Asian Journal of Computer Science and Technology
ISSN: 2249-0701 (P) Vol.7 No.2, 2018, pp.40-43
© The Research Publication, www.trp.org.in
DOI: https://doi.org/10.51983/ajcst-2018.7.2.1884

A Survey of Different Steganography Technique using Cryptographic Algorithm

Prakhar Agrawal[1] and Arvind Upadhyay[2]
[1]PG Student, [2]Associate Professor
Computer Science and Engineering, Institute of Engineering and Science,
IPS Academy, Indore, Madhya Pradesh, India
E-Mail: prakhar.agrawal277@gmail.com

(Received 3 June 2018; Revised 24 June 2018; Accepted 13 July 2018; Available online 20 July 2018)

Abstract **- Steganography and cryptography are two major aspects of data security . In this paper we are going to provide the survey of different techniques of LSB based Steganography that used cryptography algorithms to secure sensitive information. Steganography is used to hide data and Cryptography is used to encrypt the data. Although cryptography and steganography individually can provide data security, every of them has a drawback. Drawback associated with Cryptography is that, the cipher text looks meaningless, so the unintended user can interrupt the transmission or make more careful checks on the information from the sender to the receiver. Drawback associated with Steganography is that when the presence of hidden information is revealed or even suspected, the message is become known[1].By combining these two methods we can solve both of the above problem. First we encrypt the data using any cryptography technique and then embed the encrypted text into the image. Steganography is the process which hides the presence of secure data during communication. On the other hand cryptography is encrypting and decrypting of secure data and information with a secrete key so that no one can be understand the message directly.**

Keywords: ***Steganography, Images, Cryptography, ECDH, RSA, Security, Data hiding, communication Channel***

I. INTRODUCTION

In the Today's world the most convenient medium of information transfer is the internet; it work as a useful information repository that can be accessible by any people from all over the world. Despite of the various pros provided by the web environment, such as, simple information transfer and sharing, the confidentiality of critical data is also under threat of being compromised [9]. This problem of data security lead us to review and research on data security approaches.

A. Overview of Steganography

The word Steganography originally belongs to Greek word, made of steganos - covered or secret and graphy - writing or drawing. The first steganographic methodology was invented in the history of ancient Greece around 440 B.C [3]. Steganography is a process that is used to send a sensitive information from a sender to a receiver in a way such that a unintended user will not be able to know about the presence of any sensitive. Usually this is done by hiding the sensitive information into another communication medium such as text, picture, audio or video. [8] The main aim of steganography is to transfer sensitive information securely in a completely undetectable way and to avoid drawing suspicion to the transfer of a sensitive information. It is not to keep others from knowing the hidden sensitive information, but it is to keep others from thinking that the information even exists. Following are the types of steganography are Image Steganography, audio Steganography, video steganography and text file steganography [4].

B. Overview of Least Significant Bit Methodology

In a gray scale image each pixel is made up of 8 bits. The last bit of each pixel is termed as Least Significant bit by changing this value will have an effect of the value of pixel by only "1". So, this lease significant bit is used to insert the information in the image. Here we are considering last two bits as LSB bits by changing this value will have an effect of the value of pixel by only "1". This will helps us to storing extra information in the image. The Least Significant Bit (LSB) steganography is a methodology in which least significant bit of the image is replaced with infomration bit. As this technique is vulnerable to steganalysis so as to make it more safer we encipher the raw data before hiding it in the image. By doing encipher of data, steganography process increase the time complexity but on the other hand it will provide us higher security [4].

II. RELATED STUDY/LITERATURE SURVEY

For sending a data from one place to another for various application Cryptography and steganography are most widely used. Mostly in cryptography the content of sensitive information is encrypted and in stenography sensitive information is embed into the cover medium.M. Saritha *et al.* [5] proposed a highly secure model by using cryptography and stenography at the same time. In this paper Symmetric XOR algorithm is used for Cryptography and sequential algorithm is utilized for steganography

A. Dhamija and V. Dhaka [6] propose an outline for cloud engineering which guarantees secure information transmission from the customer's association to the servers of the Cloud Service supplier (CSP). Creators have utilized a consolidated approach of cryptography and steganography since it will give a two path security to the information being transmitted on the system. In the first place, the information gets changed over into a coded organize using encryption calculation and afterward this coded arrange information is again changed over into a harsh picture using steganography. In addition, steganography additionally shrouds the presence of the message, consequently guaranteeing that the odds of information being altered are insignificant.

H. A. Atee *et al.* [7] plans to enhance another plan of concealing a mystery message in a picture, by misusing the advantages of consolidating cryptography and steganography. Another proposed encryption procedure is joined and attempted on account of two steganographic strategies freely keeping the ultimate objective to show up and exhibit its execution and feasibility. The two steganographic strategies are Simple LSB and shading picture based data covering (CIBDH). Exploratory results are then evaluated with respect, as far as possible and generosity. Results achieved demonstrate that the two proposed DELSB and DECIBDH procedures are engaging the extent that security, breaking point and quality.

