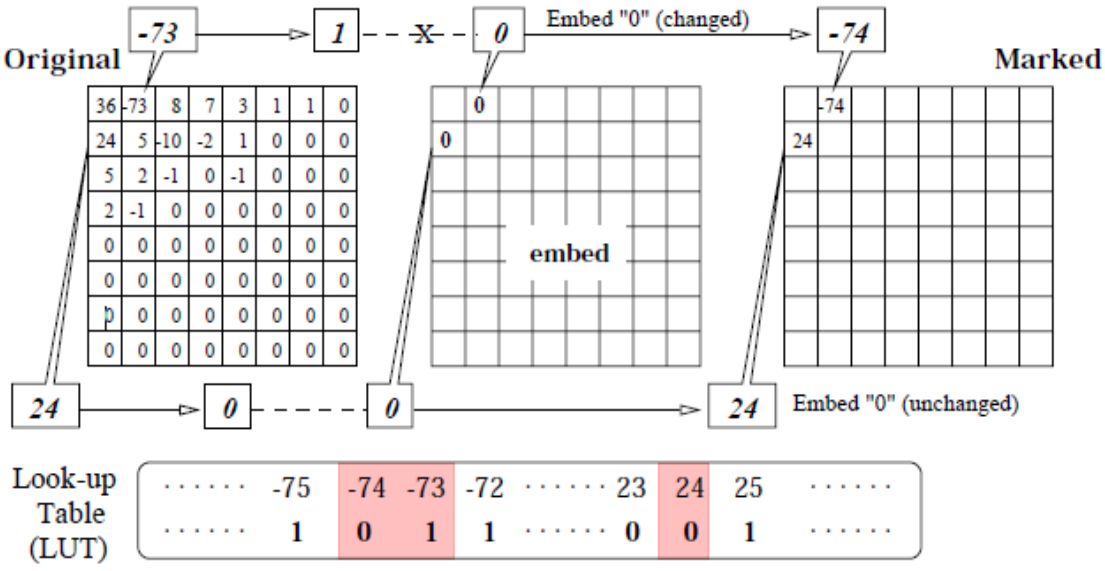
Least Significant Bit

The least significant bit insertion method is probably the most well known image Steganography technique. It is a common, simple approach to embedding information in a graphical image file.

The embedding process consists of choosing a subset $\{j_1, \ldots..,j_{l(m)}\}$ of cover elements and performing the substitution operation $c_{ji} \leftrightarrow m_I$ on them, which exchanges the LSB of c_{j1} by m_i (m_i can either be 1 or 0). One could also imagine a substitution operation which changes more than one bits of one-cover element. In the extraction process, the LSB of the selected cover-elements are extracted and lined up to reconstruct the secret message.

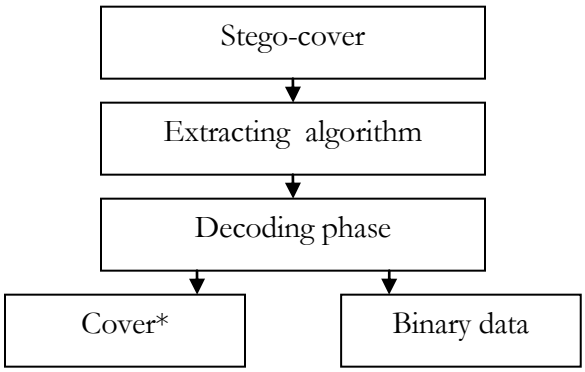
Comparing Between (1,2,3 and 4) LSBs

Method	Embedding capacity	PSNR
1LSB	0.39 %	60.71
2 LSB	2.44 %	49.2
3 LSB	3.61 %	38.9
4 LSB	5.88%	31.71



Extracting Stage

This stage represents the third stage in the proposed system , in this stage will be extracting the data that embedded in the cover (stego-cover) that resulted from the embedding stage by using the steps in the extracting algorithm,



Post-Processing Stage

This stage represent the last stage in the proposed system and it consists of two phases are :

1- Decoding phase.

2- Inverse Converting phase.

Decoding Phase

In this phase, the decoding operation is performed on each bit of extracted data, the decoding operation deals with extracted bit from the stego-cover as decimal value. The extracted bit from the stego-cover called (cipher-bit), this means the bit before decoding opration. The bit after decoding operation called (deco). The coding and decoding operations uses the same key that called (cod-k), this means, symmetric key. The symmetric key equals one in decimal system in both operations. The decoding operation uses the following equations:

IF(cipher bit=0) Then [deco=(cipher bit)+(cod-k)] …….equation(1)

IF(cipher bit=1)Then[deco=((cipher bit)+(cod-k)) mod 1]. equation(2)

Inverse Converting Phase

In this phase will convert the binary data which obtained from the decoding phase to get the original data as text form (text file), after this phase is completely the proposed system will be ended

Conclusions

1. **The LSB algorithm is simple and easy.**
2. **Embedding capacity is little if one-bit will embed in a cover, but the embedding is more if two-bit will embed in a cover and so on.**
3. **If the number of embedded bit is large than the PSNR is small, and the inverse is true.**
4. **The embedding capacity is large when we use *.bmp as a cover while the embedding capacity is less than *.bmp when we use *.gif as a cover.**
5. **If the number of embedded bit is large then the difference between cover and stego-object is large too, and the inverse is true.**

Results

In the following, the results of applying least significant bit (LSB) algorithm on (1,2,3 and 4) bit that represent least significant bit of cover.

Cover-Image(1)

Stego-Cover (1 LSB)

Cover-Image(2)

Stego-Cover (2 LSB)

Cover-Image (3)

Stego-Cover (3 LSB)

Stego-Cover (4 LSB)

References

[1] Kharrazi, M., Sencar, H. T., and Memon, N. (2004). Image Steganography: Concepts and practice. In WSPC Lecture Notes Series

[2] Domenico Daniele Bloisi , Luca Iocchi: Image based Steganography and cryptography, Computer Vision theory and Applications

[3] D.R. Stinson, Cryptography: Theory and Practice, Boca Raton, CRC Press, 1995.

[4] Provos, N. and Honeyman, P. (2003). Hide and seek: An introduction to steganography. IEEE SECURITY &PRIVACY

[5] Chandramouli, R., Kharrazi, M. & Memon, N., "Image Steganography and teganalysis: Concepts and Practice", Proceedings of the 2nd International Workshop on Digital Watermarking, October 2003

[6] Owens, M., "A discussion of covert channels and steganography", SANS Institute, 2002

[7] Jamil, T., "Steganography: The art of hiding information is plain sight", IEEE Potentials, 18:01, 1999

[8]Stefan Katznbeisser, Fabien.A., P.Petitcolas editors, Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, Boston. London, 2000.

[9] Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM, 47:10, October 2004

[10] Marvel, L.M., Boncelet Jr., C.G. & Retter, C., "Spread Spectrum Steganography", IEEE Transactions on image processing, 8:08, 1999

[11] Dunbar, B., "Steganography techniques and their use in an Open-Systems environment", SANS Institute, January 2002

[12]Bender, W., Gruhl, D., Morimoto, N. & Lu, A., "Techniques for data hiding", IBM Systems Journal, Vol 35, 1996

