Data Encryption Based Image Steganography: A Review

Shweta Dahiya
Department of Electronics and Communication Engineering
Bhagat Phool Singh Mahila Vishwavidayalaya, Khanpur Kalan, Sonepat, Haryana, India

***Abstract* - The steganography system which uses an image as the cover, there are several techniques to conceal information inside cover-image (a) Spatial Domain and, (b) Frequency Domain. The spatial domain techniques manipulate the cover-image pixel bit values to embed the secret information. The secret bits are written directly to the cover image pixel bytes. In Frequency domain first images are transformed into the frequency domain and then messages are embeddeding the transform coefficients. Consequently, the spatial domain techniques are simple and easy to implement. This paper reviews few such techniques which focus on image steganography using various data encryption techniques.**

***Keywords* - Steganography, Encryption, LSB, Image Processing.**

I. INTRODUCTION

Steganography is the art and science of communicating in a way which hides the existence of the communication Steganography plays an indispensable/vital role in information security. It is the art of invisible communication by concealing information inside other information. The term steganography is derived from Greek and actually means "covered writing". Steganography consists of three elements: 1) Cover image (which hides the secret message), 2) Secret message and 3) Stegano-image (which is the cover object with message embedded inside it). A digital image is described using a 2-D matrix of the color intestines at each grid point (i.e. pixel). Typically gray images use 8 bits, whereas colored utilizes 24 bits to describe the color model, such as RGB model. The steganography system which uses an image as the cover, there are several techniques to conceal information inside cover-image (a) Spatial Domain and, (b) Frequency Domain. The spatial domain techniques manipulate the cover-image pixel bit values to embed the secret information. The secret bits are written directly to the cover image pixel bytes (Rig Das *et al.*, 2012). In Frequency domain first images are transformed into the frequency domain and then messages are embedded in the transform coefficients. Consequently, the spatial domain techniques are simple and easy to implement (Hamid Nagham *et al*, 2012; Muhammad Khan *et al.*, 2015).

Image steganography is a technique which is used to hide secret message within an image. The binary bits of secret message are hidden in the binary of image and this slightly affects the intensities of color or brightness which is not detectable by naked human eyes there are many algorithms which are used for image steganography but some of them are very complex while some of them are simple. Images are the most popular cover objects used for steganography. In the domain of digital images many different image file formats exist, most of them for specific applications (Hamid Nagham *et al.*, 2012). For these different image file formats, different steganographic algorithms exist.

The motivation behind developing image steganography methods according to its use in various organizations to communicate between its members, as well as, it can be used for communication between members of the military or intelligence operatives or agents of companies to hide secret messages or in the field of espionage. The main goal of using the steganography is to avoid drawing attention to the transmission of hidden information. If suspicion is raised, then this goal that has been planned to achieve the security of the secret messages, because if the hackers noted any change in the sent message then this observer will try to know the hidden information inside the message. One of the most common reasons that intruders can be able to gain unauthorized access of information and they can use this information for their own purpose, to harm someone, modify and attack . As the technologies are continuously growing due to possibilities of information to be hacked or unauthorized are also growing and in modern era communication need special kind of protection from intruders. It's not only limited up to information or communication, it also applies on computer network because internet is only the medium to exchange the message. So, providing more security to computer network is more important because most of the information is transferred over the internet. The main reason to provide is to maintain the confidentiality, integrity, availability and also to stop the unauthorized use of information. This can only be stopped either hiding existence of the information or keeping the information secret. Most common ways to stop this are steganography and cryptography. Both are complementary to each other and provide better security, confidentiality and authenticity. Image steganography is one of key area in the field of steganography. As the demand of security and privacy increases, need of hiding their secret information is going on. If a user wants to send their secret information to other persons with security and privacy they can send it by using image steganography.

