International Journal of Electrical Electronics & Computer Science Engineering
Special Issue - NCSCT-2018 | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
March, 2018 | Available Online at www.ijeecse.com

Comparative Analysis of Image Cryptography and Image Steganography

Ankit Verma[1], Shruti Bijawat[2]
[1]UG Scholar, [2]Assistant Professor, CSE Department, Poornima Institute of Engineering & Technology, Jaipur, Rajasthan
[1]2014pietcsankit012@poornima.org, [2]shrutibijawat@poornima.org

Abstract: This document compares and explains about the two different techniques of Image Cryptography and Image Steganography which comes under the research area of Information Security. Information Security can be defined as preventing any third party unauthorized access of information being communicated between two parties. So basically we compare the techniques of "Image Cryptography and Image Steganography" on the basis of resultant image quality.

Keywords: Image Security, Visual Cryptography, LSB Substitution Image Steganography, Image Encryption and Decryption, Image Cryptography, Image Steganography.

I. INTRODUCTION

Information Security is the practice of implementing tools and strategies to prevent unauthorized or unauthenticated third party access to any piece of information considered secret between two parties. The third party having malicious intentions can misuse the information which can be detrimental to security of vital information being communicated. The aim of information security to prevent misuse or undesired modification to the data or information from any unauthenticated individual.

The goal of implementing security algorithms is to prevent third party interference between the communications of two parties. This is implemented using the process of Encryption and Decryption.

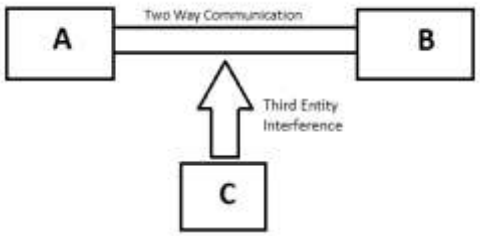

Fig. 1. Communication System

Encryption: Encryption is the process of converting any message in an encrypted format using a key such that only the intended recipient can access the actual message from the encrypted message.

Decryption: Decryption is the process of converting encrypted message into actual message using the same key used for encryption such that the intended recipient can access the actual message.

II. LITERATURE SURVEY

For my research paper I have gone through several previous published research papers as follows:

1. Review of Image Based Cryptography paper published in year 2015 by Jijo. S.Nair and Purvee Raghuwanshion Visual Cryptography and random spatial distribution method.

2. An Image Based Authentication technique using Visual Cryptography schemepaper published in year 2017 by Annie Daisy. V, Vijesh Joe. C, Shinly Swarna Sugi. S. on Visual Cryptography technique identifying the shortcomings that retrieved image suffers from degraded contrast and quality issues due to image pixels.

3. A survey on image steganography based on Least Significant bit Matched Revisited (LSBMR) algorithm paper by G. L. Smitha and E. Baburaj published in year 2016 on Least Significant Bit Matched Revisited steganography algorithm.

4. Implementation of K out of N visual cryptography using K out of K scheme paper by Abul Hasnat, Dibyendu Barman, and Satyendra Nath Mandal on Visual Cryptography published in year 2017.

5. Data Hiding in Images by Adaptive LSB Substitution Based on the Pixel-Value Differencing paper by Suk-Ling Li, Kai-Chi-Leung, L.M. Chengand Chi-Kwong Chan on Least Significant Bit Substitution Algorithm for Image Steganography published in year 2006.

III. OVERVIEW

Information Security in Image based communication for secure transfer of data or information can be implemented using various techniques. Image Based Communication Security can be defined as incorporating various security techniques in order to protect the information and required messages. Digital Images can encrypted and decrypted in such a way so as to ensure that only the intended recipient receives the information or hidden message. The most commonly used techniques for image based communication are the following:

1. Image Cryptography
2. Image Steganography

1. Image Cryptography:

Image Cryptography is the process of using an algorithm for converting an image into an encrypted such that only the intended recipient can retrieve the actual image preventing the third party access. Cryptographic algorithms normally require a set of characters called a key to encrypt or decrypt data. The

International Journal of Electrical Electronics & Computer Science Engineering
Special Issue - NCSCT-2018 | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
March, 2018 | Available Online at www.ijeecse.com

key used in the algorithm is made available only to the sender and the recipient. [1]

Image Cryptography consists of the following two components:

a) Image Encryption

b) Image Decryption

Actual Image
Fig. 2

Encrypted Image
Fig. 3

Decrypted Image
Fig. 4

Image Encryption:

Image Encryption is a process which uses a finite set of instruction called an algorithm to convert original image, known as actual image, into ciphered image, its encrypted form. The Encrypted image is then sent by the sender to the required recipient.

