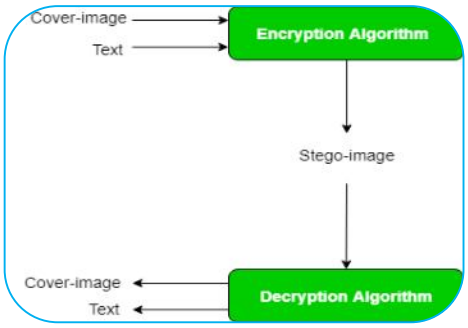
REVIEW OF RESEARCH
ISSN: 2249-894X
IMPACT FACTOR : 5.7631(UIF)
VOLUME - 10 | ISSUE - 9 | JUNE - 2021

STUDY AND ANALYSIS FOR SECURE INFORMATION INSIDE THE IMAGE USING STEGANOGRAPHY

Snehal S. Kale[1] and Dr. V. M. Deshmukh[2]
[1,2]**Department Of Computer Science And Engineering ,**
Prof Ram Meghe Institute Of Technology And Research , Badnera.

ABSTRACT

Due to advances in networking, most of information is kept electronically. Consequently, the security of information has become a fundamental issue. Besides cryptography, steganography can be employed to secure information. Steganography is a technique of hiding information in digital media. In contrast to cryptography, the message or encrypted 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.



KEYWORDS: *cryptography, digital media , secure information.*

1. INTRODUCTION

It is the art and the science of indistinguishable communication ofmessages. It is done by hiding information in other information,i.e. hiding the existence of the communicated information. In image steganography the information is hidden in images. Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels. Hiding information into a media requires following elements [1]:

- The cover media (*C*) that holds the hidden data
- The secret message (*M*), may be plain text, cipher text or any type of data.
- The stego function (*Fe)* and its inverse (*Fe-1*).
- An optional stego-key (*K*) or password may be used to hide and unhide the message.

2. STEGANOGRAPY

The secret image is concealed inside a common image through algorithm and the resultant stegno-image is then hidden again as a visible image inside another image by algorithm. To provide more than one level of protection for the hidden message, we will require additional security level to protect the secret image, which leads to increased complexity of retrieving the secrete image. The results prove the success of system after the secret image is retrieved successfully. Steganography is derived from the Greek word steganographic which means covered writing. It is the science of secret communication. The goal of steganography is to hide the existence of the message from unauthorized party. The modern secure image steganography presents a task of transferring the embedded

information to the destination without being detected by the attacker. 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 exist a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. In this paper I purposed an image based steganography that Random bit substitution technique using intgrated key technique on images to enhance the security of the communication. In the Random bit substitution approach, the basic idea is to replace the Least Significant Bits of the cover image with the Bits of the messages to be hidden without destroying the property of the cover image significantly. Random bit substitution technique using intgrated key is the most challenging one as it is difficult to differentiate between the cover-object and stego-object if few bits of the cover object are replaced.

3. IMAGE STEGANOGRAPHIC TECHNIQUES

There are several Steganographic techniques for image file format which are as follows

3.1 Spatial Domain Technique

There are many versions of spatial steganography, all directly change some bits inthe image pixel values in hiding data. Least signi_cant bit (LSB)-based steganography is one of the simplest techniques that hides a secret message in the LSBs of pixel values without perceptible distortions. To our human eye, changes in thevalue of the LSB are imperceptible. Embedding of message bits can be done either simply or randomly.Least Signi_cant Bit (LSB) replacement technique, Matrix embedding, are some of the spatial domain techniques.

Advantages of spatial domain technique are:

1.Degradation of the original image is not easy.
2.Hiding capacity is more i.e. more information can be stored in an image.

Disadvantages spatial domain technique are:

1.robustness is low
2.Hidden data can be destroyed by simple attacks.

