IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Special Issue-10, May 2019 E-ISSN: 2347-2693

Steganography With Improved Cryptography

Yogesh Gyarsia[1*], Shiv Tiwari[2]

[1,2] Department of Computer Science & Engg., SRIST, Jabalpur, India

[*]*Corresponding Author: yogeshkumar.rocks@gmail.com, Tel.: +91-8109137926*

DOI: https://doi.org/10.26438/ijcse/v7si10.162166 | Available online at: www.ijcseonline.org

***Abstract*—** With the development of technology, secret communication with audio, image and video files has become important. In this case, encryption and steganography play a major role. While encryption deals with uncatchable of message content, steganography deals with failure to understand the existence of the messages used for secret communication. Because of these features steganography and encryption are the two main elements complementing each other. The steganography is the art of hidden; its main aim is to pass unnoticed data in another data. There are many types of data that used in steganography, such as message, image, and video. In this work, we are interested in hiding a message inside an image and also securing it. Our work focuses on the study of least significant bit (LSB) technique for embedding text into image. Moreover, we propose an improved approach for LSB based image steganography and encryption decryption using partitioning, zigzag and swapping.

***Keywords*—**Image steganography, LSB, Cryptography, Symmetric Encryption, Block Cipher, Security

I. INTRODUCTION

Nowadays information concealing procedures are required because of development of web. Much information is exchanged using web. Information hiding is a technique in which mystery information is covered up in some cover media as picture, sound, video documents and more. For the most part pictures are favoured cover media because of huge transmission of pictures over internet. Various kinds of data hiding technique are present such as Reversible Data Hiding [1], Steganography [2], Cryptography [3], and Watermarking [4]. Cryptography is a technique that encrypts plain text to generate cipher text but it may be easily attacked and decrypted. A new technique, Steganography has been developed. Steganography is an art and science of hiding communication and data. Information covering up is important for assurance and validation of information. At the point when just security of information is required, it is called Steganography however when validation of information is required, it is called watermarking. In Steganography, secret communication is used while in watermarking content protection, tamper detection, content authentication and copyright management is used. With the ascent of the web, correspondence through advance media has turned out to be increasingly well known. Security of information is a major concern. In view of wide access of web to the common man, digitally transferred information has a high danger of being assaulted or destroyed. Information hiding is a procedure of concealing data. We use pictures for information hiding particularly advanced pictures. For inserting information in picture there are numerous ways in which pictures are utilized. A few procedures will embed information yet embedding causes some twisting to picture, a few systems can embed little information and a few methods will bring about distortion during extraction of information.

For secure communication of data (image) mainly two methods come into picture. The first method is cryptography, where image pixel are modified using some key and specific algorithm. It produces a scrambled image by changing its appearance. So it can be easily identified just by looking at the image. And, second method is image steganography, where data image is hidden in the cover image without affecting the visible appearance of cover image [5] [6]. The image which embeds the data is cover image. Confidential image that is being transmitted using cover image is referred as data image. The word Steganography is derived from the Greek words stegos meaning cover and grafia a meaning writing [7] defining it as covered writing. A stego-key is used for hiding/encoding process to restrict detection or extraction of the embedded data [8]. Steganography differs from cryptography [9]. The Steganography is usually modeled by prisoner's problem [10]. LSB is a type of spatial domain Steganography approach that embedded the secret data in the least significant bit(s) of the cover image. Most LSB methods contain high hiding capacity and imperceptibility but these approaches are not secure against the attacks, which are made to extract the hidden data, as the embedding positions are known [11]. Some of these attacks are compression and cropping. In [12], detection probability and false alarm are driven in using the number of hidden bits

© 2019, IJCSE All Rights Reserved

in LSB technique. Ramana and Rao [13] implemented LSB to hiding the secret image in image Steganography. They converted images to binary data. Substitution of secret data is done using least significant bits of the cover image. Modulus three of the difference between two DCT coefficients are applied in [14] for embedding two bits of the compressed form of the secret message.

