An Enhanced Method for Information Hiding Using LSB Steganography

Mr. Milan Sasmal¹, Mrs. Debasmita Mula²

Assistant Professor, JIS College of Engineering, Kalyani, Nadia, milan.sasmol@jiscollege.ac.in¹
debasmita164@gmail.com²

Abstract. This work involves a method to communicate one to one by hiding the information among all the people. Digital photographs are the most suitable components compared to other things available on the internet as transmitter based on their availability. This work basically ciphered message within a photographs. For hiding secret information in images, there exist an outsized sort of steganographic techniques some are more complex than others and every one of them have respective strong and weak points. Different applications may have separate requirements of the cipher technique used. for instance , some applications may require absolute invisibility of the key information, while others require a bigger secret message to be hidden. This work intends to offer an summary of image steganography, its uses and techniques. LSB (Least Significant Bit) technique is used for this work. Here bits of the text are replaced by the LSBs of the pixel values of the image. because the LSBs are alone changed, normal human eyes cannot predict the difference between the first image and therefore the resulting image.

In this work, the pixel indicator technique has been used to hide information in RGB Images. Least two significant bits are used for this proposed methodology as of one for the channels of Red, Green or Blue as an indicator of data existence in the other two channels. Based on the image nature indicator bits will be generated randomly in the channel.

Keywords – Steganography, Stego_crypt Algorithm, LSB

1. Introduction

Steganography is defined as the art and science of writing hidden messages in such how that nobody else, aside from the intended recipient knows the existence of the message. The word “steganography” is basically of Greek origin which means “hidden writing”. The word is classified into two parts: steganos which means “secret” and “graphic” which means “writing”. However, in hiding information, the meaning of steganography is hiding text or secret messages into another media file such as image, text, sound or video. The word “steganography” is usually considered almost like “cryptography” and “watermarking”. Whilst watermarking confirms the information integrity and cryptography scrambles the message, steganography hides it. The main motto of this method is to avoid drawing attention to the transmission of concealed message. If suspicion is raised, then this objective that has been planned to realize the safety of the key message because if the hackers noted any change within the sent message then this observer will attempt to know the hidden information inside the message.

The basic terminologies used in this proposed steganography systems are: the cover message or information, secret message, the secret key and embedding algorithm. The cover information is the carrier of the message; it may be any kind of photographs, audio-visual clips, text or some other types digital media. The secret message is the main information, which requires to be concealed in the suitable digital content.

In case of steganography, before the hiding process, the sender must choose a proper message carrier for hiding the effective information. A robust steganographic algorithm must be selected that should
be able to encrypt the actual information more efficiently. The sender then may send the hidden message to the receiver by using any of the modern communication techniques. The receiver after receiving the message, needs to decrypt the concealed information using the proper extraction algorithm. This project proposes a algorithm to hide data inside an image using steganographic technique. The algorithm that we have proposed is an enhanced version of LSB technique which is not very much robust.

This project comprehends the following objectives:
(i) To generate a security tool on the basis of steganographic techniques.
(ii) To survey a novel technique for hiding information using steganography.

2. Literature Review

Many more work has been done in the field of LSB steganography [1]. For the improvement purposes of LSB steganographic method, the bits of the information will be randomly embedded to produce more secure image. The objective is giving more complex cryptosystem maintaining the execution time as closer as the original methods. Using the technology, the text encrypted inside the image does not allow any intruder to detect that there is secret message.

The general overview of the paper : cases& examples of steganography concept, working method of steganography, commercial availability of steganography software and supported data types, availability of aide computer forensic investigators and information security system for detection, after notified detection, the embedded message can be extracted & the embedded data can be fetched from the original file[ carrier]. Finally, what are some methods to defeat the use of steganography even if it cannot be reliably detected.[2]

The main concern of the paper is using the Least Significant Bit (LSB) technique to conceal encrypted messages using image. The system enhanced the technique by random generated bits of the encrypt message in the image and prevent unauthorized access of intruder to extract the original message [3]. The proposal of the paper is combine the method of cryptography & steganography (taken as security layers) , along with an extra security layer which has been imposed in between those concept. The newly introduced secured extra layer will change the format of normal encrypted messages by embedding the encrypted message inside the multimedia cover [4]. We take a look for existent methods for conceal information into a document like images, audio files, image files, binary files [5].