Image Decryption:

Image Decryption is a process which uses a finite set of instruction called an algorithm to convert ciphered image, known as encrypted image, into original image, its actual form. Decryption of image is performed by the receiver so as to obtain the original image sent by the sender.

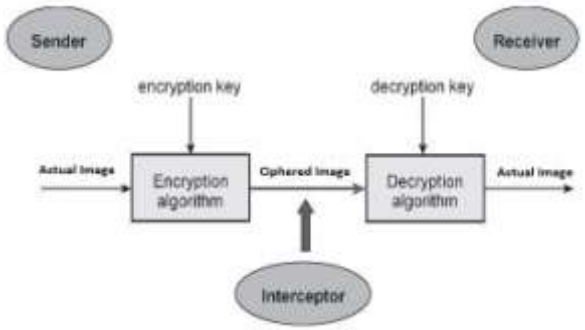

Fig. 5. Image Cryptography Block Diagram

2. Image Steganography:

Image Steganography is the process of writing hidden secret messages within an image such that only the sender and the recipient knows the existence of hidden message within an image. Image Steganography prevents unauthorized users from accessing the message that is hidden within an image. The sender and the recipient are able to communicate with each other secretly as only they know about the existence of any hidden message within an image. Applications of Image steganography include sharing of private content or files, hiding important information including passwords or intelligence information or securely transporting them etc. [3]

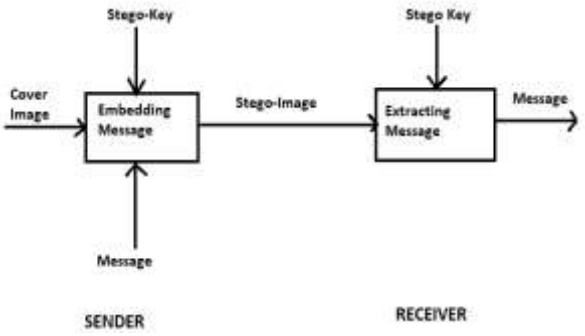

Fig. 6. Image Steganography Block Diagram

Fig. 7. Cover Image

Fig. 8. Steganographic Image

Image Steganography is performed using algorithm that may or may not use a key to hide a message within an image to obtain a stego image that can be communicated between the sender and the receiver. The receiver then is required to use a similar extraction algorithm using the same key(if any) used by the sender to be able to extract the message from the stego image.

The attacker or any other malicious third entity first should be able to detect that steganography has been used within the image in order to break it so as to obtain the hidden message.

IV. METHODOLOGY

1. Visual Cryptography:

Visual Cryptography Algorithm is a technique which allows pictures, text, etc. to be encryptedin form such that decryption is performed by the recipient via visual analysis or sight-reading. Visual Cryptography works along a secret sharing scheme in which an image is broken into n shares such that only that person having all n shares can decrypt the image via overlapping the two share images. It becomes extremely difficult for an individual to decrypt the image if he/she having even (n-1) shares i.e. all n shares of an image are required to

International Journal of Electrical Electronics & Computer Science Engineering
Special Issue - NCSCT-2018 | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
March, 2018 | Available Online at www.ijeecse.com

encrypt and decrypt the image. [4] [2]

N-Share Model:

Pixels are split into m sub-pixels:

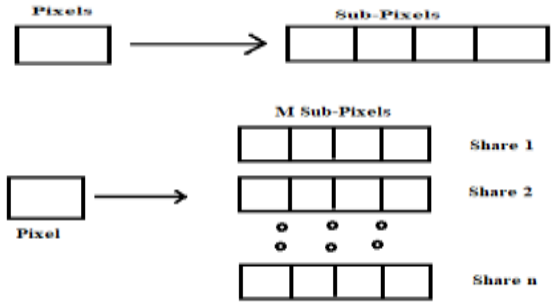

Fig. 9. N-Share Model

In Secret Sharing scheme the two share images Share 1 and Share 2 are overlapped so as to obtain the secret message of the image. Visual Cryptography thus can also be used to deliver secret messages between a sender and the recipient using a similar approach.