It should be mentioned that current Steganography approaches which aim at pixel substitution like LSB are not robust against compression attacks and filtering. Also, they depend on the format of the cover image. In transfer domain techniques, secret data can be destroyed easily using signal processing techniques. Spread spectrum approaches require more computational complexity and time in comparison with other Steganography techniques. In most distortion techniques, receiver needs the original cover image to detect secret image. If the attackers access to the original cover image, they can easily detect cover modifications and understand the secret data. The scope of the system is that it provides security for image files and reducing the Encryption time and Decryption time. The sender uses the symmetric key to encrypt and the receiver using same key to decrypt the same Image file. Here, we are implementing Image Encryption by using partitioning, zigzag and swapping and also we using this technique to secure multimedia files.

II. RELATED WORK

In recent trends of technology the challenge of improving Information security is important need when sending and receiving data in the fields of data communication and networks. To solve this problem there are several methods used to protect data from unauthorized access during transmission. Many techniques are used to protect the user data. The most efficient technique is using cryptography and Steganography. Cryptography and Steganography are the master areas which take a shot at Information Hiding and Security.

In cryptography, encryption algorithm is the technique of converting transferred data into unrecognizable form to prevent unauthorized access to data unless knowing specific information about the used key. Decryption algorithm is used to reconstruct the original data. Cryptography recently includes using advanced mathematical procedures in encryption and decryption techniques. Cipher algorithms are becoming more complex daily. There two main algorithmic approaches to encryption, these are symmetric and asymmetric [15].

Symmetric-key Encryption uses similar cryptographic key for both encryption and decryption. The used keys must to be similar or there can be a Some changes between the two keys .In asymmetric key encryption algorithms the keys used for encryption and decryption must be different.

Steganography is the technique that deals with hiding secret data in some cover media which may be image, audio, or video. The word Steganography comes from the Greek "Seganos", that mean covered or secret and "graphy" which mean writing or drawing [16].

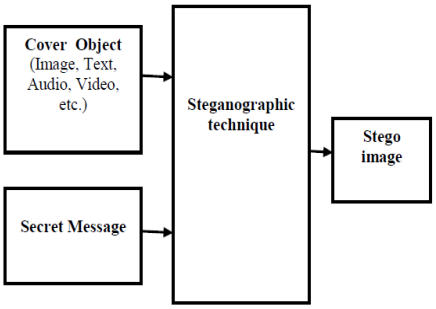

Figure 1: Steganography

The Least Significant Bit (LSB) [17] is a widely used Steganography algorithm. It is based on converting characters of the secret text message into a string of binary bits. The original algorithm uses a gray-scale cover image by embedding up to three bits from the secret text message into the least three significant bits of the cover image pixels. This algorithm was adapted to work on color images by using the three color channels. The eight bits are divided into three bits in one color channel, three bits in another color channel and two bits in the last color channel with many variations of the sequence used [18].

Another adaptation of the LSB is to use it only on a crop from the cover image [19]. It is based on extracting a crop from the cover image and then embedding the secret text message into this crop using LSB approach. The stego image is obtained by reassembling the image and the stego crop. The crop coordinates must be known to the receiver to be able to extract the message. Breaking the security of the embedded message, allowing unauthorized users to view it or detect that the image contains a secret message is discussed in [20]. That is why the Steganography algorithm must be highly secure. LSB algorithm is the simplest and widely used with Steganography technique. It is based on embedding the secret text message bits into the least three significant bits of the cover image pixels. The least significant bits of the cover image are used to hide the secret text message. The LSB Steganography approach can be classified into two main approaches, LSB replacement and LSB matching. LSB replacement is the simplest. It is based on replacing the least three bits of the cover image pixels with each up to three bits of the message data values that need to be hidden. The basic LSB approach is given by

$$C = \{ Xij \mid 0 \le i < Mc, 0 \le j < Nc \} \quad (1)$$

$$Xij \ \{0, 1, 2, 3 \ldots 255\} \quad (2)$$

© 2019, IJCSE All Rights Reserved

$M = \{mi \mid 0 \leq I < N, mi \{0, 1\}\}$.....(3)
where C is the original 8-bit gray-scale cover image of Mc x Nc pixels, and M is the n-bits secret message.
In the image representation and storage schemes, the bits of each byte carry different amounts of information. The last bit a given byte, namely most significant bit (MSB), contains the most information about it. On the other hand, the first bit, i.e., LSB, has the least information about the byte. Therefore, changing the value of this bit yields negligible distortion. This idea is used in Steganography methods for data hiding. More precisely, the bits of embedded (or the transformed) image are placed in the LSB bits of the cover image. Fig. 2 presents an example of applying LSB. In this figure, the cover and embedded data are assumed to be 1011001111001011 and 00, respectively. As it is shown in Fig. 2(C), the LSB bit of each byte in the stego data becomes equal to 0 as a result of embedding 00 in the cover data.

