A Review on Steganography Techniques

Priyanka Thakur

M.Tech. Scholar , SIST Bhopal (M.P) priyankathakur653@gmail.com

Prof. Santosh kushwaha
santosh4mf@gmail.com

Prof.Yogesh Rai
yogeshlnct65@gmail.com

Abstract: In this we are presenting general study of security technique *Cryptography technique, Steganography technique and the combination of both techniques; Both the technique can be applied on various type of secrete message like text, image, video and audio etc individually. As we know that both technique are very powerful technique to provide security which can shield secret message through alter it into unreadable (CIPHER) form by using cryptography technique and conceal with in a cover image by steganography technique and unreadable secrete message conceal inside a cover image through the combination approach Integrity, Security, and authentication for secret message are the prime concern of this work. Combined approach is the most widely used of all users in the digital world of today.*

Keywords:- ***Image Steganography, Secret Image, Cover Image, Stego Image, Steganalysis, Cryptography, LSB(Least Significant Bit), Security.***

INTRODUCTION

Currently all type of information is preserving digitally in digital media like computers. Inter is the basic medium of the digital communication where information are transferring from one user to another user. Every node that means computer system can provide various security techniques for outgoing and incoming information [1]. The sender user and receiver user assumes that transmission of information is secure. But the transmission of information is over insecure mode, then anyone can get the information and read the original information, the challenger can even change the information and send to the receiver user [1, 2]. There are two types of technique for the confidential information security; they are cryptography technique and steganography technique. Cryptography means converting the readable information to unreadable (CIPHER) information.

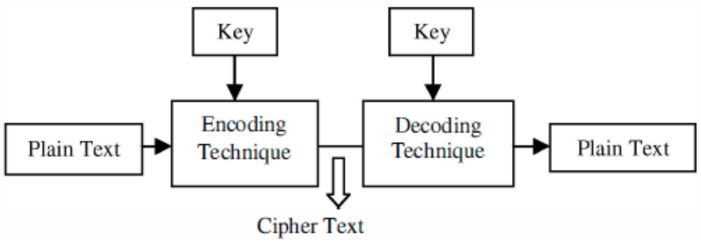

Figure 1: Block diagram for cryptography

But the unreadable information is visible to all, through cryptanalysis on unreadable information, the intruder can get the secrete message, otherwise he can change the cipher information. Steganography technique is used for concealing the information in an image [1, 2, and 3] where the information is not visible for all. Steganography technique support security principal and provides security for images, text or any other type of information also to prevent them from various types of attackers. Steganography technique embeds the secret message in a cover media like image and alter its properties. Steganography technique provides convert communication so that attacker or hacker unable to detect or find out the presence of secret message. To stop the detection of secret messages is the prime art of steganography technique. Steganography technique, derived from Greek word that means "covered writing" [2]. It includes a huge array of confidential communications process that hide the secret message's very subsistence. These process include digital signatures, microdots, invisible inks, character arrangement, spread spectrum and convert channels [1]. The fundamental concept is that it has a cover media that is used to cover the secrete message like image or text, a host entity that is the secrete message or secrete image which is to be transmitted over network, a stego-key which is helped to hide the secret message into cover media like image, and the algorithm of steganography technique to carry out the required entity. The resultant is an image known stego-image which has the secret message inside it, concealed. This stego image is then transmit to the receiver end where the receiver user retrieves the secret message by applying the reverse algorithm of steganography technique (Fig. 2 and Fig. 3) [2].

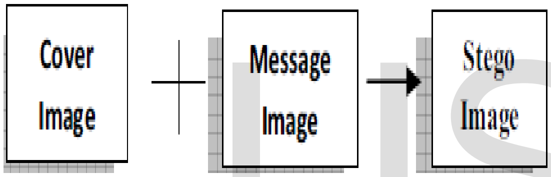

Figure 2: Steganography at sender end

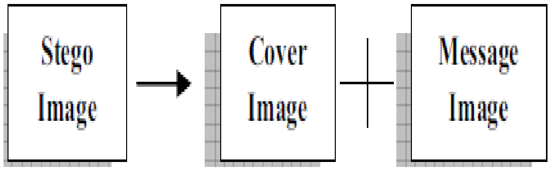

Figure 3: Steganography at receiver end

There are two main divisions in steganography based technique on the area where data is embedded; they are spatial domain steganography and frequency domain steganography [17]. In spatial domain the message is embedded into the image pixel's through least significant bits using different process and in frequency domain the image pixels are first changed into transform or frequency domain through a transformation process and then secret message is embedded in their coefficients, but earlier than transmission it must be changed back into spatial domain to make sure obscurity of embedded message.

