Implementation of LSB Steganography with 12-bit Frame Format

Aishvary Goel
Student (B. Tech.)
IMS Engineering College
Ghaziabad

Anubhav Srivastava
Student (B. Tech.)
IMS Engineering College
Ghaziabad

Alok Kr. Mishra
Student (B. Tech.)
IMS Engineering College
Ghaziabad

Ayush Agarwal
Student (B. Tech.)
IMS Engineering College
Ghaziabad

Amit Kr. Gautam
Assistant Professor
Department of CSE
IMS Engineering College
Ghaziabad

ABSTRACT
The proposed system is an approach used to embed text into image. It enables the user to provide the system with both text and cover, and obtain a resulting image that contains the hidden text inside. The system uses the least significant Bit (LSB) method to embed the secret text in image after encrypt the secret text using a proposed method and store the text in image. The proposed system aims to provide improved robustness, security due to multi-level security architecture along with faster embedding and extraction process irrespective of size of embedded text.

Keywords
Steganography, LSB technique, cryptography, encrypt, decrypt.

1. INTRODUCTION
Hiding secret messages had been the concern of people, since ancient times.. Both cryptography and steganography achieve this aim. But they use different techniques.

We have stories from the ancient world about some of the ancient civilizations. The stories demonstrate how the Greeks had received warnings about Xerxes hostile intentions from a message which was hidden underneath the wax of a writing tablet; or about a Roman general who used shaved heads of his slaves to transfer messages; or about Chinese who used to hide messages on a piece of silk which was then crushed into small pieces and then those pieces were covered by wax which the messengers used to swallow. After the hair grew back, the slave was sent to deliver the now-hidden message [1].

Steganography is the art and science of communicating in a way which hides the existence of the communication. The word Steganography is basically composed of two Greek words. These two words are 'steganos' meaning 'covered' and graphein meaning 'to write'. Protection of the transmitted data from being intercepted or tampered has led to the development of various steganographic techniques.

On the other hand, Cryptography involves converting a message text into an unreadable cipher. A large number of cryptography algorithms have been created till date with the primary objective of converting information into unreadable ciphers Cryptography systems can be broadly classified into symmetric-key systems and public key systems. The symmetric key systems uses a common key for encryption and decryption of the message. This key is shared privately by the sender and the receiver. The sender encrypts the data using the joint key and then sends it to the receiver who decrypts the data using the same key to retrieve the original message. The public-key systems that use a different key for encryption as the one used for decryption. Public key systems require each user to have two keys – a public key and a private key (secret key). The public key is used by Receiver's to encrypt the message by the sender.

A number of ways exist to hide information in digital media.

Some of the common ways of hiding data are:-

1. LSB Insertion

2. Use of Masks and Filters

3. Encrypt and Scatter

4. Use of various Algorithms and Transformations techniques

Each of these techniques can be applied, with varying degrees of success but the one which is implemented in our system is Least significant bit insertion.

1.1 LSB Insertion Method
Least significant bit (LSB) insertion is a common, simple approach for embedding information in a cover image. A bit of the secret message is used to replace the least significant bit (LSB) of some of all bytes inside an image. Let us consider a cover image contains the following bit patterns:

Byte-1=10110110 Byte-2=01011100 Byte-3=00101101

Byte-4=01010010 Byte-5=00011011 Byte-6=10100110

Byte-7=10101101 Byte-8=11000100

Suppose we want to embed a number 201 in the above bit pattern. Now the binary representation of 201 is 11001001. To embed this information we need at least 8 bytes in cover file. We have taken 8 bytes in the cover file. Now we modify the LSB of each byte of the cover file by each of the bit of embed text 11001001.

Before Replacement	Bit Inserted	After Replacement	Remarks
10110110	1	10110111	Change in bit
01011100	1	01011101	Change in bit
00101101	0	00101100	Change in bit
01010010	0	01010010	No change in bit
00011011	1	00011011	No change in bit
10100110	0	10100110	No change in bit
10101101	0	10101100	Change in bit
11000100	1	11000101	Change in bit

Table-1- LSB Operation

Here we can see that out of 8 bytes only 5 bytes get changed only at the LSB position. Since we are changing the LSB hence we are either changing the corresponding character in forward direction or in backward direction by only one unit and depending on the situation there may not be any change also as we have seen in the above example. As our eye is not very sensitive so therefore after embedding a secret message in a cover file our eye may not be able to find the difference between the original message and the message after inserting some secret text or message on to it.

2. LITERATURE SURVEY

Steganography is defined as "hiding information within a noise; a way to supplement encryption, to prevent the existence of encrypted data from being detected"[2]. It has been used in various forms for thousands of years. In the 5th century BC Histaiacus shaved a slave's head, tattooed a message on his skull and the slave was dispatched with the message after his hair grew back.

In Saudi Arabia at the King Abdulaziz City of science and technology, a project was initiated to translate into English some ancient Arabic manuscripts on secret writing which are believed to have been written 1200 years ago. Some of these manuscripts were found in Turkey and Germany[3].

