# A Review and Analysis of Steganography and Visual Cryptography for Secure Data Hiding

**Roshni Rathour[1] Mrs. Preeti Tuli[2]**
[1]Scholar [2]Reader & Head
[1,2]Department of Computer Science Engineering
[1,2]Disha Institute of Management &Technology, Raipur, India

*Abstract*— Security of the secret information has been a challenge when the huge volume of data is exchanged on the internet. Steganography is one of the technique used for concealing information inside an image. Cryptography is a technique which converts the data or plain text into an unreadable form. Visual secret sharing is the technique that divide the secret image into n several shares. Each share holds some information and when the shares are superimposed, a hidden secret image is revealed. It is totally different from the traditional cryptography, because for decrypting the secret image, it does not require any complex computation. The advantage of visual cryptography is that if any one captures a share then single share would not disclose anything about the data. This paper presents a review on various Steganography and visual cryptography techniques that is employed for information concealing. The main objective is to find out a method, which can conceal a large quantity of data in image.

***Key words*:** Steganography, Cryptography, Visual Cryptography, PSNR, Secret Sharing

## I. INTRODUCTION

Information security is a big problem while exchanging a data in an open network, as internet is not only a single network it is worldwide collection of network. It is not restricted by any geographical, national or international boundaries; it means anyone can access it from any part of the world. Although it is very useful for various purposes but there is a risk associated with security of the information which is transfer through the internet. Anyone can hack the information and then make misuse from that or corrupt it or we can say that anyone can destroy the information if it is not fully secured or protected. A secure transfer of knowledge is greatly achieved by Steganography and Cryptography. Generally Steganography is known as "invisible" communication. Steganography is a powerful security tool that has a high level of security, significantly once it is combined with encryption [1]. Steganography word is invented from Greek words Steganós (Covered), and Graptos (Writing) which exactly means "cover writing" [2]. Steganography is the art of concealing secret information in a cover. The cover can be audio, text, image, video, etc. concealment information by inserting secret data into an innocuous medium is commonly referred to as Steganography. Steganography will be applied electronically by taking a secret message (a binary file) and any type of cover (often a sound or image file) and combining both to find a "stego-object". The utilization of Steganography together with visual cryptography could be a secure model and adds lots of challenges to distinguishing such hidden and encrypted knowledge [3]. There are specific terms that are commonly used by the information hiding committees. Throughout this paper, the term 'cover image' is used to describe the selected image to hide the secret data. The image with embedded information is characterized as 'stego-image'. The detection of Stegnographically encoded package is called Steganalysis. The survey was conducted on various Steganography techniques which are very helpful and useful for providing better information security along with some visual cryptography techniques. For providing security to these data basically there are two techniques

- Cryptography
- Steganography

### A. *Cryptography*

Cryptography is a technique which converts the data into an unreadable form. There are two process of cryptography-

- Encryption
- Decryption

### B. *Steganography*

Steganography is the art & science of hiding messages, image or file within another message, image or file. So Steganography is an attempt to hide the existence of the hidden information. In Steganography, the possible cover mediums are images, audio, video, text which will hold the hidden information. Together the cover medium and the hidden message create a stego-carrier.
cover medium + message + key = stego-medium

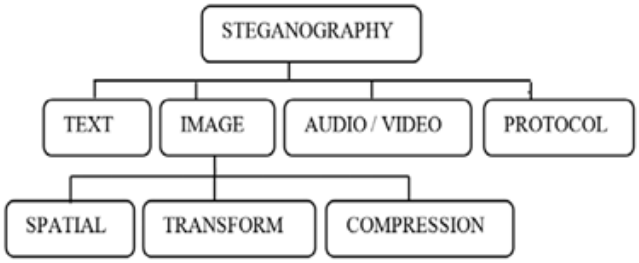


Fig. 1: Classifications of Stenographic techniques

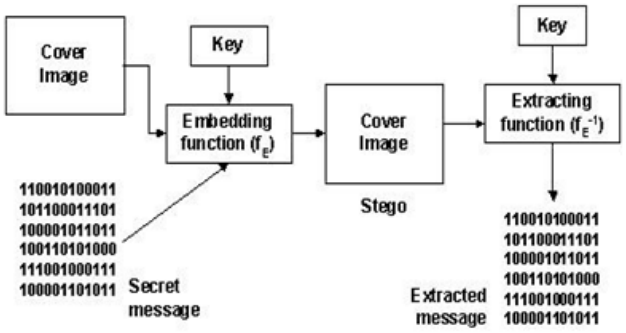


Fig. 2: Steganography process

### C. *Visual Cryptography*

In 1994 Naor & Shamir [4] proposed a new cryptography area called visual cryptography. The idea of visual