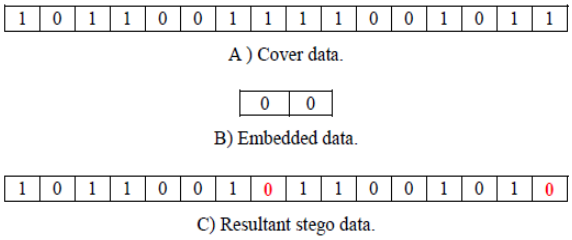

Figure 2: Byte representation for LSB

III. PROPOSED METHODOLOGY

The scope of the system is that it provides security for image files and reducing the encryption time and decryption time.

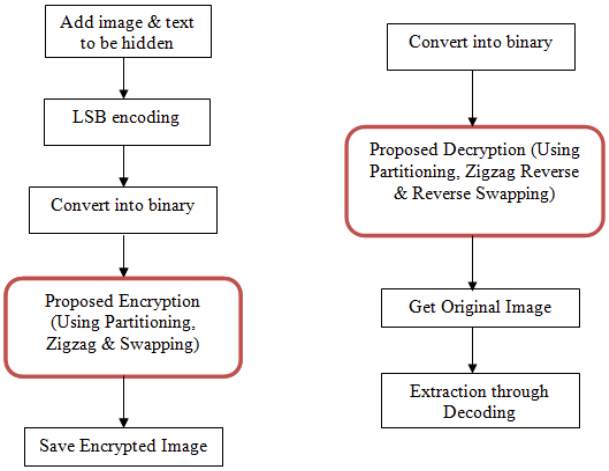

Figure 3: Proposed system

The sender using the symmetric key to encrypt and the receiver using same key to decrypt the same image file. Here, we are implementing image encryption by using partitioning, zigzag and swapping and also we using this technique to secure multimedia files. With the use of steganography, the proposed work as a whole offer maximum security. So, sender can encrypt the data to be hidden using both steganography and the image itself can be encrypted. Reciever uses reverse process to extract the same. The security hence offer is of higher level. Proposed system is shown below:
The functional overview of the system is as follows:
1. The sender gives the Image file and two keys to the system.
2. The system allows us to choose the image file and the text to be hidden using steganography.
3. The system then generates the binary file for the corresponding Image file by using conversion technique.
4. Apply the partitioning technique and zigzag rule and swapping process in accordance with the key.
5. Convert the binary file to the Image file after applying the three processes and send it to the receiver.

Proposed sender process is shown below:

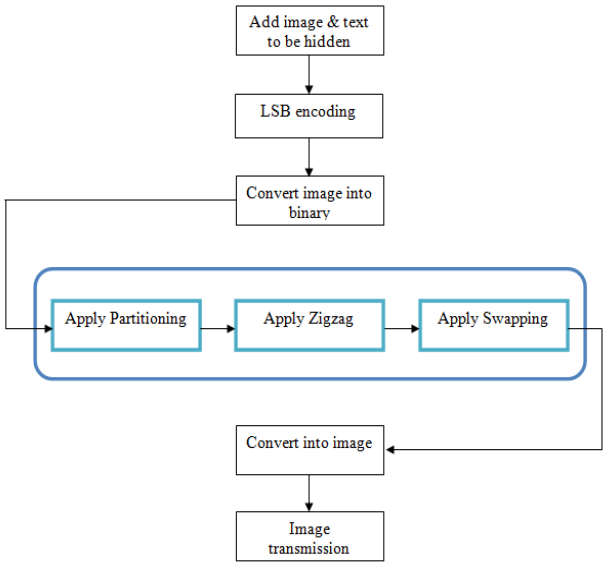

Figure 4: Sender process

Decryption process generally depends on the key. As KEY = i+j, so from first i-bits the value of N can be determined. Then each N-bit from j will select the partitions to swap. For example, when KEY = 0100 1101 0011 and i = 4: 0100 4 = N so there are 2^N or 16 partition. Remaining 8 bits (j) divided by 4 will give M = 2. Now each N or 4-bit will converted into decimal and declare which partitions to swap. As we have got the value of N, following the same procedure used in encryption method number of bits in each partition can be determinable. Then reverse of zigzag rule will apply on each partition. After that, by rearranging the partitions in reverse order) according to the key will return the original data bits.
Proposed receiver process is shown below:

© 2019, IJCSE All Rights Reserved

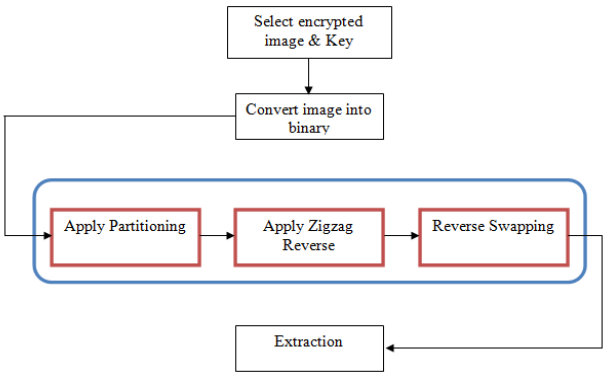

Figure 5: Receiver process

IV. RESULTS AND DISCUSSION

The proposed application takes three steps to hide the data to make impossible for a third party to view without a key to view or edit the secret message.

1. Steganography algorithm: Steganography is the art of passing information in a manner that the very existence of the message is unknown. The goal of steganography is to avoid drawing suspicion to the transmission of a hidden message. If suspicion is raised, then this goal is defeated. Steganalysis is the art of discovering and rendering useless such covert messages. This can be achieved by the title Least Significant Bit insertion means hiding the binary converted data into the LSB bits of Digital image file chosen.

2. Security through obscurity: This is useful for adding another level of security to the Steganography by positioning the bits in random order. For example, if we had 4 bits to hide and the space available was more than 4 bits we can position the 4 data bits in a random order not like as 0,1,2,3.

3. Encryption Algorithm: The last level, which is used to highly strengthen the Steganography is encryption level. This means converting the meaningful information into un-understandable form which is nothing but Cipher. The generally used encryption algorithms are block cipher techniques like advanced encryption standards. Proposed system implements image encryption, by using partitioning, zigzag and swapping of digital contents. So, sender can encrypt the data to be hidden using both steganography and the image itself can be encrypted. The security hence offer is of higher level.

In our proposed algorithm rather than making it complex our intention is to change the bit sequences and also some of the blocks of the target file using several ways. And to remove the problem of zigzag permutation we use partitioning and swapping with zigzag. As the number of partitions and also number of swaps are not constant, it will not further vulnerable for known-plaintext attack. Moreover our proposed method will overcome the size problem as the encrypted file size will remain the same as input file.

Proposed system will not increase size of image. Here, both the image and the text hidden using LSB algorithm are inaccessible to unauthorized parties. The algorithms used in the project are very simple to analyze but when these are implemented together in a sequence, the process of encryption is very solid and cannot be accessed by the unauthorized parties or intruders. Even when the encrypted image and the key is accessed by the intruders, They cannot access the information as they do not know the sequence of steps undergone during the process of encryption which makes them clueless regarding the decryption process.

V. CONCLUSION

Image encryption is one of the oldest and efficient techniques which took data confidentiality to a whole new level. In the project we employ algorithms like steganography, partitioning, zigzag and swapping. Here, both the image and the text hidden using LSB algorithm are inaccessible to unauthorized parties. The algorithms used in the project are very simple to analyze but when these are implemented together in a sequence, the process of encryption is very solid and cannot be accessed by the unauthorized parties or intruders. Even when the encrypted image and the key is accessed by the intruders, They cannot access the information as they do not know the sequence of steps undergone during the process of encryption which makes them clueless regarding the decryption process. Though the encryption techniques used in the project aren't the most complex techniques of image encryption, they are used altogether in a sequence which results in flawless security.

REFERENCES

[1] . X. Zhang, "*Reversible data hiding in encrypted images,"*IEEE Signal Process. Lett. vol. 18, no. 4, pp. 255–258, Apr. 2011.

[2] Pramod R Sonawane, K.B .Chaudhari ,"*Reversible image watermarking using adaptive prediction error expansion and pixel selection*" International Journal Of Engineering Science And Innovative Technology (Ijesit) , Volume 2, Issue 2, March 2013.