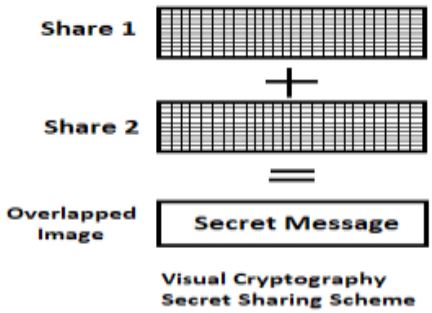

Fig. 10. Secret Sharing Scheme

Demonstration

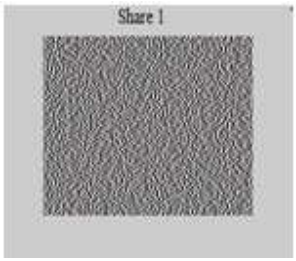

Fig. 11. Share 1 (Encrypted)

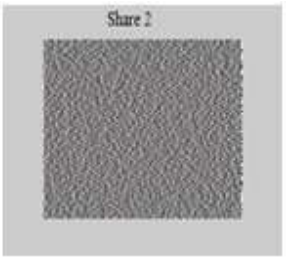

Fig. 12. Share 2 (Encrypted)

Fig. 13. Original Image

Fig. 14. Decrypted Image

2. LSB Substitution Steganography Algorithm:

Least Significant Bit (LSB) Substitution algorithm is the most efficient Steganography Algorithm. In LSB the binary representation of required hidden information is taken and then LSB of each byte within the cover image are overwritten. [5]

We can hide messages within an image if we replace the last bit of every colour's byte with a bit from the message.

Suppose, the binary representation of the colour image is as follows:

10000100 00001001

10010100 00001110

Suppose we want to "hide" the following 4 bits of data: 1011 we get the following,

1000010**1** 0000100**1**

1001010**0** 0000111**1**

Where the each data bits are accommodated in the Least Significant Bits of each byte of the Image.

In Least Significant Bit Substitution Steganography Algorithm, there occurs very minor distortion in the image which is negligible to a human vision. However the distortion in the image increases as the number of bits substituted increases. For example, image with two bits substituted is less distorted than the image with more than two bits substituted i.e. distortion in steganography image depends on the number of least significant bits substituted.

Demonstration

Fig. 15. Cover Image

Fig. 16. Message to be hidden

Fig. 17. Steganographic

Fig. 18. Extracted

Image Quality Analysis:

PSNR stands for the Peak Signal to Noise ratio and is used to identify and measure the quality of an Image.

PSNR Value of an image is an important parameter in image processing applications.

PSNR of an image can be calculated using the following:

To calculate PSNR, Mean Squared Error (MSE) is calculated using the following:

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

The PSNR (in dB) is defined as:

$$\begin{aligned} PSNR &= 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right) \\ &= 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \\ &= 20 \cdot \log_{10}(MAX_I) - 10 \cdot \log_{10}(MSE) \end{aligned}$$

Fig. 19. PSNR and MSE Formulas

V. RESULTS

The following table consists of the PSNR values of the output extracted images for the given sample input message images for both the Visual Cryptography algorithm and the LSB substitution steganography algorithm with 2-bit substitution:

Image	Visual Cryptography	LSB Algorithm
1	23.2452	46.9382
2	32.5455	37.3456
3	15.4243	25.4673
4	26.8662	48.3423
5	42.2117	41.2421
Mean Value	**28.0585**	**39.8671**

VI. CONCLUSION

According to my study, LSB Substitution Steganography Algorithm gives much better results as the Mean PSNR value of LSB algorithm is higher compared to the Mean PSNR value of Visual Cryptography algorithm for the given sample input message images. Higher PSNR value of the extracted output images indicates the higher quality if the image and thus LSB algorithm provides both security to the hidden message and also delivers high quality output than the Visual Cryptography algorithm.

VII. REFERENCES

[1] International Journal of Computer Security & Source Code Analysis, ISSN (O): 2454-5651.

[2] International Conference on Innovative Systems and Control, (ICISC-2017), 978-1-5090-4715-4/17.

[3] 2016 International Conference on Emerging Technological Trends [ICETT], 978-1-5090-3751-3.

[4] International Conference on Innovations in information Embedded and Communication Systems, 978-1-5090-3294-5.

[5]International Conference on Innovative Computing, Information and Control, 0-7695-2616-0.