JCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-2, Issue-4 E-ISSN: 2347-2693

Comparative Analysis of Steganography for Coloured Images

Shrutika Suri[1], Himani Joshi[2], Vishakha Mincoha[3*] and Akash Tyagi[4]

[1,2,3,4]A.P, CSE, MRIU, India*

www.ijcseonline.org

Received: 11/03/2014 Revised: 2/04/2014 Accepted: 26/04/2014 Published: 30/04/2014

Abstract- Information security has become a major cause of concern because intruders are concerned with reading the information. It is because of electronic dropping security is under threat. This paper deals with the comparative analysis of steganography over coloured images. “Steganography” is a greek word which means “hidden writing”. It is the art of hiding the secret message within a image. The goal of steganography is to avoid drawing suspicious to transmission of hidden message. It serves a better way of securing message than cryptography which provide security to content of message and not the existence. Original message is being hidden within a carrier such that the changes occurred in carrier are not observed. The hidden message in carrier is difficult to detect without retrieval.

Different techniques are described in this paper for steganography over coloured images. One of them is spatial steganography. In this technique some bits in the image pixel is used for hiding data. Second technique is Transform Domain Technique which is a more complex way of hiding information in an image. Using Distortion technique, a stego object is created by applying a sequence of modifications to the cover image. The message is encoded at pseudo-randomly chosen pixels. Masking and Filtering technique embed the information in the more significant areas than just hiding it into the noise level. The hidden message is more integral to the cover image. Steganography is efficient, simple and decreases the degree of attack on secret information and improve image quality.

Keywords: Steganography, Cryptography, Secret Information, Distortion, Spatial, Tranform Domain, Masking and Filtering

I. INTRODUCTION

In the field of Data Communication, security-issues have got the top priority. Internet users frequently need to store, send, or receive private information. The most common way to do this is to transform the data into a different form. The resulting data can be understood only by those who know how to return it to its original form. A major drawback to encryption is that the existence of data is not hidden. Data that has been encrypted, although is unreadable, still exists as data. If given enough time, someone could eventually unencrypt the data. It is easy for the intruder to get information about the key which is used to encrypt the secret information. Before the invention of digital means, traditional methods were being used for sending or receiving messages. Traditional methods were used to encrypt the message to provide security from the intruder[3].

Cryptography is a way to secure the plain text messages. Cryptography was created as technique for securing the secrecy of communication. Many different methods have been developed to encrypt and decrypt secret information in order to keep the it secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it is also necessary to keep the existence of the message secret[13]. Cryptography is used to keep the message secret but it does not provide secrecy of the message.

A solution to this problem is steganography. Steganography by word is classified into two parts : steganos which means “secret or covered” and graphics which means “writing”. The purpose of steganography is covert communication to hide a message from a third party. A steganographic system thus embeds hidden content in cover media so as not to arouse an eavesdropper’s suspicion. Steganography is the process of hiding a secret message within a carrier in such a way that someone cannot know the presence of the hidden message. The basic structure of Steganography is made up of three components: the “carrier”, the message, and the key1.[3]

The carrier can be a painting, a digital image, an mp3, even a TCP/IP packet among other things. It is the object that will ‘carry’ the hidden message. A key is used to decode/decipher/discover the hidden message[6].

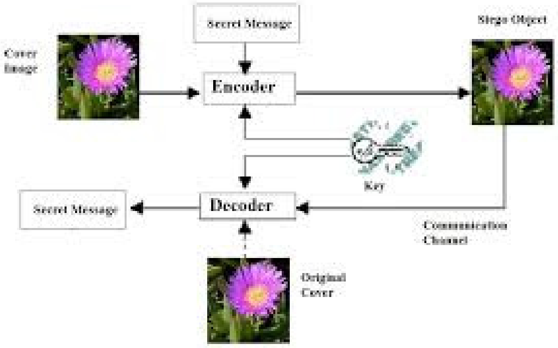

Fig 1. Structure of Steganography

Steganography is often confused with cryptography because the two are similar in the way that they both are used to protect confidential information. The difference between

Corresponding Author: *Vishakha Mincoha3*
A.P, CSE, MRIU, India

the two is that the output of cryptography is scrambled so that it can draw attention but the output of steganography operation is not apparently visible, so both techniques have difference in the appearance in their processed outputs. Steganography and Cryptography are great partners in spite of functional difference. Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated. The strength of steganography can thus be amplified by combining it with cryptography.

A. *TYPES OF STEGANOGRAPHY*

*Text Steganography***:** Text steganography can be achieved by altering the text or by altering certain characteristics of textual elements. It includes line-shift coding, word-shift coding and feature coding[5].