S. Roy and R. Parekh [8] proposed an enhanced steganography approach for concealing instant messages inside lossless RGB pictures. The target of this work is to build the security level and to enhance the capacity limit while bringing about negligible corruption of the picture. The security level is extended by dispersing the message over the entire picture instead of grouping inside specific picture packages, as in like manner by including a mystery key approval intend to ensure that the message can be recuperated just by the arranged recipient. Capacity limit is expanded by using all the shading channels for putting away data as opposed to holding one of the channels as pixel marker. Picture degradation is constrained by changing only a solitary LSB bit for each shading channel for covering the information along these lines achieving negligible change in the main picture. Experimentations enhanced the circumstance separating as far as possible and quality corruption, set up the commonness of the proposed approach inverse contemporary existing techniques.

In most of the frameworks the right puzzle information is concealed inside the cover picture in a way that it is absolutely unrecognizable. Henceforth, if the introducing instrument is jeopardized, its completely incomprehensible that the covered message can remain unexposed. Security of the secret information can be enhanced if the genuine riddle message isn't embedded in the cover picture by any stretch of the creative ability. S. Samima *et al.* [9**]** proposed a novel method to manage picture steganography through picture affirmation has been proposed in which, rather than sending the genuine riddle information some mapping information of the secret information is embedded in the stengo picture. The bona fide affirmation of the riddle information is moored using a multi layered secure pass key.

In Steganography, the aggregate message will be imperceptible into a cover media, for example, content, sound, video, and picture in which assailants don't have any thought regarding the first message that the media contain and which calculation use to insert or concentrate it. Md. R. Islam *et al* [10]**,** the proposed procedure has concentrated on Bitmap picture as it is uncompressed and helpful than some other picture organization to execute LSB Steganography strategy. For better security AES cryptography system has additionally been utilized as a part of the proposed technique. Before applying the Steganography procedure, AES cryptography will change the mystery message into figure content to guarantee two layer security of the message. In the proposed system, another Steganography procedure is being produced to shroud substantial information in Bitmap picture utilizing sifting based calculation, which utilizes MSB bits for separating reason. This strategy utilizes the idea of status checking for inclusion and recovery of message. This technique is a change of Least Significant Bit (LSB) strategy for concealing data in pictures. It is being anticipated that the proposed strategy will ready to shroud huge information in a solitary picture holding the focal points and disposing of the burdens of the conventional LSB technique. Different sizes of information are put away inside the pictures and the PSNR are likewise computed for every one of the pictures tried. In light of the PSNR esteem, the Stego picture has higher PSNR esteem when contrasted with other strategy. Thus the proposed Steganography strategy is extremely proficient to shroud the mystery data inside a picture.

Steganography is an information concealing procedure that is generally utilized as a part of different data anchoring applications. Steganography transmits information by concealing the presence of the message with the goal that a watcher can't distinguish the transmission of message and thus not ready to decode it. D. Baby *et al.,* [11] proposes an information anchoring procedure that is utilized for concealing numerous shading pictures into a solitary shading picture utilizing the Discrete Wavelet Transform. The cover picture is part up into R, G and B planes. Mystery pictures are inserted into these planes. A N-level deterioration of the cover picture and the mystery pictures are done and some recurrence parts of the same are joined. Mystery pictures are then removed from the stego picture. Here, the stego picture acquired has a less recognizable changes contrasted with the first picture with high general security.

Data security is a standout amongst the most critical components to be viewed when mystery data hosts as imparted between two gatherings. Cryptography and steganography are the two systems utilized for this reason. Cryptography scrambles the data, yet it uncovers the presence of the data. In steganography the mystery data to be imparted is covered up in some other bearer such that the mystery data is imperceptible. S. Hemalatha *et al.,* [12] a picture steganography system is proposed to conceal sound flag in picture in the change space utilizing wavelet change.

The sound flag in any configuration (MP3 or WAV or some other sort) is encoded and conveyed by the picture without uncovering the presence to anyone. At the point when the mystery data is covered up in the transporter the outcome is the stego flag. The outcomes indicate great quality stego flag and the stego flag is dissected for various assaults. It is discovered that the strategy is vigorous and it can withstand the assaults. The nature of the stego picture is estimated by Peak Signal to Noise Ratio (PSNR), Structural Similarity Index Metric (SSIM), Universal Image Quality Index (UIQI). The nature of extricated mystery sound flag is estimated by Signal to Noise Ratio (SNR), Squared Pearson Correlation Coefficient (SPCC). The outcomes demonstrate great qualities for these measurements.