3.2 Masking and Filtering

Masking and Filtering is a steganography technique which can be used on gray- scale images. Masking and Filtering is similar to placing watermarks on a printed image. These techniques embed the information in the more significant areas than just hiding it into the noise level. Watermarking techniques can be applied without the fear of image destruction due to lossy compression as they are more integrated into the image.

Advantages of Masking and filtering Techniques : This method is much more robust than LSB replacement with respect to compression.

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

3.3 Transform Domain Technique

The Frequency domain the message is inserted into transformed coeficients of image giving more information hiding capacity and more robustness against attacks. Transform domain embedding can be termed as a domain of embedding techniques for which a number of algorithms have been suggested. Most of the steganographic systems today operate within the transform domain Trans- form domain techniques have an advantage over LSB techniques as they hide information in areas of the image that are less exposed to compression, cropping, and image processing. 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 of different types:

1. Discrete Fourier transformation technique (DFT).
2. Discrete cosine transformation technique (DCT).

3. Discrete Wavelet transformation technique (DWT).

3.4 Distortion Technique

In this technique, store information by signal distortion and measure the deviation from the original cover in the decoding process. Distortion techniques need knowledge of the original cover image during the decoding process where the decoder functions to check for differences between the original cover image and the distorted cover image in order to restore the secret message. In this technique, a stego-image 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. If an attacker interfere with the stego-image by cropping, scaling or rotating, the receiver can easily detect it.

4.Image Steganalysis

Steganalysis is the breaking of steganography and is the science of detecting hidden information . The main objective of steganalysis is to break steganography and the detection of stego image. Almost all steganalysis algorithms depend on steganographic algorithms introducing statistical differences between cover and stego image.

Steganalysis are of three different types:

Visual attacks it discovered the hidden information, which helps to separate the image into bit planes for further more analysis. Statistical attacks Statistical attacks may be passive or active. Passive attacks involves with identifying presence or absence of a secret message or embedding algorithm used. Active attacks is used to investigate embedded message length or hidden message location or secret key used in embedding. Structural attacks The format of the data files changes as the data to be hidden is embedded, identifying this characteristic structure changes can help us to find the presence of image/text.

5. Random Bit Substitution Technique

LSB is the most simple and a straight forward approach to embed or hide a message into a *cover-image*. The message is embedded with sequence-mapping technique in the pixels of a *cover-image*. Although LSB hides the message in such way that the humans do not perceive it, it is still possible for the opponent to retrieve the message due to the simplicity of the technique. Therefore, malicious people can easily try to extract the message from the beginning of the image if they are suspicious that there exists secret information that was embedded in the image. Therefore, a system named Random Bit Substitution is proposed to improve the LSB scheme. Random Bit Substitution overcome the sequence-mapping problem by embedding the message into a set of random pixels, which are scattered on the *cover-image*. The bits of the secret message is embedded in pixels of the *cover-image* that are generated by Pseudo Random Number Generator.

The algorithm used for Encryption and Decryption in this application provides using random bit of image. This project has two methods – Encrypt and Decrypt. In encryption the secret information is hidden in any type of image file. Decryption is getting the secret information from image file. The data hiding patterns using the steganographic technique in this project can be explained using three phases:

1. Encryption phase
2. Transmission phase
3. Decryption phase

Pseudo Random Number Generator(PRNG) refers to an algorithm that uses mathematical formulas to produce sequences of random numbers. PRNGs generate a sequence of numbers approximating the properties of random numbers. A PRNG starts from an arbitrary starting state using

a seed state. Many numbers are generated in a short time and can also be reproduced later, if the starting point in the sequence is known. Hence, the numbers are deterministic and efficient. Random Number Generators are suitable for applications where many random numbers are required and where it is useful that the same sequence can be replayed easily. Popular examples of such applications are simulation and modeling applications. PRNGs are not suitable for applications where it is important that the numbers are really unpredictable, such as data encryption and gambling.