Image Steganography:Images are the most popular cover objects used for steganography. . In the domain of digital images many different file formats exist and for these file formats different algorithms exist[12]. These different algorithms used are least significant bit insertion, Masking and filtering, Redundant Pattern Encoding, Encrypt and Scatter, Algorithms and transformations.

Audio Steganography:In audio steganography, secret message is embedded into digitized audio signal which result slight altering of binary sequence of the corresponding audio file. There are several methods like LSB coding, Phase coding, spread spectrum, Echo hiding which are used for audio steganography.

Video Steganography:Video files are generally a collection of images and sounds, so most of the presented techniques on images and audio can be applied to video files too. The great advantages of video are the large amount of data that can be hidden inside and the fact that it is a moving stream of images and sounds[11].

Protocol Steganography:The term protocol steganography refers to the technique of embedding information within messages and network control protocols used in network transmission. There are covert channels in the layers of the OSI network model where steganography can be used.

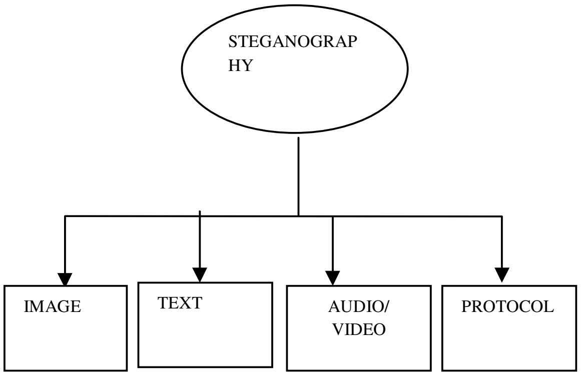

Fig 2. Types of Steganography

B. *TYPES OF CRYPTOGRAPHY*

Cryptography is used to provide security to the plain text. It is used to encrypt the message with key so that no intruder can read the message and decrypt to get the message back. The person who knows the keys will be able to encrypt or decrypt the message[3].

Secret key Cryptography:With secret key cryptography, a single key is used for both encryption and decryption. The sender uses the key (or some set of rules) to encrypt the plaintext and sends the ciphertext to the receiver. The receiver applies the same key to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption.With this form of cryptography, it is obvious that the key must be known to both the sender and the receiver; that, in fact, is the secret. The biggest difficulty with this approach, of course, is the distribution of the key.Secret key cryptography schemes are generally categorized as being either stream ciphers or block ciphers. Stream ciphers operate on a single bit (byte or computer word) at a time and implement some form of feedback mechanism so that the key is constantly changing. A block cipher is so-called because the scheme encrypts one block of data at a time using the same key on each block. In general, the same plaintext block will always encrypt to the same ciphertext when using the same key in a block cipher whereas the same plaintext will encrypt to different ciphertext in a stream cipher.

*Public key Cryptography:*One of the keys is designated the public key and may be advertised as widely as the owner wants. The other key is designated the private key and is never revealed to another party. It is straight forward to send messages under this scheme. Suppose Alice wants to send Bob a message. Alice encrypts some information using Bob's public key; Bob decrypts the ciphertext using his private key. This method could be also used to prove who sent a message; Alice, for example, could encrypt some plaintext with her private key; when Bob decrypts using Alice's public key, he knows that Alice sent the message and Alice cannot deny having sent the message. It helps to provide non-repudiation.

II. MECHANISM

Steganography is the technique of hiding the message in a chosen carrier such that no one except the intended recipient is aware of its existence[3].

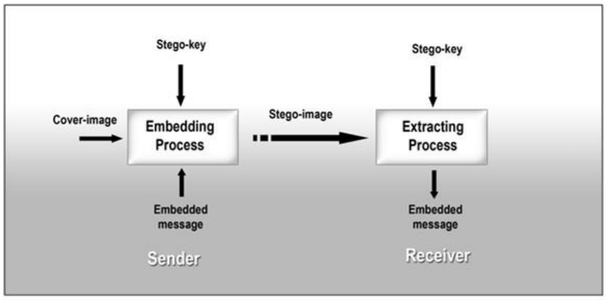

Fig 3.Steps for Steganography

A secret data is being embedded inside a cover image to produce the stego image. A key is often needed in the embedding process. The proper stego key is used by the sender for the embedding procedure[13]. The same key is used by the recipient to extract the stego cover image in order to view the secret data. The stego image should look almost identical to the cover image.

