International Journal of Engineering Research & Management Technology ISSN: 2348-4039
May-2017 Volume- 4, Issue-3
Email: editor@ijermt.org www.ijermt.org

SECRETLY CONCEALING MESSAGE USING ADVANCED IMAGE PROCESSING

NARESH SHARMA[1], ABHISHEK TRIPATHI[2], SWATI TIWARI[3]
[1] Assistant Professor, [2,3] B.Tech Students
Department of Computer Science and Engineering
SRM University NCR Campus, Modinagar

ABSTRACT: Steganography is the process of hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the internet. For hiding secret information in images, there is a large variety of steganography techniques some are more complex than others and all of them have respective strong and weak points. Different applications may require absolute invisibility of the secret information, while others require a large secret message to be hidden. This project focuses on Patterned LSB technique with modifications made to enhance security. It also attempts to identify the requirements of a good steganography algorithm and briefly reflects on which steganography techniques are more suitable for which applications. With image steganography we can take advantage over the limited power of the HVS so as to transmit data over public channels that too being undetected. The message that we are going to transmit is going to be hidden in the bits of the image. Steganalysis on the other hand is a way of detecting possible secret communication that has been steganographed.
The main aim of steganography is to transmit a message through some innocuous carrier i.e. text, image, audio and video over a communication channel where the existence of the message is concealed. Information hiding is an emerging research area, which encompasses applications such as copyright protection for digital media, watermarking, fingerprinting, and steganography

Keywords: Steganography, Secret Information, Patterned LSB, Communication, Steganalysis

1.INTRODUCTION

One of the reasons that intruders can be successful is that most of the information they acquire from a system is in a form that they can read and comprehend. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. One solution to this problem is, through the use of steganography. Steganography is a technique of hiding information in digital media. In contrast to cryptography, it is not to keep others from knowing the hidden information but it is to keep others from thinking that the information even exists.

Steganography became even more important as more people joined the cyberspace revolution. Steganography is the art of concealing information in ways that prevents the detection of hidden messages. It includes an array of secret communication methods that hide the message from being seen or discovered.

Due to advances in ICT, most of the information is kept electronically. Consequently, the security of information has become a fundamental issue. Besides cryptography, steganography can be employed to secure information. In steganography, the message is embedded in a digital host before passing it through the network,

thus the existence of the message is unknown. Besides hiding data for confidentiality, this approach of information hiding can be extended to copyright protection for digital media: audio, video and images.

The growing possibilities of modern communications need the special means of security especially on a computer network. The network security becomes more important as the amount of data being exchanged on the internet increases. Therefore, the confidentiality and data integrity is to be protected against unauthorized access and use. This has resulted in an explosive growth of the field of information hiding.

Information hiding is an emerging research area, which encompasses applications such as copyright protection for digital media, watermarking, fingerprinting, and steganography.

2. LITERATURE SURVEY

There are two ways to encode information in a palette-based image; either the palette or the image data can be manipulated. The LSB of the color vectors could be used for information transfer, just like the substitution methods presented. Alternatively, since the palette does not need to be sorted in any way, information can be encoded in the way the colors are stored in the palette. For N colors since there are N! Different ways to sort the palette, there is enough capacity to encode a small message. However, all methods which use the order of a palette to store information are not robust, since an attacker can simply sort the entries in a different way and destroy the secret message. The tools and resources available to help us realize the scope of steganography in an open systems environment were analyzed. The medium and the message to be transmitted can be an image, audio or video file.[1]

An overview of Steganographic techniques in biometric systems was taken. Different compression methods and techniques based on spatial domain and transform domain were overviewed. Techniques observed: DCT, DWT, and HAAR. [2]

Overview of DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform), LSB (Least Significant Bits), Hash LSB, Spread Spectrum in Image Steganography. The importance of Security, Capacity and Robustness in Steganography. [3]

The means of concealing an encoded message within text. The merits in such a system is its potential for hiding the fact that encoding is taking place. Techniques used: Word replacement. [4]

For encryption we have reviewed the patterned LSB where we use four digit channel code ranging from 0001 to 9999 which is used to encrypt the data the encrypted data is sent to the receiver, the receiver uses the same channel code to decode the data and retrieve information.

