Information Hiding Techniques – A Review

Gaurav
Research Scholar, Department of CSE, UIET, MDU, Haryana

Abstract – Today, secure correspondence is the need of the general public. Most well known methods utilized for secure correspondence in the present time are Steganography and Cryptography. Steganography is utilized to conceal the presence of the information inside some spread media like picture record, sound document, video document, content document and so forth. Image file is most abundantly used as a carrier for steganography. Numerous algorithms are available for image steganography like PC technique, Least significant bit technique and Matrix Determinant technique. Some of the available techniques have been reviewed by me in this paper.

Keywords – Stego Image, Cover Image, High Quality Image, Cryptography, Steganography and so on.

I. INTRODUCTION

As the web is the fundamental need in the present life. Web is the most unbound stage to impart but since of its highlights numerous clients lean toward this stage to convey and that is the reason the security include comes as a main priority [1]. With the progression of web innovation, advanced media including pictures are transmitted effectively over the system. So as to guarantee the protected transmission of information over the web, information encoding [11] and information concealing [4– 9, 12– 16, 19, 21– 22] are two generally utilized procedures. Information encoding is a system used to shield information from illegal access by changing it into unimportant codes. Information concealing is unique in relation to information encryption as it shrouds the mystery information into a spread that might be a picture, sound, video, information or other media to occupy the consideration of the eyewitness [5, 6]. These pictures are promptly accessible on web with various record groups stimulate little doubt and it gives rich repetition to information implanting [9]. Information security is typically accomplished utilizing different cryptography methods. The idea of numerous encryptions of the information is likewise announced in [1, 12] to give extra layers of security to the mystery information. In numerous encryptions, yield of one encryption technique is made as the contribution to the next encryption strategy.

Nonetheless, information encryption isn't everything that gives solid security to the information. What's more, nearness just as transmission of information is likewise required to be made secure. For the protected nearness just as transmission of information, steganography is required constantly. Be that as it may, neither cryptography nor steganography guarantees complete security to the information or data remarkably as an independent application. So as to beat this disadvantage, present day pattern is to coordinate these two strategies to accomplish basic security. There are a few papers in writing in which unique information is encoded before implanting into the spread picture for extra layer of security. These strategies incorporate Advanced Encryption Standard (AES) [11], Data Encryption Standard (DES) [2, 10, 11, 20], Triple DES [10, 11, 20], International Data Encryption Algorithm (IDEA) [10, 11], Rivest-Shamir-Adleman (RSA) [1], Substitution Cipher [11], Play reasonable Cipher [11], Rivest Cipher-4 (RC 4) [11], Secure Hash Algorithm-2 (SHA-2) [10] or changed encryption techniques. In any case, DES and AES are not reasonable for dealing with massive information (advanced pictures) because of their serious computational procedure [10, 20] except if quickened by equipment usage. In writing, different information concealing strategies are additionally accessible, be that as it may, to go about as independent application as it were. Concealing information in pictures utilizing Least Significant Bit (LSB) substitution just as its ensuing alterations is accounted for broadly in the writing [6, 21, 22]. However, effortlessness of supplanting LSBs of picture pixels with the mystery message gives obvious favorable position to this strategy, yet the mystery message can be destructed effectively by the assailant by basically exchanging or supplanting the message data put away in the LSB places of the picture pixels either by zeros or ones or blends of ones.

To expand the information concealing limit and security, unique information is packed (utilizing existing data\image pressure systems) before implanting into the spread picture [15, 17, 18]. The information concealing technique is

displayed dependent on the idea of equality condition [3, 13]. They separate the picture pixel into two squares, one square is called Parity Reflecting Block (PRB), while other square is known as Pixel Adjustment Block (PAB). The data about concealed piece is reflected by equality condition in the equality reflecting square. To expand the information concealing limit mystery information is scrambled and compacted utilizing Chinese Remainder Theorem (CRT) before inserting into spread picture [3]. They utilized the lower bits just as fifth and sixth upper bits for pixel change in accordance with improve the visual nature of stego picture. In 2014, Jindal and Singh portrayed the information concealing technique that legitimately supplanted the fourth LSB bit [14]. In this strategy lower bits just as fifth upper piece is utilized for pixel alteration which fundamentally improve the visual nature of stego picture.

We define 'cryptography' as a technique of keeping and sending content such that only the authorized users can access and perform operations on the desired content. We can also call it as a way of securing contents by encrypting it into non-readable format. Cryptography is a viable method for defensive delicate data as it is put away on media or transmitted through system correspondence ways [23]. Despite the fact that a definitive objective of cryptography and the components that influence it to up, is to conceal data from unapproved people. Steganography was typically utilized related to cryptography to additionally conceal mystery data [24].