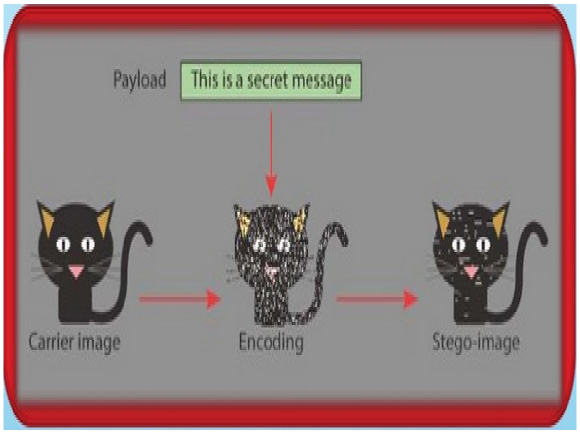

Fig 4. Mechanism of Steganography

III. DIFFERENT TECHNIQUES FOR STEGANOGRAPHY

A. Spatial Domain Methods:

There are many versions of spatial steganography, all directly change some bits in the image pixel values in hiding data[10]. Least significant bit (LSB)-based steganography is one of the simplest techniques that hides a secret message in the LSBs of pixel values without introducing many perceptible distortions. Changes in the value of the LSB are imperceptible for human eyes[4].

Spatial domain techniques are broadly classified into:

1. Least significant bit (LSB)
2. Pixel value differencing (PVD)
3. Edges based data embedding method (EBE)
4. Random pixel embedding method (RPE)
5. Mapping pixel to hidden data method
6. Labeling or connectivity method
7. Pixel intensity based method
8. Texture based method
9. Histogram shifting methods

Advantages of spatial domain LSB technique are:

1. There is less chance for degradation of the original image.
2. More information can be stored in an image.

Disadvantages of LSB technique are:

1. Less robust, the hidden data can be lost with image manipulation.
2. Hidden data can be easily destroyed by simple attacks.

B. Transform Domain Technique:

This is a more complex way of hiding information in an image. Various algorithms and transformations are used on the image to hide information in it[10]. Transform domain embedding can be termed as a domain of embedding techniques for which a number of algorithms have been suggested. The process of embedding data in the frequency domain of a signal is much stronger than embedding principles that operate in the time domain. Most of the strong steganographic systems today operate within the transform domain. Transform domain techniques have an advantage over spatial domain techniques as they hide information in areas of the image that are less exposed to compression, cropping, and image processing[9]. Some transform domain techniques do not seem dependent on the image format and they may outrun lossless and lossy format conversions.

Transform domain techniques are broadly classified into:

1. Discrete Fourier transformation technique (DFT).
2. Discrete cosine transformation technique (DCT).
3. Discrete Wavelet transformation technique (DWT).
4. Lossless or reversible method (DCT)
5. Embedding in coefficient bits

C. Distortion Techniques:

Distortion techniques need knowledge of the original cover image during the decoding process where the decoder functions need to check for differences between the original cover image and the distorted cover image in order to restore the secret message. The encoder adds a sequence of changes to the cover image. So, information is described as being stored by signal distortion[9] . Using this technique, a stego object is created by applying a sequence of modifications to the cover image. This sequence of modifications is use to match the secret message required to transmit.

The message is encoded at pseudo-randomly chosen pixels. If the stego-image is different from the cover image at the given message pixel, the message bit is a “1.” otherwise, the message bit is a “0.” The encoder can modify the “1” value pixels in such a manner that the statistical properties of the image are not affected. However, the need for sending the cover image limits the benefits of this technique. In any steganographic technique, the cover image should never be used more than once. If an attacker tampers with the stego-image by cropping, scaling or rotating, the receiver can easily detect it. In some cases, if the message is encoded with error correcting information, the change can even be reversed and the original message can be recovered.[10]

D. Masking and Filtering:

These techniques hide information by marking an image, in the same way as to paper watermarks. These techniques embed the information in the more significant areas than just hiding it into the noise level. The hidden message is more integral to the cover image. Watermarking techniques can be applied without the fear of image destruction due to lossy compression as they are more integrated into the image.[10]

Advantages of Masking and filtering Techniques:

1. This method is much more robust than LSB replacement with respect to compression since the information is hidden in the visible parts of the image.