Five hundred years ago, the Italian mathematician Jérôme Cardan reinvented a Chinese ancient method of secret writing. The scenario goes as follows: a paper mask with holes is shared among two parties, this mask is placed over a blank paper and the sender writes his secret message through the holes then takes the mask off and fills the blanks so that the message appears as an innocuous text . This method is credited to Cardan and is called Cardan Grille.

2.1 The Scope Of Steganography

With the boost in computer power, the internet and with the development of digital signal processing (DSP), information theory and coding theory, steganography has gone ''digital''. Due to growing number of interesting applications which steganography has created in the digital world, its continuous evolution is guaranteed. But, here arises a problem. Cyber-crime is supposed to be benefited by this revolution. Hence an immediate concern is to find out best possible attacks to carry out steganalysis, and simultaneously, finding out techniques to strengthen existing steganography techniques against popular attacks like steganalysis.

2.2 Cryptography

Cryptography encodes information in such a way that nobody can read it, except the person who holds the key. More advanced crypto techniques ensure that the information being transmitted has not been modified in transit. There is some difference in cryptography and steganography, in cryptography the hidden message is always visible, because information is in plain text form but in steganography hidden message is invisible.

2.3 Steganography Versus Cryptography

The comparison and contrast between steganography and cryptography is illustrated from the following table :-

S.NO	Context	Steganography	Cryptography
1	Host files	Image, Audio, Text, etc .	Mostly text files
2	Hidden files	Image, Audio, Text, etc	Mostly Text Files
3	Result	Stego File	Cipher Text
4	Type of Attack	Steganalysis: Analysis of a file with a objective of finding whether it is stego file or	Cryptanalysis

Table-2- Steganography vs. Cryptography

2.4 Steganalysis

Steganalysis is a relatively new research discipline with few articles appearing before the late-1990s. Steganalysis is "the process of detecting steganography by looking at variances

between bit patterns and unusually large file sizes"[4]. It is the art of discovering and rendering useless covert messages. Some of the goals of steganalysis are: to identify suspected streams of information, to determine whether or not they have hidden messages encoded into them, and at last, if possible, to recover those hidden messages. The challenge of steganalysis is that:

1. The suspect information stream, such as a signal or a file, may or may not have hidden data encoded into them.

2. The hidden data, if any, may have been encrypted before being inserted into the signal or file.

3. Some of the suspect signal or file may have noise or irrelevant data encoded into them (which can make analysis very time consuming).

4. Unless it is possible to fully recover, decrypt and inspect the hidden data, often one has only a suspect information stream and cannot be sure that it is being used for transporting secret information

2.5 Types Of Attacks

Attacks and analysis on hidden information may take several Forms : detecting , extracting , and disabling , destroying or modifying hidden information. An attack approach is dependent on what information is available to the steganalyst (the person who is attempting to detect steganography -based information streams). The possible attacks on a stego media can be one of the following:

1. Steganography-only attack: Only the steganography medium is available for analysis.

2. Known-carrier attack: The carrier, that is, the original cover, and steganography media are both available for analysis.

3. Known-message attack: The hidden message is known.

4. Chosen-steganography attack: The steganography medium and tool (or algorithm) are both known.

5. Chosen-message attack: A known message and steganography tool (or algorithm) are used to create steganography media for future analysis and comparison. In this corresponding patterns in the steganography medium are determined which may be helpful in pointing to the use of specific steganography tools or algorithms.

3. PROPOSED WORK

3.1 Encryption Algorithm

The proposed encryption algorithm will work in two steps. In the first step we will increase the ASCII value of each alphabet in the message sequentially and in increasing order as well.

For e.g. If the message to be embed is hello then-

• Add 1 in ASCII value of ‘h’ such that it becomes ‘i’

• Add 2 in ASCII value of ‘e’ such that it becomes ‘g’

• Add 3 in ASCII value of ‘l’ such that it becomes ‘o’

• Add 4 in ASCII value of ‘l’ such that it becomes ‘p’

• Add 5 in ASCII value of ‘o’ such that it becomes ‘t’

Following this ‘hello’ is encrypted as ‘igopt’

Then while embedding the encrypted message we will send data in a frame format. If we want to send a byte of message say 11010010 i.e. 8 bits then we will take a frame of 12 bits of which first and last bits will be fixed to 1 and 2^{nd} bit will be the result obtained after XORing the 8 bits of message and 11^{th} bit will be the result obtained after ORing the 8 bits of message. Here after XORing and ORing the message bit by bit we get 0 and 1 respectively. So the frame to be send will be 101101001011.

3.2 Embedding the encrypted text in the carrier image

LSB is a approach which is used to embed information in a cover image. The pixel values of encrypted image is hidden in the LSB of pixels of carrier image. If the size of the encrypted image is mxn ,then the size of carrier image must be mxnx8 as each encrypted byte requires 8 bytes (pixels)of carrier image. so if the carrier image size is not eight times the size of the payload , then it has to be resized. In this procedure LSB algorithm helps for securing the originality of image.