3. Methodological Aspects and Algorithm

3.1. Methodological aspects

Steganography refers to the technique of conversion of communications. By Implementing the method, possibly A can send a secret text to B that no-one else can understand the existence of encrypted information using the cover Work [text is embedded inside the object], by tweaking its characteristics. This is called stegogramme such that it is the symmetrical perceptual model of the cover Work, but it will contain the hidden information. By using stegogramme, conversation of messages can be possible between A and B. If intruder attack intercepts in between communication, it is difficult to understand by them the stegogramme technique. So objective of the steganography is to ensure the adversary regards the stegogramme - and thus, the communication - as innocuous.

Around 440 BC in Greek History, the oldest examples of steganography dates back to the 5th Century BC, by Herodotus, a Greek historian revealed the concept in his work entitled "The Histories of Herodotus". One interesting example is that Histaeus, ruler of Miletus, tattooed secret information on bareheaded slave who is one of his most trusted. After the hair had fill out with time, the slave was
sent to Aristagorus where he was shaved and the information that tattooed, a revolt against the Persians. Here the slave is the carrier for the embedded information, and others who knew about the slave, they were sent to Aristagorus, not knowing about the fact that they also the carrier of the secret information. As a result, the information reached the destination with no suspicion of covert communication ever.

Nowadays, steganography is usually implemented by computational method, where cover works such as text files, images, audio files, and video files are tweaked in such a way that a secret message can be embedded within them. Though the digital watermarking technique is looking similar, the main difference is in digital watermarking, the concept is on ensuring that none can delete or tamper the content of the watermarked data, even though it might be exists. Other side, Steganography aim on making it extremely crucial to know that secret information exists. If an unauthorized access is happened and the intruder able to decode the secret file then steganography has failed.

The main difference of Steganography and cryptography is that the latter does not attempt to hide the fact that a message exists. In spite of that, cryptography dubious the integrity of the message so that not making sense to anybody but the sender and the recipient. The intruder can see a message exists, and the inverse process of cryptanalysis involves trying to turn the meaningless information into its original form.

3.2. Stego_crypt Algorithm

The following comprehensive algorithm can represent the pixel indicator technique that is to be prescribed.

This proposed method uses at least two significant bits [LSB] of one of the channels Red, Green or Blue used as the indicator of data existence in the other two channels. The channel for the indicator is not fixed as these are chosen sequentially. If in the first pixel Red is the indicator, while Green is identified as channel 1 and Blue is identified as channel 2 and at the second pixel, if Green is the indicator, while Red is identified as channel 1 and Blue is identified as channel 2 and at the third pixel if Blue is the indicator, while Red is identified as channel 1 and Green is identified as channel 2.

To improve security we have used a randomly generated pixel from which the embedding will be started. The length of the text and the random number will be sent through the cover image.

| Indicator | Channel 1 | Channel 2 |
|-----------|-----------|-----------|
| 00        | No hidden data | No hidden data |
| 01        | Hide 2 message bits | No hidden data |
| 10        | No hidden data | Hide 2 message bits |
| 11        | Hide 2 message bits | Hide 2 message bits |

3.3 Embedding Algorithm:
1. Read the RGB cover image.
2. Enter the string.
3. Store the number of message bits in the variable remaining.
4. Generate a random number and find the corresponding row index r and column index c.
5. Reserve last two pixels for sending the random number and length of the string.
6. Embed the message bit from the pixel with row index r and column index c.
7. Check the two LSB bits of the indicator
8. If two LSBs of indicator is ‘00’
9. No change in channel 1 & channel 2.
Else
10. If 2 LSBs of indicator is ‘01’
11. Embed two message bits in the LSB of channel 1.
12. Set remaining=remaining-2
Else
13. If 2 LSBs of indicator is ‘10’
14. Embed 2 message bits in the LSB of channel 2.
15. Set remaining=remaining-2
Else
16. If 2 LSBs of indicator is ‘11’
17. Embed 2 message bits in the LSB of channel 1.
18. Set remaining=remaining-2
19. If remaining==0 then exit.
20. Embed 2 message bits in the LSB of channel 2.
21. Set remaining=remaining-2
22. If remaining==0 then exit.
End if
23. Change the row index r and column index c.
24. Go to step 7 while remaining>0
25. End.