The advantage of steganography is that it can be used to secretly transmit messages without the fact of the transmission being discovered. Often, using encryption might identify the sender or receiver as somebody with something to hide. For example, the picture of your cat could conceal the plans for your company's latest technical innovation (Arun Sharma, 2014). Steganography

has a number of disadvantages as well. Unlike encryption, it generally requires a lot of overhead to hide a relatively few bits of information. Also, once a steganographic system is discovered, it is rendered useless. This problem, can be overcome if the hidden data depends on some sort of key for its insertion and extraction (Arun Sharma, 2014).

II. RELATED WORK

Lionel Fillatre [2012]; worked with the detection of hidden bits in the least significant bit plane of a natural image. The mean level and the covariance matrix of the image, considered as a quantized Gaussian random matrix, are unknown. An adaptive statistical test is designed such that its probability distribution is always independent of the unknown image parameters, while ensuring a high probability of hidden bits detection [1].

Hamid Nagham *et al.* [2012]; reviewed the main steganographic techniques for both lossy and lossless image formats, such as JPEG and BMP. The consequences are presented in terms of a taxonomy that focuses on three principal steganographic techniques for hiding information in image files. Those techniques include those modifying the image in the spatial domain, in the transform domain, and those modifying the image file formatting. Each of these techniques tries to satisfy the three most important factors of steganographic design (imperceptibility or undetectability, capacity, and robustness) [2].

Swain Gandharba *et al.* [2012]; a new LSB array based image steganographic technique using encryption by RSA algorithm is proposed. The four arrays, namely the LSB, LSB1, LSB2 and LSB3 are formulated separately by collecting the bits from the 8^{th} (LSB), 7^{th}, 6^{th} and 5^{th} bit locations of the pixels respectively [3].

Parisa Gerami *et al.* [2012]; optimized two image hiding techniques to improve the quality of the stego-image. The first one is to find the best block matching matrix and the other one is to find the optimal substitution matrices. The proposed method utilizes particle swarm optimization (PSO) for finding the best pixel locations, and then the secret image is transformed to a new secret image[4].

Rig Das *et al.* [2012]; described a novel technique for image steganography based on Huffman Encoding. Two 8 bit gray level image of size M X N and P X Q are used as cover image and secret image respectively. Huffman Encoding is performed over the secret image/message before embedding and each bit of Huffman code of secret image/message is embedded inside the cover image by altering the least significant bit (LSB) of each of the pixel's intensities of cover image[5].

Mandal J. K., and Debashis Das *et al.* [2012]; used pixel value differencing (PVD) method for secret data embedding in each of the component of a pixel in a color image. But when we use pixel-value differencing method as image stegano graphic scheme, the pixel values in the stego image may exceed the range 0~255 [6].

Ankit Chadha *et al.* [2013]; introduced a novel method for steganography. It is based on least significant bit manipulation and inclusion of redundant noise as secret key in the message. This method is applied to data hiding in images. For data hiding in audio, Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) both are used. All the results displayed prove to be time-efficient and effective [7].

Arun K. *et al.* [2015]; devised Multi-level encrypted reversible data hiding using histogram shifting for configurable embedding rate. This paper created a reversible data hiding (RDH) scheme for gray scale cover images with highly sensitive cover content [8].

Muhammad Khan *et al.* [2015]; presented secure image steganography using cryptography and image transposition. In this investigation, a new steganographic method based on gray-level modification for true color images using image transposition, secret key and cryptography is presented. Both the secret key and secret information are initially encrypted using multiple encryption algorithms (bit xor operation, bits shuffling, and stego key-based encryption), these are, subsequently, hidden in the host image pixels [9].

Gunda Sai Charan *et al.* [2015]; presented a novel LSB based image steganography with multi-level encryption. In this investigation, a novel approach of encrypting the plain text into cipher text and embedding it into a color image is proposed. Encryption is done in two stages, during first stage it is encrypted by Ceaser cipher technique and in the second stage it is encrypted based on chaos theory. The cipher text obtained after encryption is embedded using 3, 3, 2 LSB replacement algorithm [10].

B. Srinivasan *et al.* [2015]; explained a novel approach for color image, steganography using nubasi and randomized, secret sharing algorithm. A new approach for concealing secret message in a digital image by adding three layer securities has discussed [11].