3.3 Extracting the encrypted image in carrier image

The extracting is reverse to embedding the encrypted image. In extracting, the carrier image in which the data is hidden is given as an input file. Here the given image is first encrypted and then the encrypted image is hidden in the carrier image. Finally the hidden encrypted image is decrypted. The Least Significant bit technique by which the encoded bits in the image is decoded and turns to its original state and gives the output as a image. The encryption and decryption in order to secure from unauthorized access.

4. CONCLUSION

The proposed system provides LSB method with a encryption algorithm and hope for embedding text in image.

A number of conclusions were derived from this study:-

1. Steganography is not intended to replace cryptography but rather to supplement it. If a message is encrypted and hidden with a steganographic method it provides an additional layer of protection and reduces the chance of the hidden message being detected.

2. The amount of the information embedded in the other media depends on the statistical properties of the cover media, where this amount is small the noise in the media is not perceptible.

3. From the implementation we conclude that the proposed system is very rapid in performing extraction process and the size of the embedded text does not affected the speed of the system very much.

5. SUGGESTION FOR FUTURE WORK

Many suggestions can be given to enhance the work of the proposed system they are:-

1. The method of embedding is trivial which is LSB insertion, in the future another embedding method should be employed like wavelet or DCT transform based methods.

2. Improved system to deals with video image and audio.

3. The encryption algorithm can be replaced for increasing the security level.

6. REFERENCES

[1] N. Johnson and S. Jajodia. Exploring Steganography: Seeing the Unseen. Computer, vol. 31, no. 2, pp. 2634, 1998.

[2] C. Kurak and J. McHugh, A cautionary note on image downgrading, in: Proceedings of the IEEE 8 Annual Computer Security Applications Conference, 30 Nov-4 Dec, 1992, pp. 153-159.

[3] S.B. Sadkhan, Cryptography: Current status and future trends, in: Proceedings of IEEE International Conference on Information & Communication Technologies: From Theory to Applications, Damascus. Syria, April 19-23, 2004, pp. 417-418.

[4] W. Huaiqing and S. Wang. Cyber warfare:Steganography vs. steganalysis. Communi-cations of the ACM, 47(10):76–82, 2004.

[5] Cryptography and Network , William Stallings , Prentice Hall of India

[6] J.C. Judge, Steganography: Past, present, future. SANS Institute publication.

[7] Km. Pooja ,Arvind Kumar , "Steganography- A Data Hiding Technique" International Journal of Computer Applications ISSN 0975 – 8887, Volume 9– No.7, November 2010.

[8] Johnson, Neil F., Duric, Zoron Jajodio, "Information Hiding Steganography and Watermarking –Attack and Countermesures", Kluwer Acdemic Publishers, 2001.

[9] Benjamin B., Santiago G., and victor B., "Steganographic Watermarking for Documents", proceeding on the 34th Hawaii International conference on system science, 2001.

[10] Gruhl , D., Bender W., "Information Hiding to Foil the Casual Counterfaiter ",information hiding :second international workshop, proceeding Vol 1525, springger 1998.

[11] P. Moulin and R. Koetter, Data-hiding codes, Proceedings of the IEEE, 93 (12)(2005)2083-2126.

[12] R. Chandramouli, M. Kharrazi, N. Memon, "Image Steganography and Steganalysis: Concepts and Practice " , International Workshop on Digital Watermarking, Seoul, October 2004.

[13] R.J. Anderson and F. A. P. Petitcolas (2001) On the limits of the Stegnography, IEEE Journal Selected Areas in Communications, 16(4), pp. 474-481.

[14] M. G. J. Fridrich. Practical steganalysis of digital images - state of the art. Security and Watermarking of Multimedia Contents IV, 4675:1–13, 2002.

[15] N. Johnson and S. Jajodia. Steganalysis of images created using current steganography software. Workshop on Information Hiding, 1998.

[16] Mohammed S.,"Text file hiding Techniques with Implemntation",M.Sc. thesis , National Computer Center,2001.

[17] Al-hamami, M., "Information Hiding attack in Image" , M.Sc.thesis, Iraqi commission for computer &Informatics , Informatics Institute for Postgraduate Studies 2002.

[18] Zollenr J., Fderrath H., Klimant H., Pfitzman A., Piotraschke R., "Modelling the Security of Steganography System", Information Hiding :Second International Workshop Proceeding VOL1525, PP244-354. 1998.

[19] A. D. Ker. A fusion of maximum likelihoodand structural steganalysis. In Proceedings of the 9th international conference on In-formation hiding, IH'07, pages 204–219, Berlin, Heidelberg, 2007. Springer-Verlag.

[20] A. Kerckhoffs. La Cryptographie Militaire (Military Cryptography). In J. Sciences Militaires (J. Military Science, in French), 1883.

[21] R. Krenn. Steganography and steganalysis.Whitepaper, 2004.