Watermarking is characterized as a procedure of implanting data like proprietor name, organization logo and so on in the host information. Advanced watermarking implants a flag into the first component with the end goal that the flag exceptionally recognizes the proprietor. Watermarking has turned into the key strategy for securing computerized components, for example, picture, sound and video [25]. The center thought of fingerprinting is that every client gets a duplicate of the article being referred to, containing a remarkable stamping [26].

We differentiate watermarking in a way that it protects against the uncertified imitation of the contents unlike cryptography.

II. LITERATURE SURVEY

In this paper, I have inspected different systems of picture steganography. The subtleties of some prominent methods are given in the following segments. Table I demonstrates the diverse systems with their highlights, points of interest and disservices.

Table I

Authors	Year of Publication	Major Contributions	Algorithms/Model Used	Pros and Cons
M. Tahghighi and H. Ghorbani [27]	2018	High security hybrid approach, The goal is to increase the PSNR value by considering the high embedding capacity	Symmetric Cryptography Algorithm and Imperialist Competitive Algorithm	High quality, high security image, more secure than other methods Embedding capacity is only 25 %.
Kamaldeep Joshi et. al [28]	2017	Proposed method blends the advantage of 2 bit LSB and XOR operation	Uses XOR operation	High imperceptibility and high message capacity
Ratul Chowdhury et al. [29]	2016	Cryptography and steganography are combined to perform a powerful encryption	Dual encryption methodology	Powerful encryption, cost of enhanced data security

B. Jindal and A. P. Singh [30]	2015	Pixel adjustment process to improve the visual perception of stego images	Multilayer security model	Provides high robustness to the attacks on the stego image.
Rashi Singh et al. [31]	2014	Message information is scattered randomly over the second last bit of the cover image pixels	7^{th} bit of pixel is used.	Extraction of original message difficult.
Hina Anand et al. [32]	2013	Image is divided into non-overlapping blocks of 16*16 so as to embed secret information	Modified Discrete Cosine Transform	Better method validated by MSE and PSNR.
Jose and Abraham [33]	2013	Image encrypation Chaotic sequence	Image encrypation Chaotic sequence	High embedding capacity
Das. Et. al [34]	2012	LSB:- 32bit secret key Blind extraction ASCII hvs	32bit secret key is used	Efficient Method & embedded information is completely invisible
Mare et. al [35]	2012	Stronger steganographic model, size of jump table for extraction reduces	LSB:-RGB images Payload Adaption	Jump table cannot be stored in noisy areas
Yadav et. al [36]	2011	Pixel is divided into two parts & their difference is used for insertion & retrieval	SPD method	Change in image quality is less. Not immune to noise and compression
Yadav et.al [37]	2011	Image is divided into equal size blocks and message is inserted into central pixel of the selected block using cyclic combination of last three bits	Cyclic combination method	Uniform distribution of message & chances of message insertion are 100%
Yadav et. al [38]	2010	Parity of pixel bits are used for message insertion & retrieval	PC method	Easy to implement. Not immune to noise & compression
Yadav et. al [39]	2010	6th,7th & 8th bit are used for message insertion	Bit Plane method	Chances are message insertion are 85.49%
Bhattaacharyya & Sanyal [40]	2009	Independent of the nature of the data Produces a stego image with minimum degradation	Eight neighbourhood of each selected pixel are used for insertion.	Less Embedding Capacity
Chan & Chan et. al [41]	2004	Optimal pixel adjustment process is used	Optimal pixel adjustment	Less Worst Mean Square Error

			process is used	
Potdar, & Chang [42]	2004	Gray level value of pixel is used	Gray level value of pixel is used	Chances of insertion of data are optimal. Easy to implement.
Wu & Tsai [43]	2003	Pixel value difference is used	Pixel value difference is used	High hiding capacity & outstanding
Chang et. al [44]	2002	Uses dynamic programming strategy	Uses dynamic programming strategy	Reduced computational time
Chan & Chang [45]	2001	Uses Moderate significant bits	Uses Moderate significant bits	Improve sensitivity to modification
Neil F. Johnson & Sushil Jajodia [46]	1998	Spatial Domain Technique Uses LSB of pixel	Spatial Domain Technique Uses LSB of pixel	Simple to implement 100% chances of insertion.

III. Parameters of Steganography

There are many parameters that affect steganography techniques. These parameters include concealing limit, perceptual straightforwardness, robustness, capability [25, 26].