All rights reserved by www.ijsrd.com 

cryptography model is to split a secret image into random shares which separately reveal no information about the secret image. The secret image can be recovered by superimposing the shares. Where the decryption is done by the human visual system. Hence, there is no need of any complex cryptographic function for decryption. In Visual cryptography, the secret image is hidden into two or a lot images which are called shares or cover images. Visual cryptography can be used in many applications like transmitting financial documents, banking applications, remote electronic voting applications, authentication & validation. More recent applications are in the field of biometrics such as face privacy, iris authentication & fingerprint scanning. Biometric information in the form of facial, fingerprint and signature images can be kept more secret by splitting into shares, which may be distributed for safety to a number of parties.

### *D. Image Halftoning*

A halftone image is formed from of a series of dots instead of continuous tone. These dots can be completely different sizes, completely different colors, and generally even completely different shapes.

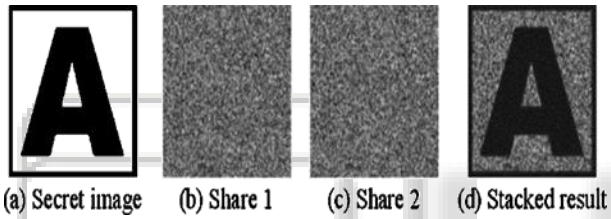


Fig. 3: Working of (2, 2) Visual Cryptography scheme

## II. LITERATURE SURVEY

This section describes the previous work which had been done for data hiding.

### *A. Steganography*

Mehdi Hussain et al., (and other) [1] critically analyzed various Steganography techniques and also covered Steganography overview, its major types, classification and application.

Rahul Joshi et al, [9] introduced the concept of Steganography using LSB method. This method is easy to implement but has some disadvantages. One of the major disadvantage is that intruder can change LSB bit of all image pixels. Hidden message will be destroyed by changing the image quality. It is not immune to noise and compression technique.

Shivani kundra and Nishi madaan, [10] performed analysis of different image Steganography techniques and their comparison is done. They found that performance of the Hash-LSB would be more secure than other techniques and RSA algorithm itself is very secure that no one can break it easily

In [11] author proposed a new method for hiding the information that is instead of hiding data only in least significant bit, hide the data in combination of LSBs. Pairs of bits has been selected to replace with the data bits. Performance of a new method is evaluated by some parameters like PSNR, MSE and Standard deviation. LSB(1,2) bit pair is better than LSB(2,3) as secret message is less visible in LSB(1,2) and by analyzing the values of various parameters quality is also better than LSB(2,3).

Firas A. Jassim, [5] proposed method to hide the secret message inside the cover image using five modulus method. The main advantage of that novel algorithm is to keep size of cover image constant while secret message increased in size.

Chaithra h et al., [3] developed proposed system is to hide message using FMM along with genetic algorithm and Visual Cryptography to ensure improved security and reliability. The major merit of that system is to increase the embedding capacity and secure the information.

In [12] author provides overview of image Steganography and its technique. Author fully analyzed that which technique is best for high level of invisibility. Comparison of different image Steganography algorithm has been discussed based on certain requirements. Some technique lacks in robustness while other lacks in payload capacity. While some techniques provide more security and some become difficult to implement.

In [13] author proposed edge detection method to hide the data into the color images. In this method edge detection, Randomization of edge, encoding text data, decoding text data were the four phases to be performed. Edges were detected using 3*3 window and encode text data into the blue component of sorted edge pixels. Text data can be recovered from encoded image. This method comes under spatial domain technique and result in high data embedding capacity. Edges could hide more data without losing the quality of image. This method also results in good quality of encoded image I.

### *B. Visual Cryptography*

In 1994[4], Naor & Shamir, proposed visual cryptography scheme. In this secret image is divided into exactly two shares & both shares are required for the decryption process. In this, the shares generated are meaningless and is used for black & white images only.

