Survey of Hiding the Information Message Through Image Steganography Techniques

[1]Apeksha,[2] Nitin Choudhary

·Research Scholar[1],· Head Computer Scinece & engg[2]

[12]KIST College, Bhopal

Abstract — As the unimaginable development of network technologies will increase the communication of knowledge over the channel needs way higher than the bottom level of security. Image steganography is a common technique of concealment info into cowl image by exploitation digital suggests that by applying Least Significant Bit technique stego-image quality may be considerably increased with none overhead and complexness. Previous Steganography algorithms principally focuses on such embedding policy wherever less pre-processing is applied i.e. secrete image secret writing. This paper is essentially uses the DES (encoding algorithmic program with S box mapping that strengthen secret key. The secret image preprocessing is completed by steganography algorithmic program that uses two distinct S- Boxes. This preprocessing of secret image offers the algorithm strength no one will extract the data exclusive of knowing the mapping rules and function's secret key. To get high security, steganography methodology is is combining with a science secret writing decipherment in order that although anyone discover the existence of secret information, it's still not comprehendible. This paper surveys several such algorithms and conjointly will the comparative study of all the techniques along as a section of literature survey.

Keywords: Steganography, Cryptography, DES,LSB Technique, S-Box.

I. INTRODUCTION

Cryptography is a system to jumble up information using a secret key and this jumbling should be in manner that that no one can understand what was the actual message with no knowledge of key value .The word 'cryptography' was coined by combining two greek word 'kryptos' meaning hidden and 'graphene' meaning writting. such as privacy, integrity of data and entity. Data integrity means how to maintain the accurancy and consistency of data by using hash function or critical subsystems. There should be some uniqueness in cryptographic algorithm to increase the intensity of security, performance of algorithm, and ease of implementation. Security Level expressed by a higher level of work is necessary to defeat the objective. Ease of implementation means the difficulty of realizing the algorithm through practical implementation. There are numerous appearance of security. They are security service, attack on security and mechanism for security. Security examines an overhaul that increases the processing system of data security and data transfers of any association. Security mechanism means that are designed to detect, prevent, or pull through from a security attacks. Any accomplishment that affects the security of information hold by an association is called Security attack..

Encryption: Encryption uses a systematic or step-by-step procedure called an algorithm to convert data or the text (Plain Text) of an original message into cipher text. This is a encrypted form of data. A key that is a string of characters, normally require by a Cryptographic algorithms to encrypt or decrypt data. Those who possess the key and the algorithm can encrypt the plaintext into cipher text and then decrypt the cipher text reverse into plaintext.

Two types of encryption are there: Symmetric & Asymmetric.

In symmetric encryption also known as the Private Key Method, a solo key is applied for encryption and decryption of data. Symmetric encryption is said to be fast type of encryption, but it has a serious problem. The inherent weak point of this method is mostly the requirement of a key exchange between communications partners.

In Asymmetric encryption also known as the Public Key Method, it uses two different keys: the private key and public key. The public key is distributed freely and the private key is known only to the owner of a key. The two keys have a (mathematical) relationship. However, for obvious reasons, calculation of a private key on the basis of the public key must be impossible or at least not feasible.

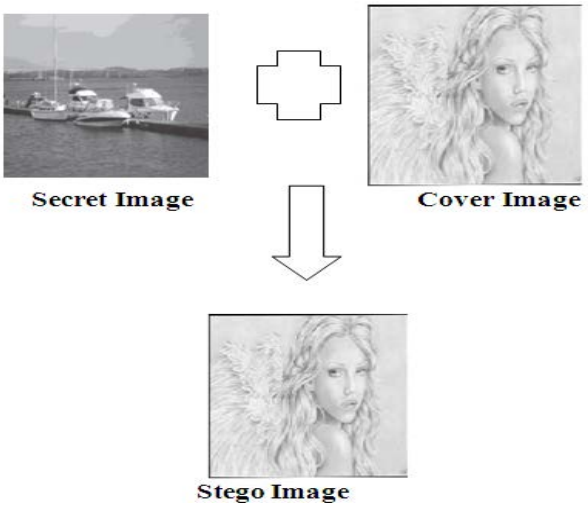

Figure 1.1: The Block Diagram of Steganographic system

Stegnography: This word is originated from Greek and is used for hiding something behind images or any other text

and basically it means "to hide in plain vision. Steganography is the ability of discreetly veiling data within other data. When this concept of steganography is combined with cryptography it carried the security to a high level of security.

Steganography Types :

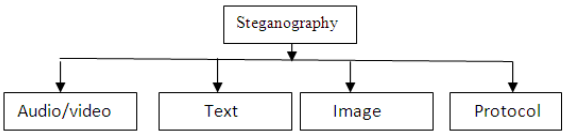

Figure 1.2: Steganography Types

Audio/Video Steganography

In Audio/Video steganography, a information message is hide inside the audio/video file. The binary sequence of audio/video file is slightly differ from original file which cannot be easily be detected by human eyes [8]. Least Significant Bit is most commonly used in this category.