- **Concealing Limit**

Concealing limit is the extent of data that can be concealed in respect to the span of the proprietor. A bigger concealing limit permits the utilization of a littler spread for a message of fixed size and in this way diminishes the transfer speed required to transmit the stego-picture.

- **Perceptual Straightforwardness**

The demonstration of concealing the message in the spread requires some noise modulation or twisting of the cover picture. It is critical that the insertion happen without noteworthy debasement or loss of perceptual nature of the cover.

- **Robustness**

Robustness refers to the ability of embedded data to remain intact if the stego-image undergoes transformations, such as linear and non-linear filtering, addition of random noise, sharpening or blurring, scaling and rotations, cropping or decimation.

- **Tamper Resistance**

Beyond robustness to destruction, tamper – resistance refers to the difficulty for an aggressor to change or manufacture a message once it has been implanted in a stego picture, such as a pirate replacing a copyright mark with one claiming legal ownership. In a copyright assurance application, accomplishing great tamper resistance can be difficult because a copyright is effective for many years and a watermark must remain resistant to tampering even when a pirate attempts to modify it using computing technology decades in the future.

IV. Popular Techniques of Image Steganography

A. A new combined method with high security for digital images steganography based on imperialist competitive algorithm and symmetric encryption algorithm [27]

In this paper, a high-security hybrid approach is proposed to digital images steganography based on the Imperialist Competitive Algorithm and Symmetric Cryptography Algorithm. The proposed technique, by thinking about the Imperialist Competitive Algorithm, makes a top notch, high-security picture. Before information addition, symmetric encryption of data happens, and afterward encoded data is inserted in the spread picture. The consequences of the usage of the proposed technique demonstrate that notwithstanding upgrading the picture nature of the steganography, it is more secure than different strategies.

B. An Enhanced Method for Data Hiding using 2-Bit XOR in Image Steganography [28]

In this paper, another procedure is anticipated whose aim is to keep secrete communication intact. The proposed strategy mixes the benefit of 2 bit LSB and XOR task. In this, first we are XORing the 8th, 1st bit of data and 7th, 2nd bit of data after this two bit are obtained. These obtained bits are replaced at the LSB position. However, with some way, any person get know about hidden message and it takes the LSB position bit then there are no chances of getting message as it is not the actual message. An examination was performed with various dataset of pictures. Besides, it was seen that the proposed strategy guarantees great outcome as the PSNR and MSE are great. At the point when the strategy was contrasted and other existing techniques, it indicates improvement in the imperceptibility and message limit.

C. A View on LSB Based Audio Steganography [29]

In this paper the idea of cryptography and steganography are joined to play out a ground-breaking encryption. Here we propose a novel methodology where a double encryption procedure has been executed. In the first level of encryption a pattern matching algorithm has been employed to encrypt the text message in terms of their positional value. In second level, the conventional LSB method has been used to embed the positional value in the cover file. Such a duel encryption technique will guarantee information security in an effective way. Finally the performance of the proposed method is evaluated in terms of means square error (MSE) and signal to noise ratio (SNR). An examination has been completed with ordinary LSB strategy. The trial results and the examinations showed that our calculation is exceedingly proficient as far as encryption and the limit size of the content.

D. Parity Checker Method [38]

In our method, we used the concept of even and odd parity by using the parity checker. As we already know that even parity means that the pixel value contains even number of 1's and odd parity means that the pixel value contains odd number of 1's. We inserted 0 at a pixel value where pixel value had odd parity and if odd parity is not present over there than we made the odd parity by adding or subtracting 1to the pixel value. Similarly, we inserted 1 at a pixel value if it had even parity. In case, if even parity is not present at that location then we made even parity over that location by adding or subtracting 1. In this way we can insert 0 or 1 at any location.

E. Hiding Data in 6th, 7th and 8th Bit of Pixel Values [39]

In this paper, an insertion method is obtained which increases the chance of insertion at first instance to 85.93% and includes all advantages offered in [7]. In this technique sixth, seventh and eighth bits of the picture pixels are utilized to conceal the message. Since this method involves 8th bit for concealing the message, intruder can easily change

eighth bit of all image pixels and this may result in the loss of message. To avoid this, time factor has been introduced, i.e. at some time t1, sender sends the cover object with message and at some other time t2 sender sends the cover object without message. Sender and recipient agree on this time factor initially before starting any communication. The advantage of introducing time factor (slot) is that if least significant bits of all pixels are changed by the intruder even then the message can be retrieved by comparing the two cover objects, i.e. one containing the message and the other not containing the message.