Until the year 1997, visual cryptography schemes were applied to solely black & white pictures. Initial colored visual cryptography theme was developed by Verheu l & Tilborg [7]. The disadvantage of this theme is that they use purposeless shares to cover the key image & the standard of the recovered plain text is unhealthy.

In 2002, Nakajima & Y. Yamaguchi [8], projected a system that take a three photos as associate input & generates 2 pictures that correspond to 2 of the three input photos. The third image is recovered by stacking the 2 output pictures along. While the previous researchers mainly concentrate on binary pictures like text pictures this paper uses the EVC theme appropriate for natural pictures like photography.

In 2003, Hou [14] proposed another color VC scheme. Supported the halftone technique & color decomposition, it decomposes the secret image into three colors C, M & Y. By manipulating the three colors values, the color pixels within the secret image can be represented.

In [15] author proposed aunique approach for concealment knowledge in color images by combining Steganography and extended visual cryptography. In Visual cryptography secret images are partitioned into n range of shares for concealment informationin color images, this

All rights reserved by www.ijsrd.com 

paper utilizes text embedding algorithm and then for share creation which is a visual cryptography part, utilizes VIP synchronization & error diffusion technique. VIP synchronization, this scheme, keep possession of place of pixels having visual information of original images & error diffusion technique is employed to produce share of good quality.

In [16] author introduced a novel concept for conceal data in color images by integrating Steganography and extended visual cryptography. For share generation this paper uses the visual information pixel synchronization. VIP synchronization preserves the positions of pixels carrying visual information of original images throughout the color channels and error diffusion generates shares satisfying to human eyes.

## III. CRITICAL ANALYSIS

| Lit. Ref. | Image Steganography Techniques | Description | Advantage |
|---|---|---|---|
| [17] | Extension of LSB(Least significant bit) | Compression algorithm is used to maximize storage Capacity. | Robust and efficient for hiding text and works efficiently for.bmp images. |
| [18] | Hash-LSB | Uses a hash function to generate a pattern for hiding data bits in LSB. | Hash-LSB with RSA increases the security of secret message. |
| [19] | LSB and DCT(Discrete Cosine Transform) | Comparative Analysis of two techniques based on Security, PSNR. | Peak signal to noise ratio is improved using LSB but security wise DCT is best |
| [20] | LSB with compression technique | Preprocess data is embedded into the LSBs of the pixels. | High image embedding capacity, sufficient payload and high security |
| [21] | IWT(Integer Wavelet Transform) | Hide multiple secret images and keys in cover image. | High quality of the stego image and having high PSNRvalues. |
| [2] | LSB replacement | Generate cross platform and use selected pixel value to represent character. | Increase message security and reduce the distortion rate. |
| [13] | Edge Detection | Edges hide the data without altering the quality of image | High embedding capacity and high quality of encoded image. |
| [22] | DCT (Discrete Cosine Transform) | Hidden data can be distributed more evenly over the whole image in such a way as to make it more robust | It is less robust than DWT and It does not maintain temporal information during transformation. |
| [23] | DWT (Discrete Wavelet Transform) | Coefficients of the wavelets are altered with the noise within tolerable level. It has high flexibility. | Many No of Coefficients are needed to account edge. |

Table 1: Comparison of Steganography Technique-

## IV. CONCLUSION

This paper introduced Steganography and Visual Cryptography analyzed numerous techniques of Steganography, Steganography hides the message in order that intermediate persons cannot see the message. Completely different Steganography techniques have their own robust and weak points. So, it depends upon the size of image (8bit or 24bit) and type of image (jpeg, png, gif etc.), number of secret images& kind of share generated, that which technique is to be chosen. The LSB technique has additional concealment capability but is less robust than other alternative techniques like filtering and transform. On the other hand filtering and masking techniques is restricted to 24 bit and transform techniques are complex and slower. This paper covers review of Steganography and its various techniques of Steganography and visual cryptography used for data hiding. It has concluded from the literature review that there were certain limitations in the existing techniques related to data hiding and data security. So further research in the field is recommended to rectify those limitations.