[3] Tausif Anwar, Dr. Sanshita Paul and Shailendra Kumar Singh, "*Message Transmission Based on DNA Cryptography: Review*", International Journal of Bio – Science and Bio – Technology, Vol. 6, Issue 5, pp. 215 - 222, 2014.

[4] N. Memon and P. W. Wong, 2001, "*A buyer-seller watermarking protocol*," IEEE Trans. Image Process., vol. 10, no. 4, pp. 643–649.

[5] Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn, "*Information Hiding- a survey*", Proceeding of the IEEE, special issue on protection of multimedia content, pp. 1062-1078, July 1990.

[6] J. Fridrich, M. Goljan, and R. Du, "*Detecting LSB Steganography in color and gray-scale images*," IEEE Multimedia, vol. 8, no. 4, pp. 22–28, Oct. /Dec. 2001.

© 2019, IJCSE All Rights Reserved

[7] R.Anderson and F. Petitcolas, "*On the limits of steganography*" IEEE Journal of Selected Areas in Communications, Vol. 16, No. 4,May 1998.

[8] Niels Provos, Peter Honeyman, "*Hide and Seek: An Introduction to Steganography*," IEEE computer society, 2003.

[9] Chi-Kwong Chan, L.M. Cheng *,"Hiding data in images by simple LSB substitution"*, Department of Computer Engineering and Information Technology, City University of Hong Kong, Hong Kong Received 17 May 2002.

[10] B. Li, J. He, J. Huang and Y. Q. Shi, *"A survey on image Steganography and steganalysis*", Journal of Information Hiding and Multimedia Signal Processing, 2011.

[11] A. Kumar, S. Kumari, S. Patro, T. Sh and A. K. Acharya, *"Image Steganography using Index based Chaotic Mapping*", In IJCA Proceedings on International Conference on Distributed Computing and Internet Technology, ICDCIT, pp.1-4,2015

[12] R. Chandramouli and N. Memon, *"Analysis of LSB based image steganography techniques*", International Conference on Image Processing, IEEE, 2001.

[13] D. V. Ramana and P. N. Rao, *"Steganography Algorithms for Image Security Using LSB Substitution Method*", International Journal of Modern Embedded System, 2016.

[14] A. A. Attaby, M. F. M. Ahmed and A. K. Alsammak, *"Data hiding inside JPEG images with high resistance to steganalysis using a novel technique: DCT-M3*", Ain Shams Engineering Journal, 2017.

[15] Q. Kester, *"A cryptographic Image Encryption technique based on the RGB PIXEL shuffling A cryptographic Image Encryption technique based on the RGB PIXEL shuffling*", International Journal of Advanced Research in Computer Engineering & Technology, vol. 2,no.2 pp.848-854, January 2013.

[16] P. Sahute, S. Waghamare, S. Patil, and A. Diwate, *" Secure Messaging Using Image Stegnography*", International Journal of Modern Trends in Engineering and Research,vol.2,no.3, pp. 598–608, March 2015.

[17] Jassim, Firas A., "*A novel Steganography algorithm for hiding text in image using five modulus method*", arXiv preprint arXiv, Vol. 72, No.17, PP. 39-44, 2013.

[18] Krati Vyas, B.L.Pal, "*A proposed method in image steganography to improve image quality with lsb technique*", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, No. 1, PP. 5246-5251, 2014.

[19] Bandyopadhyay, Debiprasad, et al., "*A Novel Secure Image Steganography Method Based on Chaos Theory in Spatial Domain*", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 3, No. 1, PP. 11-22, 2014.

[20] Thiyagarajan, P., G. Aghila, and V. Prasanna Venkatesan., *"Stego-Image Generator (SIG)-Building Steganography Image Database*", Advances in Digital Image Processing and Information Technology Springer Berlin Heidelberg, PP. 257-267, 2011.

Authors Profile

Mr. Yogesh Gyarsia pursing Master of Technology, in Computer Sc. & Engg. From SRIST, Jabalpur, MP.

Mr Shiv Tiwari is working as assistant profesor in CSE, SRIST, Jabalpur. He pursed Bachelor of Technology and Master of Technology in IT from RGPV Bhopal. He has published many research papers and having more than five years of teaching experience.

© 2019, IJCSE All Rights Reserved