3.4 Retrieval Algorithm:
1. Read the cover image.
2. Extract the random number and length of the string from the image.
3. Store the number of message bits in the variable remaining.
4. Find the row index r and column index c from the random number.
5. Retrieval will be started from the pixel with row index r and column index c.
6. Check the 2 LSBs of the indicator channel
7. If 2 LSBs of the indicator are ‘00’
8. No change.
Else
9. If 2 LSBs of the indicator are ‘01’
10. Extract 2 message bits LSBs from channel 1.
11. Set remaining=remaining-2
Else
12. If 2 LSBs of the indicator are ‘10’
13. Extract 2 message bits LSBs from channel 2.
14. Set remaining=remaining-2
Else
15. If 2 LSBs of the indicator are ‘11’
16. Extract 2 message bits LSBs from channel 1.
17. Set remaining=remaining-2
18. If remaining==0 then exit.
19. Extract 2 message bits LSBs from channel 2.
20. Set remaining=remaining-2
21. If remaining==0 then exit.
End if
22. Modify the row index r and column index c
23. Go to step 6 while remaining >0
24. End

4. Result and Discussion

This is the in face of the work for information using an enhanced method of LSB steganography. First we have to choose the image by clicking the ‘Load Image’ button as shown in Fig.1.

Fig. 1.Load image
After that we have entered the text which we want to hide in the cover image, as written within the Fig.2.

Fig.2.Read the text
Now a random number will be generated between 1 and (no of row x no. of column) -2) by clicking the ‘Generate a random number’ button as shown in Fig.3. From the randomly generated number the
row index and column index will be computed from where the hiding of the message bits will be started.

Fig.3. Generate a random number

After we have embedded the text in the cover image by clicking ‘Hide the text’ button and at the same time the stego image will be displayed as per Fig.4.

Fig.4. Hide the text

Finally the text will be retrieved from the stego image by clicking the ‘Get the text’ button, shown in Fig. 5. It is clearly visible that original information, which was encrypted and the decrypted information is exactly same. And the shared information can only be retrieved by using the proper
decryption algorithm. So this proposed method can be used for the secure sharing of any kind of information, like as defence, banking system etc.

![Diagram of decryption algorithm]

5. Conclusion
The conclusive remarks may be tangibly presented as follows:
The advantages of the LSB steganography are clear. It is very simple to implement, and generally quite difficult to detect. Here, we have presented an enhancement of the image steganography system using LSB approach to provide a means of secure communication. A random number has been generated during embedding of the message into the cover-image. In our proposed approach, the message bits are embedded by pixel indicator technique into the cover image pixels. In algorithm the indicator channel is not fixed. The indicators are chosen based on a sequence. For the first pixel Red works as indicator, while Green is for channel 1 and Blue is for the channel 2. In the second pixel, Green works as indicator, while Red is for channel 1 and Blue is for channel 2. In third pixel Blue works as a indicator, while Red is for channel 1 and Green is for channel 2. To improve security we have used a randomly generated pixel from which the embedding will be started.
The strength of Steganography lies in the sheer amount of information that changes hands every day. It is very simple using digital technology to conceal any given digital information within other information, so virtually anything could contain a hidden meaning. There is no practical way to check it all. However, none of steganography methods we examined could resist a concerted attack if someone knew that there was a message in a given document. For the greatest level of secrecy, a combination of both the technique, steganography and cryptography is necessary.

References
[1] Jassim Mohammed Ahmed and Zulkarnain Md Ali, “Information Hiding using LSB technique”, IJCNSNS International 18 Journal of Computer Science and Network Security, VOL.11 No.4, April 2011
[2] Shawn D. Dickman,” An Overview of Steganography”, Computer Forensics Term Paper, James Madison University
[3] M. M. Amin, et al., “Information hiding using steganography,” in Telecommunication Technology, 2003. NCTT 2003 Proceedings. 4th National Conference on, 2003, pp. 21-25.
[4] Debnath Bhattacharyya, Pouliami Das, Samir Kumar Bandyopadhyay, and Tai-hoon Kim, “Text Steganography: A Novel Approach” International Journal of Advanced Science and Technology Vol. 5, February, 2009.
[5] Richard Popa ,”An Analysis of Steganographic Techniques”.
[6] Adnan Gutub, Mahmoud Ankeer, Muhammad Abu-Ghalioun, Abdulrahman Shaheen, Aleem Alvi “Pixel Indicator High Capacity Techniquefor Rgb Image Based Steganography”.

Fig.5. Retrieve the text