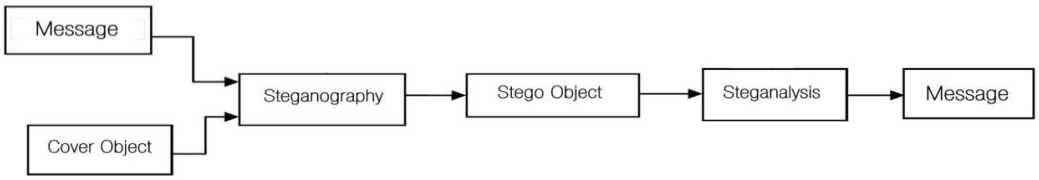
3. EXISTING METHODOLOGY

The problem that we face with the current trend of general Steganography algorithm implementation such as LSB, F5, DCT and DWT is that they are susceptible to:

1. Unwanted detection.
2. Modification of data.
3. Loss of data during retrieval.
4. Drastic increase in size.

Plus there is also the code complexity that increases with the increase in complexity of the above specified algorithms.

Example: If an image is steganographed, the differences in the histograms of the normal and steganographed image are easily visible. This becomes a breach point for detection by hackers and thus a major vulnerability.

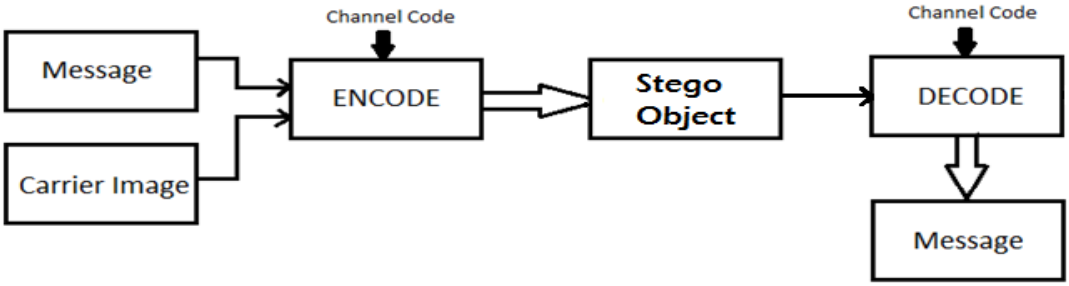


Block diagram: Existing method

4. PROPOSED METHODOLOGY

The prevalent algorithms that we have researched had some or the other shortcomings regarding security, algorithmic complexity and size.

The major point of focus of our study was the LSB algorithm. After research we found out that LSB technique was vulnerable to detection by the intruders because of the visible differences in the color histograms of the sample images. It has also become a very common technique in today's world, thus being much more susceptible to tampering. The LSB technique when implemented also increases noise, image distortion and gives off noise, redundant data when encoding and decoding respectively. Because of the above stated factors we did not inculcate the above technique. Thus we derived a way of encoding data into certain specific pixels of the image, which is not easily susceptible to discovery. The pattern of pixels chosen for encoding is derived from the channel code predefined between the two parties communicating. This channel code is the key to encoding, hence an intruder without the key cannot obtain the hidden message. We call this technique Patterned LSB Encoding.

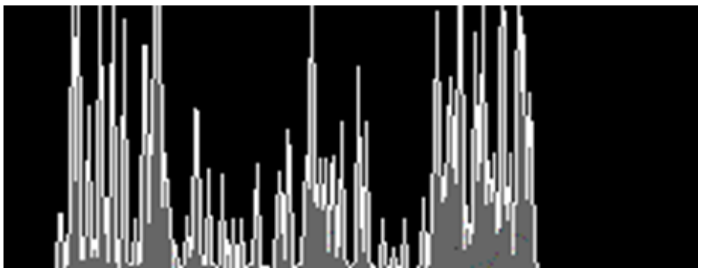


Block Diagram: Proposed System

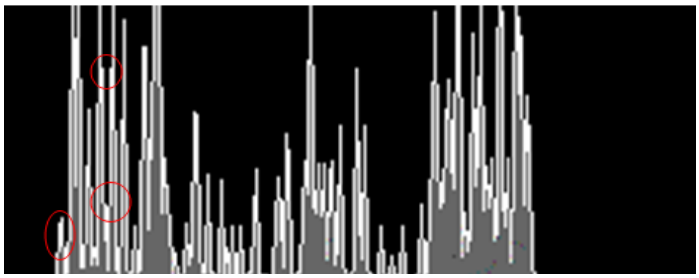
5.RESULT

Comparison of previously used LSB technique with our Patterned LSB technique:
LSB Technique:

(a) Cover Image (b) StegoObject



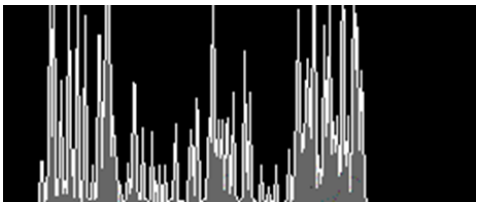
(a) Histogram of Cover Image



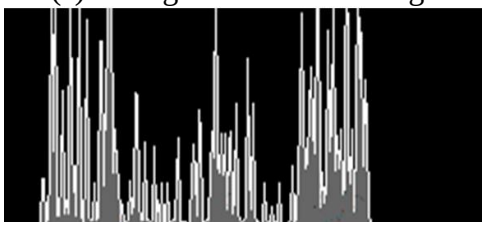
(b)Histogram of StegoObject

Patterned LSB Technique:

(a) Cover Image (b)StegoObject



(a) Histogram of Cover Image



(b) Histogram of StegoObject

Thus, the above defined methodology is *not susceptible to unwanted discovery by hackers or intruders.* Plus there is an additional layer of security due to the channel code.
This application provides the user with the feature of securely hiding a text message in an image file. The plain text message is steganographed by the Patterned LSB Algorithm using a 4-digit channel code. The Steganographed image, whose size does not vary more than the size of the original image, can then be transmitted over a network as per the user requirements. The receiver can then steganalyze the StegoObject with the correct channel code on his/her own end and retrieve the original plain text.

In this way, a covert communication is implemented.

6. CONCLUSION

Although there are many applications that implement steganography but this concept helps us overcome many shortcomings of the existing popular methods such as security and robustness.

User should be aware of the following measures:

1. Both users should have the same key for encryption and decryption [optional].
2. The carrier image should not smaller than 100*100pixels.
3. The text to be embedded should be smaller than the number of pixels in the image.

This project has been a rewarding experience in more than one way. The entire project work has enlightened us in various areas of coding, algorithm design and software modeling. This project seeks to better understand the concept and need for covert communication.

7. REFERENCES

1. Bret Dunbar, *A detailed look at steganographic techniques and their use in an open systems environment*, 2012.
2. H.R. Patel, K. Kishore, K. Sawant. *Fingerprint based image steganography in transform domain*, 2015.
3. P.R. Patel, Yask Patel. *Survey on Different Methods of Image Steganography*, 2014.
4. Michael Morran, George R.S. Weir. *An Approach to Textual Steganography*, 2010.
5. Phillip I Wilson, Mario Garcia. *A Modified Version of the Vigenère Algorithm, IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.3B, March 2006.*
6. D.C. Wu and W.H. Tsai, *A steganographic method for images by pixel-value differencing, Pattern Recognition Letter*s, 24 (9-10)(2003)1613-1626.
7. L.M. Marvel and C.T. Retter, *A methodology for data hiding using images, in: Proceedings of IEEE Military Communications Conference, MILCOM'98, Boston, MA, USA*, 18-21 Oct. 1998, pp.1044-1047.
8. P. Civicioglu, M. Alci and E. Besdok, *Impulsive noise suppression from images with the noise exclusive filter, EURASIP Journal on Applied Signal Processing*, 2004(16)(2004)2434-2440.
9. Anil Kumar, Rohini Sharma. *A secure image steganography based on RSA algorithm and hash LSB technique*, 2013.
10. A. Nikolaidis and I. Pitas, *Region-based image watermarking, IEEE Transactions on Image Processing*, 10(11)(2001)1726-1740.
11. A. Rodriguez and L. Rowe, *Multimedia systems and applications, IEEE Computer,* 28 (5)(1995)20- 22.
12. Bishop, M. Computer Security Art and Security. Person Education Inc. New York, New York, 2003.
13. Dachselt, F., Kelber, K., Schwarz, W., Vandewalle, J. "Chaotic versus classical stream ciphers-a comparative study," Circuits and Systems, 1998. ISCAS '98. Proceedings of the 1998 IEEE International Symposium on Volume 4, 31 May-3 June 1998 Page(s):518 - 521 vol.4
14. Du, W., Atallah, M. "Privacy-Preserving Cooperative Statistical Analysis," ACSAC, p. 102, 17th AnnualComputer Security Applications Conference (ACSAC'01), 2001.
15. Impagliazzo, R. "No Better Ways to Generate Hard NP Instances than Picking Uniformly at Random,"Foundations of Computer Science, 1990. Proceedings., 31st Annual Symposium on 22-24 Oct. 1990 Page(s):812 - 821 vol.2