Disadvantages of Masking and filtering Techniques:

1. Techniques can be applied only to gray scale images and restricted to 24 bits.

IV. CONCLUSION AND FUTURE SCOPE

Steganography aims to hide the existence of communication by embedding messages within other cover object.[3] So, to obtain privacy we have used the concept of cryptography and on the other hand to implement secrecy, we have used steganography. Steganography is important ,thinking of how to detect and attack it and the methods to do so are far more complex than actually doing the steganography itself. Imagesteganography and its derivatives are growing in use and application[8].In areas where cryptography and strong encryption are being outlawed, citizens are looking at steganography to circumvent such policies and pass messages covertly. As with the other great innovations of the digital age: the battle between cryptographers and cryptanalysis, security experts and hackers, record companies and pirates,
steganography and Steganalysis will continually develop new techniques to counter each other[11]

In this paper we have discussed different techniques of image steganography. Transform domain techniques have an advantage over spatial domain techniques as they hide information in areas of the image that are less exposed to compression, cropping, and image processing .Masking and filtering Technique is much more robust than LSB replacement with respect to compression since the information is hidden in the visible parts of the image.

The possible use of steganography technique is as following:

- Hiding data on the network in case of a breach.
- Peer-to-peer private communications.
- Posting secret communications on the Web to avoid transmission.
- Embedding corrective audio or image data in case corrosion occurs from a poor connection or transmission

ACKNOWLEDGEMENT

We express our deep thanks to **Dr. S.S. TYAGI**, Head of Department (CSE) for warm hospitality and affection towards us. We thank the anonymous referees for their reviews that significantly improved the presentation of this paper.
We are thankful to Ms. "**Shrutika Suri**" for her variable advice and support extended to us without which we could not has been able to complete our paper. Words cannot express our gratitude for all those people who helped us directly or indirectly in our endeavour. We take this opportunity to express our sincere thanks to all staff members of CSE department of MRIU for the valuable suggestion.

REFERENCES

[1] R.Amirtharajan and R.John Bosco Balaguru. ―Constructive Role of SFC& RGB Fusion versus Destructive Intrusion‖.*Proc. International Journal of Computer Applications*1(20):30–36

[2] W. Bender, D. Gruhl, N. Morimoto, A. Lu, ―Techniques for data hiding. *Proc. IBM* Syst. J. 35 (3&4) (1996) 313–336.

[3] N. Provos and P. Honeyman, ―Hide and seek: An introduction to steganography, *Proc. IEEE Security Privacy Mag.*,1 (3) (2003) 32–44

[4] Sutaone, M.S., Khandare, M.V, "Image based steganography using LSB insertion technique", *Proc. IEEE WMMN*, pp. 146-151, January 2008.

[5] Shareza Shirali, M.H, "Anew Approach to persain/Arabic Text Steganography", Computer and Information Science, 2006, ICISCOMSAR 2006,*Proc. 5th IEEE/ACIS International Conference,* 10- 12 July 2006 pp 310-315.

[6]R.Amirtharajan and Dr. R. John Bosco Balaguru, ―*Tri-Layer Stego forEnhanced Security – A Keyless Random Approach*‖ - IEEE Xplore, DOI, 10.1109/IMSAA.2009.5439438.

[7] F.A.P. Petitcolas, R.J. Anderson, and M.G. Kuhn, "Information Hiding—A Survey," *Proc. IEEE*, vol. 87, no. 7, 1999, pp. 1062–1078.

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

[9] Jagvinder Kaur and Sanjeev Kumar, " Study and Analysis of Various Image Steganography Techniques"*Proc. IJCST* Vol. 2, Issue 3, September 2011

[10] R.Amirtharajan and R. Akila," A Comparative Analysis of Image Steganography;" *Proc. International Journal of Computer Applications* (0975 – 8887) ,Volume 2 – No.3, May 2010.

[11]Video Steganography by LSB Substitution Using Different Polynomial Equations‖, A. Swathi, Dr. S.A.K Jilani, *Proc.International Journal of Computational Engineering Research (ijceronline.com)* Vol. 2 Issue. 5

[12]Chandramouli, R., Kharrazi, M. & Memon, N., "Image steganography and steganalysis: Concepts and Practice", *Proceedings of the 2 ndInternational Workshop on DigitalWatermarkin*g, October 2003.

[13]Moerland, T., “Steganography and Steganalysis”, *Leiden Institute of AdvancedComputing Scienc*e,www.liacs.nl/home/tmoerl/privtech.pdf

Author Profile

Shrutika Suri, Assistant Professor,CSE Manav Rachna International University, Faridabad(India). Topics of interest and research fields are Storage area networks and network security.

Himani Joshi pursuing B. Tech. in CSE at Manav Rachna International University, Faridabad(India). Topic of interest is network security management.

Vishakha Minocha pursuing B. Tech. In CSE at Manav Rachna International University, Faridabad
(India). Topic of intersest is network security

Akash Tyagi pursuing B. Tech. in CSE at Manav Rachna International University, Faridabad(India). Area of interest- storage management.