V. Conclusion and Future Scope

In this paper, I reviewed some existing techniques of the image steganography. I have reviewed various existing techniques like Parity Checker Method; 6^{th}, 7^{th} & 8^{th} bit method, LSB based audio steganography, enhanced data hiding method using 2-bit XOR. Every research leaves some space for some improvement. So, in future I will try to develop some new techniques which provide us robustness and highly embedding capacity and remove the disadvantages associated with the existing techniques.

REFERENCES

1. Kamaldeep Joshi et al., "An Enhanced Method for Data Hiding using 2-Bit XOR in Image Steganography", International Journal of Engineering and Technology, Vol. 8, No. 6, Jan 2017.
2. Abhilash G, Sudhakar KN, Mungara J (2012) Advanced symmetric keycryptography using extended MSA method: BLZ symmetric key algorithm. Int J Comput Sci Eng Technol 2(7):1321–1326.
3. Amirtharajan R, Rayappan JBB (2012) An intelligent chaotic embedding approach to enhance stego-image quality. Inf Sci 193:115–124.
4. Balkrishan S AP (2013) Enhanced bandwidth utilization in image steganography with enhanced data security. Int J Comput Appl 84(11):31–38.
5. Balkrishan, Singh AP (2011) Moderate bit insertion for hiding crypto data in digital image for steganography. IJCA, Special issues on IP Multimedia Communications 136–138.
6. Bender W, Gruhl D, Morimoto N, Lu A (1996) Techniques for data hiding. IBM Syst J 35(3 & 4):313–336.
7. Chan CK, Cheng LM (2004) Hiding data in images by simple LSB substitution. Pattern Recogn 37(3):469– 474.
8. Chang CC, Hsiao JY, Chan CS (2003) Finding optimal lsb substitution in image hiding by dynamic programming strategy. Pattern Recogn 36(7):1583–1595.
9. Chang CC, Lin MH, Hu YC (2002) A fast and secure image hiding scheme based on LSB substitution. Int J Pattern Recognit Artif Intell 16(4):399–416.
10. Cheddad A, Condell J, Curran K, Kevitts PM (2010) Digital image steganography: surveyand analysis of current methods. Signal Process 90(3):727–52.
11. Cheddad A, Condell J, Curran K, McKevitt P (2010) A hash-based image encryption algorithm. Opt Commun 283(6):879–893.
12. Forouzan BA (2008) Cryptography and network security. Publisher McGraw-Hill Higher Education, India.
13. Guha S, Das T, Ghosh S, Nath J, Das S, Nath A (2012) A new data hiding algorithm withencrypted secret message using TTJSA symmetric key crypto system. J Global Res Comput Sci 3(4):11–16.
14. Jindal B, Singh AP (2013) Camouflaging in digital image for secure communication. J IE(I)-Springer Electric Electron Telecommun Comput Eng 94(2):85–92.
15. Jindal B, Singh AP (2014) Image steganography with multilayer security using moderate bit substitution. J Appl Sci 14(8):738–747.
16. Pol K (2014) Image steganography based on DWTusing Huffman LWZEncoding. Int J Eng Tech Res 2(3): 100–103.
17. Potdar V M, Chang E (2004) Grey level modification steganography for secret communication. In Proceedings of IEEE 2nd International Conference on Industrial Informatics INDIN 04, Berlin, Germany 223 – 228.
18. Satir E, Isik H (2012) A compression-based text steganography method. J Syst Softw 85(10):2385–2394.
19. Satir E, Isik H (2014) A Huffman compression based text Steganography method. Multimed Tools Appli 70(3):1–26.