## REFERENCES

[1] Nagham Hamid, AbidYahya, R. Badlishah Ahmad, DheiaaNajim, LubnaKanaan," Steganography in image files- A survey", Australian Journal of Basic and Applied Sciences, 7(1), 2013
[2] Mehdi Hussain and MureedHussain, "A Survey of Image Steganography Techniques", International Journal of Advanced Science and Technology Volume 54, May 2013
[3] Ravindra Gupta, Akanksha Jain, Gajendra Singh, "Combine use of Steganography and Visual cryptography for Secured Data hiding in Computer Forensics", International Journal of Computer Science and Information Technologies, Vol. 3 , 2012
[4] M. Naor and A. Shamir, "Visual cryptography", in EUROCRYPT '94 Proceedings, Lecture Notes in Computer Science, Springer-Verlag, vol. 950, pp. 1-12, 1995

All rights reserved by www.ijsrd.com 

[5] Firas A. Jassim, "A Novel Steganography Algorithm for Hiding Text in Image using Five Modulus Method", International Journal of Computer Applications (0975 – 8887) Volume 72– No.17, June 2013
[6] Chaithra H, Manjula Y, M Z Kurian, Dr. K. B. Shivakumar, Nuthan A C, "Hiding Technique Using FMM, Visual Cryptography and Genetic Algorithm", International Journal for Research and Development in Engineering (IJRDE) 2014. Vol2-Issue3
[7] Mr. Deepak S. Bhiogade, Prof. Shaikh PhirojChhaware" Steganography and Visual Cryptography for Secured Data Hiding" International Conference on Industrial Automation and Computing (ICIAC),13th April 2014
[8] OmprasadDeshmukh 1, ShefaliSonavane "Multi-Share Crypt-Stego Authentication System" IJCSMC, Vol. 2, Issue. 2, February 2013
[9] Rahul Joshi, LokeshGagnani, Salony Pandey, "Image Steganography with LSB", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 1, January 2013
[10] ShivaniKundra, Nishi Madaan, "A Comparative Study of Image Steganography Techniques", International Journal of Science and Research (IJSR) Volume 3 Issue 4, April 2014
[11] R. Kaur, B. Singh and I. Singh, "A Comparative Study of Different Bit Positions in Image Steganography", International Journal of modern engineering research,vol2, 2012
[12] T. Morkel J.H.P Eloff, M.S. Olivier, "An overview of Image Steganography", information and computer security architecture research group department of computer science, 2005
[13] S. Arora, S. Anand, "A Proposed method for Image Steganography using Edge Detection", International Journal for emerging technology and "Pattern Recognition", 2003
[14] Y. C. Hou, "Visual Cryptography for color images", "Pattern Recognition", volume 17773, 2003
[15] MeghaGoel, M. Chaudhari,"Secured data hiding by using Extended Visual Cyptography", International Journal of Research in Engineering and Technology, Volume 3 Issue 11, Nov 2014
[16] MeghaGoel, Mr. M. Chaudhari," A Novel Approach for Data Hiding by integrating Steganography & Extended Visual Cryptography", International Journal Of Engineering And Computer Science, Volume 3 Issue 7, July 2014
[17] Vipul Sharma, Sunny Kumar," A New Approach to Hide Text in Images Using Steganography", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, April 2013
[18] Kumar and R. Sharma, "A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique", International Journal of Advanced Research in computer science and Software Engineering, vol3, 2013
[19] G. Kaur and A. Kochhar, "A Steganography Implementation based on LSB and DCT", International Journal for Science and Emerging Technologies, vol4, 2012
[20] R. Jain and N. Kumar, "Efficient data hiding scheme using lossless data compression and Image Steganography", International journal of engineering science and technology, volume l4,2012
[21] S.Jayasudha,"Integer Wavelet Transform Based Steganography Method Using Opa Algorithm", Research Inventy- International Journal of Engineering and Science,Volume 2, Issue 4, February 2013
[22] Hardik Patel and Preeti Dave," Steganography Technique Based on DCT Coefficients", International Journal of Engineering Research and Applications, Vol. 2, Issue 1,JanFeb 2012
[23] Barnali Gupta Banik and Prof. Samir K. Bandyopadhyay,"A DWT Method for Image Steganography ",International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 6, June 2013

All rights reserved by www.ijsrd.com 