Parameters	Researchers
LSB Substitution based image steganography	Koushik Dasgupta *et al.* [2012]; Lionel Fillatre [2012]; Swain Gandharba *et al.* [2012]; Parisa Gerami *et al.* [2012]; Ankit Chadha *et al.* [2013]; Khan Muhammad *et al.* [2015]; Gunda Sai Charan *et al.*

Pixel based color image steganography	Mandal J. K., and Debashis Das [2012]; B. Srinivasan *et al.* [2015].
Huffman coding based image steganography	Rig Das *et al.* [2012].
Multil level image steganography	Gunda Sai Charan *et al.* [2015];. [2015]; Arun K *et al.* [2015];
Bio-inspired methods based steganography	Parisa Gerami *et al.* [2012];
Surveys and Comparisons	Hamid Nagham *et al.* [2012];
Image transposition based steganography	Muhammad Khan *et al.* [2015].

III. CONCLUSION

In this work the focus of concern is image because of its widely use in internet and also in mobile system. In this paper, the basics of the steganography, steganalysis and cryptography have been studied. From which Image steganography has been used. As it provides more security and privacy to the user who is sending the secret information to other users. Steganalysis is used to detect the presence of secret information within a specified medium. Now days, image steganography is broadly used in steganography field.

REFERENCES

[1] Fillatre, Lionel, "Adaptive steganalysis of least significant bit replacement in grayscale natural images," Transactions on Signal Processing, IEEE, Vol. 60, No. 2, pp: 556-569, 2012.

[2] Hamid, Nagham, Abid Yahya, R. Badlishah Ahmad, and Osamah M. Al-Qershi, "Image steganography techniques: an overview," International Journal of Computer Science and Security (IJCSS), Vol. 6, No. 3, pp: 168-187, 2012.

[3] Swain, Gandharba, and Saroj Kumar Lenka, "LSB array based image steganography technique by exploring the four least significant bits," InGlobal Trends in Information Systems and Software Applications, pp. 479-488. Springer Berlin Heidelberg, 2012.

[4] Gerami, Parisa, Subariah Ebrahim, and Morteza Bashardoost, "Least significant bit image steganography using particle swarm optimization and optical pixel adjustment," International Journal of Computer Applications, Vol. 55, No. 2, 2012.

[5] Rig Das and Themrichon Tuithung "A novel steganography method for image based on Huffman Encoding," Emerging Trends and Applications in Computer Science (NCETACS), 3rd National Conference, IEEE, pp: 14-18, 2012.

[6] Mandal, J. K., and Debashis Das, "Colour image steganography based on pixel value differencing in spatial domain," International Journal of Information Sciences and Techniques, Vol. 2, No. 4, 2012.

[7] Chadha, Ankit, and Neha Satam, "An efficient method for image and audio steganography using Least Significant Bit (LSB) substitution," International Journal of Computer Applications, Vol. 77, No. 13, pp: 37-45, 2013.

[8] Sharma, Arun, " An overview and survey on image steganography technique," International Journal of Advancement Research in Computer Science and Software Engineering (IJARCSSE), Vol. 4, No. 11, pp: 512-516, 2014.

[9] Muhammad, Khan, Muhammad Sajjad, Irfan Mehmood, Seungmin Rho, and Sung Wook Baik, "A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image," Multimedia Tools and Applications, pp: 1-27, 2015.

[10] Charan, Gunda Sai, S. S. V. Nithin Kumar, B. Karthikeyan, V. Vaithiyanathan, and K. Divya Lakshmi, "A novel LSB based image steganography with multi-level encryption," International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), 2015, pp. 1-5, IEEE, 2015.

[11] Srinivasan, B., S. Arunkumar, and K. Rajesh, "A novel approach for color image, steganography using nubasi and randomized, secret sharing algorithm," Indian Journal of Science and Technology, Vol. 8, No. S7, pp: 228-235, 2015