In another way there are three kind of steganography techniques are available for hiding the secrete message in a cover image, that is Transformation techniques, Masking and Least Significant Bit Insertion, The above mention three techniques having their own attributes or features [4, 5]. Least significant bit (LSB) insertion is the best technique among all other technique for embedding the secret message in a cover image with less noise ratio, but it is suitable only for a little amount of secrets message where transformation techniques are suitable for embedding the huge amount of secret message in a cover image, the important drawback of transformation technique is, it produces more noise ratio in the produced stego image [10]. By using least significant bit technique, huge amount of secret message cannot be embedded in a cover image [11]. To overcome this problem first applies transformation techniques on the secret message and then apply LSB technique to embed the information.

RELATED WORK

In [1] presented technique before embedding the confidential information into an image, the private data has been compressed through the wavelet transform technique. The bits that are obtained as a result of compression are encoded using quantum gates.

In [2] provides concept for the defense of digital medical images. In this a viable steganography technique using Integer Wavelet Transform (IWT) to protect the MRI type of medical image into a single container image. The stored image was taken and turn over left was applied and the mannequin storage image was access. Then the patient's medical diagnosis image was taken as private image and Arnold transform was tested and contend of secret image was access. In the first case, the scrambled secret image was embedded into the copy container image and Inverse IWT was taken to get a copy secret image. In the second case, the stored image was appropriated and fused with the copy of secret image and stego image was access.

In [3] Data Encryption Standard (DES) based image steganography technique is presented. In this the stability of S- Box mapping & Secret key of DES are used. The preprocessing of confidential image is carried by embedding function of the steganography technique using two exclusive S-boxes. The preprocessing offer high level security and extraction is not possible without the information of mapping rules and private key of the function.

In [4] concerned with carry out Steganography for images, with an change in both security and image quality. The one that is presented here is a deviation of LSB (Least Significant Bit) algorithm. In this assured least significant bits of a cover image are disordered after LSB steganography that co-occur with various prototypes of other bits and that decrease the number of customized LSBs. Thus, fewer numbers of least significant bits of a cover image is changed in comparison to LSB technique, enhancing the PSNR of stego-image. By storing the bit arrangement where LSBs are inverted, message can be obtained properly. To get better the robustness of steganography technique, RC4 technique has been used to achieve the randomization in hiding message image bits into cover image pixels instead of storing them sequentially. This process randomly disperses the bits of the message in the cover image and thus, making it harder for illegal people to remove the unique message.

In[5] a tutorial study of the steganography techniques appeared. Several image steganography techniques have been presented. In this investigation founded various steganography techniques with its Steganalysis. It states a bunch of criteria to examine and calculate the strengths and weaknesses of the earlier presented techniques. The least-significant bit (LSB) insertion technique is the very frequent and easy method for embedding data in a cover image with good capability, while it is noticeable by statistical analysis like Chi-square analyses and RS.

In [6] it is observed that an method for Image steganography based on LSB technique using X-box mapping presented where they it used numerous Xboxes having unique information. The embedding part is completed by Steganography in which four unique X-boxes with sixteen other values and every value is mapped to the four LSBs of the cover image.

In [7] propose three methods which variant of Cipher Block Chaining concept mode for image encryption by considering three various traversing paths Horizontal, Diagonal and Vertical. In this method one straightforward Raster Scan has been working to scramble the secret Image known as Horizontal Image Scrambling. Second method is an alternative of first method known as Vertical Image Scrambling; here traversing pathway would be left to Right and top to bottom. Third method works diagonal traversing pathway known as Diagonal Image Scrambling. Later Image Steganography has been tailored to send these Scrambled Images in an invisible manner.

In [8] a technique based on Huffman Encoding for image steganography is granted. In which two 8 bit gray level image of size A X B and R X S are using as a secret image and cover image respectively. Huffman method is applying on the secret message earlier than embedding and every bit of Huffman code of message /secret image is embedded within the cover image by altering the least significant bit (LSB) of each of the pixel's intensities of cover image. Huffman encoded bit stream Size and Table of Huffman are also embedding within the cover image.

Hence, in [9] described and reviewed the dissimilar research that has done in the direction of text encryption and information in the block cipher. As well as, in this suggests a cryptography model in the block cipher. There is type of security issues in message communication. Cryptography is a substantially safe approach to provide protection in data sending and receiving.

In [10] secret allocation refers to a manner of distributing a confidential amongst a group of members, each of whom is allocated with distributes of the confidential. The participant's division is used to rebuilt the secret. Single specific participants division is of no use. The unpredictable image distribution threshold and approach schemes are used achieve the novel private color image allocation. The confidential image (Color) pixels will be transformed to N-ary notational system. The reversible polynomial function will be generated using (k-1) digits of confidential image (color) pixels. Confidential shares are produced with the help of participant's numerical key and the reversible polynomial function. The cover image and the confidential image is embedded with each other to build a stego image. The reversible image sharing method is used to rebuild the cover image and confidential image. The secret is access by the Lagrange's formula produced from the sufficient confidential shares.