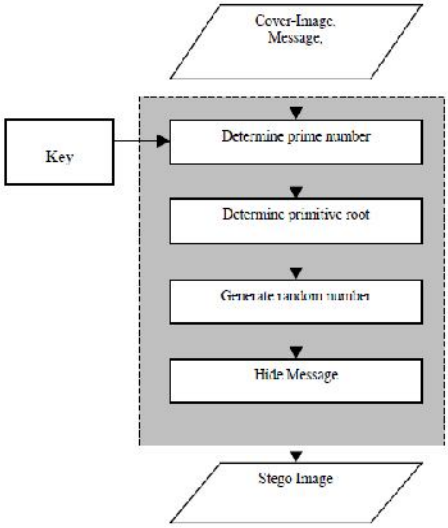


Fig : Flowchart for Random Bit Substitution Technique

SL. No	Imperceptibility	Robustness	Capacity	Tamper Resistance
Simple LSB	High	Low	High	Low
Random Bit Substitution	Higher	Low	High	High

Table : Comparison of characters of above two technique

6. CONCLUSION

The growing possibilities of modern communications need the special means of security especially on computer network. The network security is becoming more important as the number of data being exchanged on the Internet increases. Therefore, the confidentiality and data integrity are requires to protect against unauthorized access and use. This has resulted in an explosive growth of the field of information hiding..

7. REFERENCES

[1] X. Liao, Q. Wen and J. Zhang, (2011).”A steganographic method for digital images with four-pixel differencing and modified LSB substitution”, Journal of Visual Communication and Image Representation, vol 22, no 1, pp. 18.

[2] M. H. Marghny, S. E. El-Gendi, F. Al-Afari and M. ElMelegy, (2009).”Steganography for Secure Data Communication”, Msc Thesis, Faculty of Science, Assiut University, pp. 120.

[3] E. Lin and E. Delp, 1999”A Review of Data Hiding in Digital Images”, in Conference on Image Processing, Image Quality, and Image Capture Systems, PICS, pp. 274-278.

[4] M. H. Marghny, N. M. AL-Aidroos and M. A. Bamatraf, (2012).”Innovative Multi-Level Secure Steganographic Scheme based on Pixel Value Difference”, International Journal in Foundations of Computer Science & Technology, vol. 2, no. 6, pp. 1-13.

[5] S. Katzenbeisser and F.A.P. Petitcolas,(2000) "Information Hiding Techniques for Steganography and Digital Watermarking".

[6] M. H. Marghny, F. Al-Afari and M. A. Bamatraf,(2011) "Data Hiding by LSB Substitution Using Genetic Optimal KeyPermutation", International Arab Journal of e-Technology.

[7] M. Al-Husainy, (2011)."A New Image Steganography Based on Decimal-Digits Representation, Computer and Information Science", vol. 4, no. 6, pp. 38-47.

[8] R.-Z. Wang, C.-F. Lin and J.-C. Lin,(2000). "Hiding data in images by optimal moderately significant-bit replacement", IEE Electron. Lett , vol.36, no. 25, pp. 2069070.

[9] R.-Z. Wang, C.-F. Lin and J.-C. Lin,(2001). "Image hiding by optimal LSB substitution and genetic algorithm", Pattern Recognition, vol. 34, no. 3, pp. 671683.

[10] N. M. AL- Aidroos, M. H. Marghny, and M. A. Bamatraf,(2010). "Data Hiding Technique Based on Dynamic LSB", Naif Arab University for Security Sciences.

[11] N. Wu and M. Hwang,(2014). "Data Hiding: Current Status and Key Issues" International Journal of Network Security, vol. 4.

[12] A. Al-Ataby and F. Al-Naimab (2010). A Modified High Capacity Image Steganography Technique Based on Wavelet Transform, The International Arab Journal of Information Technology, vol. 7, no. 4, pp. 358-364.

[13]Dr N D Jambhekar, Citra Dhawale (july 2015). Bit Level Key Agreement and Exchange Protocol for Digital Image Steganography.