TABLE I REMARKS ON THE PAPER

S. No.	Paper Title	Publication and Year	Algorithm/Method used	Remark
1.	Image and Text Steganography with Cryptography using MATLAB	IEEE 2016	Sequential algorithm for Steganography and Symmetric XOR algorithm for Cryptography	Proposed software is user friendly and help to reduce manual effort and time.
2.	A novel cryptographic and steganographic approach for secure cloud data migration	IEEE 2015	SCMACS (Secure Cloud Migration Architecture using Cryptography and Steganography)	It proposed cloud architecture to secure data transmission from client organization to servers
3.	Cryptography and Image Steganography Using Dynamic Encryption on LSB and Color Image Based Data Hiding	IDOSI 2015	Dynamic Encryption LSB (DELSB) and Dynamic Encryption Color image based data hiding (DECIBDH)	It enhance the quality of image and storage capacity as compare to simple LSB for both gray scale and true color image.
4.	A secure keyless image steganography approach for lossless RGB images	ICCCS 2011	Distribute message over entire image algorithm for steganography	It increase the security level and storage capacity over the existing Pixel Indicator Technique (PIT)
5.	Secure Key Based Image Realization Steganography	IEEE 2013	Image realization algorithm used for steganography	In this rather than sending data some mapping data of original data is embedded.
6	An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography	IEEE 2014	AES algorithm for cryptography and filtering based approach for steganography.	This AES provide two layer security for the message. And Improve the quality of image as compare to LSB based steganography technique.
7	A Novel DWT based Image Securing Method using Steganography	IEEE 2010	It use Discrete wavelet transform for steganography	It hide multiple cover image into single image.
8	Wavelet transform based steganography technique to hide audio signals in image	ELSEVIER 2015	Wavelet transform technique for steganography	It hides audio signal into image.

III. PROBLEM FORMULATION

LSB is one of the most well-known methodology that are used for conceal the sensitive information. LSB hiding methodology use last two significant bits of pixel of image to hide the secret sensitive information in the image, this will impact on the resolution of the image, because of this quality of image will be degraded and someone will be able to attack on image. So there could be always a possibility to remove this drawback and make the sensitive message more safer and improve the quality of the image.

IV. CONCLUSION

In this paper, we presented a review of the algorithms that are used for steganography combined with cryptography. All the review paper focus on improving the quality of image. It is found that there will be always a possibility to improve the quality of image and increase capacity of data that can be hide in the image.

REFERENCES

[1] A. A. Pujari and S. S. Shinde, “Data Security Using Cryptography and Steganography Techniques”, *IOSR Journal of Computer Engineering (IOSR-JCE)*, Vol. 18, No. 4, pp. 130-139, 2016.

[2] H. Abdulzahra, R. Ahmad1 and N. M. Noor, “Combining Cryptography and Steganography for Data Hiding in Images”, *International conference on applied computer and applied computational science (ACACOS’ 14)*, pp. 128-134, 2014.

[3] N. D. Jambhekar and C. A. Dhawale, “The Act of Steganography from Ancient Era to Digital Age”, *IJCA Proceedings on National Conference on Knowledge, Innovation in Technology and Engineering, NCKITE-2015*, pp. 1-4.

[4] M. Pavani, S. Naganjaneyulu and C. Nagaraju, "A Survey on LSB Based Steganography Methods", *International Journal Of Engineering And Computer Science*, Vol. 2, No. 8, pp. 2464-2467, 2013.

[5] M. Saritha, M. Vishwanath Khadabadi and M. Sushravya, "Image and text steganography with cryptography using MATLAB", *In Signal Processing, Communication, Power and Embedded System (SCOPES), 2016 International Conference* on IEEE,, pp. 584-5872016.

[6] Dhamija, Ankit, and Vijay Dhaka. "A novel cryptographic and steganographic approach for secure cloud data migration", *In Green*

Computing and Internet of Things (ICGCIoT),International Conference on IEEE, 2015, pp. 346-351, 2015.

[7] Atee, Hayfaa Abdulzahra, Robiah Ahmad and Norliza Mohd Noor. "Cryptography and Image Steganography Using Dynamic Encryption on LSB and Color Image Based Data Hiding", *Middle-East Journal of Scientific Research*, Vol. 23, No. 7, pp. 1450-1460, 2015.

[8] Sankar Roy and Ranjan Parekh, "A secure keyless image steganography approach for lossless RGB images", *In Proceedings of the 2011 International Conference on Communication, Computing & Security*, pp. 573-576. ACM, 2011.

[9] Samima, Shabnam, Ratnakirti Roy and Suvamoy Changder, "Secure key based image realization steganography", *In Image Information Processing (ICIIP), 2013 IEEE Second International Conference on* IEEE, pp. 377-382, 2013.

[10] Md. R. Islam, A. Siddiqa, Md. P. Uddin, A. K. Mandal and Md. D. Hossain, "An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography", *International Conference on Informatics, Electronics & Vision*, pp. 1-6, 2014.

[11] D. Baby, J. Thomas, G. Augustine, E. George and N. R. Michael, "A Novel DWT based Image Securing Method using Steganography", *Procedia Computer Science,* Vol. 46, pp. 612-618, 2015.

[12] S Hemalatha, U. D. Acharya and A. Renuka, "Wavelet transform based steganography technique to hide audio signals in image", *Procedia Computer Science*, Vol. 47, pp. 272 – 281, 2015.