In [11] focused on the consolidation of cryptography and steganography methods and a technique – Metamorphic Cryptography. The data is transformed into a cipher image by a key value, hided into another image by steganography through converting it into an intermediate text and then finally transformed intermediate text into an image.

In [13] describe on privacy and strategies to achieve social privacy issues. they describe both teens' practices and the structural circumstances where they are concealed, highlighting the ways where privacy, as it acting out in per day life, is correlated more to organization and the capability to manage a social situation than particular characteristic of information.

In [15] ASK algorithm is used by a novel algorithm for hiding information. Using cryptography perceptive information is hided in a color image. This shows how to send data using a color image without illiteracy of third party. The algorithm explains a method for vanishing data in a color image.

ANALYSIS

Generally an image steganography is classified in following aspects [18].

- High Capacity: Maximum size of message can be entrenched into image.
- Perceptual Transparency: After beating process into a cover image, quality of perceptual will be besmirched into stego image as compare to original cover image.
- Robustness: After embedding, information should keep on integral if stego image goes into a number of transformation such as filtering, addition of noise cropping and scaling.

- Temper confrontation: It should be not easy to amend the message once it has been entrenched into stego image.
- Calculation of Complexity: How much valuable it is computationally for entrenching and removing a concealed message?

Table-1 presents the best steganography measures.

Table 1: Algorithm of Image Steganography Measures [18]

Measures	**Drawback**	**Benefit**
Capacity High	Low	High
Perceptual Transparency	Low	High
Robustness	Low	High
Temper Resistance	Low	High
Computation Complexity	High	Low

From the study of earlier presented work and on these measurements the main disadvantage of such methods, however, is that one cannot send large messages because there is a trade-off between the size of the message and robustness against attack. What concerns us most in this paper is the fact that almost all steganography methods applied on digital images change the structure and statistics of the images in when a hidden message is embedded in them. Furthermore we have observed security issues and selection process of LSB from cover image. In security point of view there is no private key and its size define by the many earlier presented work Furthermore selection of LSB bits from cover image to replace one secrete bits which is the causes of larger cover image size and we have already know that large size of cover image can affected execution speed. Another issues we have observed that is large cover image is required to embedded secret information, due to this reason efficiency and quality of the stego image are degrading.

CONCLUSION

Here, we gave a general idea of various steganography techniques its main types and categorization of steganography technique which have been presented in the literature for the duration of last few years. We have significant analyzed various presented techniques which show that illustration quality of the stego image is degraded when concealed message increased up to certain limit through LSB based process. There are three mainly required evaluation parameters for good steganography techniques are Imperceptibility Capacity and Robustness. But there is no such type technique so far for any type of color images where it would target to full fill all these parameters effectively. So there is requirement of such type technique where it would provide high PSNR value, good capacity and opposed to all targeted as well as common Steganalysis attacks. The strength of Least-Significant-Bit (LSB) steganography technique are that it is easy to understand, simple to implement, and it generate stego-image that is approximately comparable to cover image and its illustration infidelity cannot be measured by naked eyes. In future we will design and developed hybrid security concept in which cryptography and steganography both will provide their own strength.

REFERENCES

[1]Kumar, R.P. ; Hemanth, V. ; Shareef, M. "Securing Information Using Sterganoraphy" Published in IEEE International Conference on

Circuits, Power and Computing Technologies (ICCPCT), 20-21 March 2013 Page(s):1197 - 1200 Print ISBN:978-1-4673-4921-5 INSPEC Accession Number:13583743

[2] Prabakaran, G., Bhavani, R. Rajeswari P.S. "Multi secure and robustness for medical image based steganography scheme" Published in IEEE International Conference on Circuits, Power and Computing Technologies (ICCPCT), 20-21 March 2013

Page(s): 1188 - 1193 Print ISBN:978-1-4673-4921-5 INSPEC Accession Number:13583718

[3] Ramaiya MK, Hemrajan N.i, Saxena A.K. "Security Improvisation in Image Steganography using DES" Published in IEEE 3rd International Advance Computing Conference (IACC), 22-23 Feb. 2013 Page(s): 1094 - 1099 Print ISBN:978-1-4673-4527-9 INSPEC Accession Number: 13498964

[4] Akhtar, N. ; Johri, P. ; Khan, S. "Enhancing the Security and Quality of LSB Based Image Steganography"