20. Usha S, Kumar GAS, Boopathybagan K (2011) A secure triple level encryption method using cryptography and steganography. In Proceeding of IEEE International Conference on Computer Science and Network Technology (ICCSNT), Harbin, 24–26 Dec. vol. 2, 1017–1020.
21. Usman K, Juzoji H, Nakajima I, Soegidjoko S, Ramdhani M, Hori T, Igi S(2007) Medical image encryption based on pixel arrangement and random permutation for transmission security. In Proceeding of 9th IEEE International Conferenceone-Health Networking, Application and Services, Taipei, Taiwan.19–22Jun.244–247.
22. Wang RZ, Lin CF, Lin JC (2001) Image hiding by optimal lsb substitution and genetic algorithm. Pattern Recogn 34(3):671–683.
23. Wu DC, Tsai WH (2003) A steganographic method for images by pixel-value differencing. Pattern Recogn Lett 24(9–10):1613–1626.
24. N. F. Johnson et al., "Information Hiding : Steganography and Watermarking – Attacks and Countermeasures", Advances in Information Security, Vol. 1, Feb 2001.
25. S. K. Pal et al., "Image Steganography for wireless networks using the handmaid transform", International Conference on Signal Processing & Communications (SPCOM).
26. M. Tahghighi and H. Ghorbani, "A New Combined Method With High Security For Digital Images Steganography Based On Imperialist Competitive Algorithm And Symmetric Encryption Algorithm", International Journal of Research in Computer Applications and Robotics, Vol. 6, Issue 1, pp. 1-12, Jan 2018.
27. Kamaldeep Joshi et al., "An Enhanced Method for Data Hiding using 2-Bit XOR in Image Steganography", International Journal of Engineering and Technology, Vol. 8, No. 6, Jan 2017.
28. Ratul Chowdhury et al., "A View on LSB Based Audio Steganography", International Journal of Security and its Applications, Vol. 10, No. 2, pp. 51-62, Mar 2016.
29. B. Jindal and A. P. Singh, "Concealing data in a digital image with multilayer security", Multimedia Tools Applications, © Springer Science, New York 2015
30. Rashi Singh et al., "Data Hiding At 7th Bit (RGB) With Cryptography", International Journal of Computer Science and Mobile Computing, Vol. 3, Issue 5, pp. 1041-1045, May 2014.
31. Hina Anand et al., "Implementation of 16*16 Quantization Table Steganography on Gray Scale Images", International Journal of Science and Research, Vol. 2, Issue 7, July 2013.
32. Jose, R. and Abraham, G. (2013), "A separable reversible data hiding in encrypted image with improved performance", Emerging research areas and 2013 international conference on microelectronics, communications and renewable energy (AICERA, ICMiCR), Annual international conference on 4-6 June, 2013, page(s): 1-5.
33. Das, S., Bandopadhyay, P. and Banerjee, M. (2012), "A secured key based digital text passing system through color image pixels", Advances in engineering, science and management (ICAESM), International conference on 30-31 March, 2012, page(s):320-325.
34. Mare, S.F., Vladutiu, M. and Prodan, L. (2012), "High capacity steganographic algorithm based on payload adaptation and optimization", Applied computational intelligence and informatics (SACI), 7th IEEE international symposium on 24-26 May, 2012, page(s): 87-92.
35. Yadav, R., Chawla, G. and Saini, R. (2011), "Semi pixel difference method for digital image watermarking with minimum degradation in image quality", International Journal of Computer Technology & its applications, Vol. 2, Issue 5, pp. 1297-1314.
36. Yadav, R., Saini, R. and Kamaldeep (2011), "Cyclic combination method for digital image steganography with uniform distribution of message", Advance Computing: An International Journal (ACIJ), Vol. 2, No. 6.
37. Yadav, R., Rishi, R. and Batra, S. (2010), "A new steganography method for gray level images using parity checker", International Journal of Computer Applications (0975-8887), Vol. 11.
38. Batra, S., Rishi, R. and Yadav, R. (2010), "Insertion of message in 6th, 7th & 8th bit of pixel values and retrieval in case intruder changes the least significant bit of image pixels", International Journal of Security and its Applications, Vol. 4, Issue 3.
39. Souvik Bhattacharya and Gautam Sanyal (2009), "Hiding data in images using PCP", World Academy of Science, Engineering and Technology.
40. C.K. Chan and L.M. Cheng (2004), "Hiding data in images by simple LSB substitution", Pattern Recognition, Vol. 37, Issue3, pp. 469-474.
41. Potdar, V. and Chang, E. (2004), "Gray Level Modification Steganography for Secret Communication", IEEE International Conference on Industrial Informatics, Berlin, Germany.
42. D.C. Wu and W.H. Tsai (2003), "A steganographic method for images by pixel value differencing", Pattern Recognization Letters, Vol. 24, pp 1613-1626.
43. C. C. Chang, J. Y. Hsiao and C.S. Chan (2003), "Finding optimal least significant bit substitution in image hiding by dynamic programming strategy", Pattern Recognization, Vol. 36, Issue 7, pp. 1583-1595.

44. R. Z. Wang, C. F. Lin and J.C. Lin (2001), "Image hiding by optimal LSB substitution and genetic algorithm", Pattern Recognization, Vol. 34, pp. 671-683.
45. Neil F Johnson, Sushil Jajodia (1998), "Exploring Steganography: Seeing the unseen", IEEE Computer, pp 26-34.