Published in 5th IEEE International Conference on Computational Intelligence and Communication Networks (CICN), 27-29 Sept. 2013 Page(s):385 - 390 INSPEC Accession Number: 13896095

[5] Selvi, G.K. ; Mariadhasan, L. ; Shunmuganathan, K.L. "Steganography Using Edge Adaptive Image" Published in IEEE International Conference on Computing, Electronics and Electrical Technologies (ICCEET), 21-22 March 2012 Page(s):1023 - 1027 Print ISBN: 978-1-4673-0211-1 INSPEC Accession Number: 12761978

[6] Nag A., Ghosh S., Biswas S., Sarkar D., Sarkar P.P. "An Image Steganography Technique using X-Box Mapping" IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012) March 30, 31, 2012

[7] Amirtharajan, R. ; Anushiadevi, R. ; Meena, V. ; Kalpana, V. "Seeable Visual But Not Sure of It" IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM - 2012) 30-31 March 2012 Page(s):388 - 393 Print ISBN:978-1-4673-0213-5 INSPEC Accession Number: 12818719

[8] Das, R. ; Tuithung, T."A Novel Steganography Method for Image Based on Huffman Encoding" Published in 3rd IEEE National Conference on Emerging Trends and Applications in Computer Science (NCETACS), 30-31 March 2012 Page(s):14 - 18 Print ISBN: 978-1-4577-0749-0 INSPEC Accession Number:12772541

[9] Al-Abiachi, A.M. ; Inf. Technol. Dept., Univ. Utara Malaysia, Sintok, Malaysia ; Ahmad, F. ; Ruhana, K. "A Competitive Study of Cryptography Techniques over Block Cipher" Published in 13th IEEE International Conference on Modelling and Simulation March 30 2011-April 1 2011 Page(s):415 - 419 E-ISBN :978-0-7695-4376-5 Print ISBN:978-1-61284-705-4 INSPEC Accession Number:11963172

[10] Anbarasi, L.J. ; Kannan, S. "Secured Secret Color Image Sharing With Steganography" Published in IEEE International Conference on Recent Trends In Information Technology (ICRTIT), 19-21 April 2012 Page(s):44 - 48 Print ISBN:978-1-4673-1599-9 INSPEC Accession Number:12769941

[11] Philjon, J.T.L. ; Rao, N.V. "Metamorphic Cryptography - A Paradox between Cryptography and Steganography Using Dynamic Encryption" Published in IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 3-5 June 2011 Page(s):217 - 222 Print ISBN:978-1-4577-0588-5 INSPEC Accession Number:12145614

[12] Rosziati Ibrahim and Teoh Suk Kuan "Steganography Algorithm to Hide Secret Message

inside an Image" Published in international journal of Computer Technology and Application 2011, PP102-108

[13] danah boyd and Alice Marwick "Social Steganography: Privacy in Networked Publics" ICA 28 May 2011 www.danah.org/papers/2011/Steganography-ICAVersion.pdf

[14] Yandji, G.-A. ; Lui Lian Hao ; Youssouf, A.-E. ; Ehoussou, J. "research on a normal file encryption and decryption" Published in IEEE International Conference on Computer and Management (CAMAN), 19-21 May 2011 Page(s):1 - 4 Print ISBN:978-1-4244-9282-4 INSPEC Accession Number: 12033234

[15] Gupta, A. ; Mahapatra, S. ; Singh, K. " Data Hiding in Color Image Using Cryptography with Help of ASK Algorithm" Published in IEEE International Conference on Emerging Trends in Networks and Computer Communications (ETNCC), 22-24 April 2011 Page(s):15 - 17 Print ISBN:978-1-4577-0239-6 INSPEC Accession Number:12121399

[16]Kaushik, A. ; Kumar, A. ; Barnela, M. " Block Encryption Standard for Transfer of Data "Published in IEEE International Conference on Networking and Information Technology (ICNIT), 11-12 June 2010 Page(s):381 - 385 E-ISBN :978-1-4244-7578-0 Print ISBN:978-1-4244-7579-7 INSPEC Accession Number:11432174.

[17] Siva Janakiraman, Anitha Mary.A, Jagannathan Chakravarthy " Pixel Bit Manipulation for Encoded Hiding-An Inherent stego" Published in International Conference on Computer Communication and Informatics (ICCCI -2012), PP no 1-6 Jan. 10 – 12, 2012, Coimbatore, INDIA.

[18] Mehdi Hussain and Mureed Hussain "A Survey of Image Steganography Techniques" published in International Journal of Advanced Science and Technology Vol. 54 May , 2013 PP 113-124.Avilable at http://www.sersc.org/journals/IJAST/vol54/11.pdf