Text Steganography:

Text Steganography means Concealing information inside the text file. It is in olden times the most imperative type of steganography. In this type of steganography, secret message is masked in a text. There many techniques are used such sequencing in which each character of information message is masked a fix position of text or information message binary value is hidden in binary value of text.

Image Steganography:

Image is a set of bytes holding different intensities of light in different area of the image. The technique which is applied to conceal secret message contained by an image is called image steganography.

Protocol Steganography:

The name protocol steganography specify to the method of implanting information inside any messages and in network transmission network control protocols are used. OSI network model layer used this type of Steganography.

The other section of paper is arranged as follows. Section II defines the associated systems and Literature evaluation on existing Steganography methods. The Section III describes the methodology used to meet the research objectives in terms of proposed concept.

The Section IV states various assumptions taken, data & algorithms used to develop the application and also provide a view of working environment in which application will run. The conclusion and future scope of the paper is shown in Section V.

II. LITERATURE SURVEY

Authors have done many research and found variety of techniques to hide the secret message many after the process of encryption. Many of them use the technique to hide message contained by any text or document file or even sound file whereas others use image files.

In recent scenario the works on steganography systems to cover their objects using images is gaining popularity. My work is also trying to conceal the secret data behind the cover image without leaving any sort of mark.

Shashikala Channalli et al. (2009) have proposed a novel form of steganography in which information has made hidden on-line on the output screens of the instrument. This method has mainly used in order to announce a secret message in the unrestricted place. It has been also extended to some another means such as electronic advertising board around the stadium, railway station or the airport. This steganography technique is extremely almost similar to the video and image steganography. for secret information hiding symmetric key steganography is used by both Private marking system and LSB technique.

This paper represents a unique scheme in which it can transmit lots of secret information in addition to provide a secured communication between two communicating parties. Both cryptography including steganography can be entwined into this scheme in order to make the detection more difficult. Text data are of several kinds and it can be employed as secret msg. The secret message that uses the concept of steganography is sent over the network [1].

Fadhil Salman et. al. (2010) produce the idea of hiding text in an image file by using the combined concept of steganography and cryptography. In their proposed system they used the method of DCT Quantization through steganography process. The two levels of security technique used by the author: the RSA algorithm and the digital signature. Finally the image is stored in a JPEG format. In this case, the information message seems like plaintext with digital signature while the colored image is a cover file. The proposed system can be distinct as asymmetric key Steganography. Their implementation results prove that their algorithm is faster in extracting the information message [2].

Nath, Asoke, et.al (2010) in their current work they had embedded sound file in an image file ,any text , word, excel file or within a pdf file. The main constraint is that the size of cover file essentially be at least 10-20 times larger than the embedded file. In the present paper they had applied (i) changing LSB, (ii) changing LSB+1 bit, (iii) changing LSB+3 bit for inserting secret message inside a cover file. We have also supposed the password for in receipt of into the secret file. If the password found not correct then we will not be able to extract message from the cover file [3].

Nath, et.al (2011) showed that the existing work the journalists had introduced a new technique with the purpose of cover any encrypted clandestine message contained by a cover file. To encrypt the secret message the researchers have used a novel algorithm which was projected by Nath et. al. (1). For plain text file encryption and cipher text file decryption the matrix of randomized key have generated by authors using method of randomization [4].

Das, Debanjan (2011)In the existing work the researchers had introduced a technique based on an integrated symmetric key cryptographic named DJMNA which has used to combine two independent approaches (i)MGVC :Modified Generalized Vernam Cipher (ii) DJSA technique which is mainly the extension of MSA technique. The algorithm Generalized Vernam Cipher has generally extended the encryption of any type of text or data. Tis work is done by using all characters ASCII code (0-255). This adapted form of Generalized Vernam Cipher mainly used threw “feedback” effect as well as reverses the file while encryption [5].

Abed, Fadhil Salman (2012) Author have introduced a new technique of hiding information which combines two previous techniques (i) RSA cryptosystem: for information encoding (ii) Fractal image compression method: for hiding the cipher information(cipher text) [6].

Niemiec, Marcin, and Lukasz Machowski (2012) In this paper authors have deliberate a exclusive algorithm that is based on symmetric cryptography called S boxes . The cipher text confirms a high-level of confidentiality due to the S-boxes which is key-dependent. These S boxes were key dependent and ensure high level confidentiality. This technique was based on the Rijndael S-box which has used in the AES algorithm. The method is as general as and it can be planted on any S-box [7].

Mathur Akanksha(2012) has written a paper which mainly present an algorithm for both encryption as well as decryption data . This method was based on ASCII codes in the plaintext. This algorithm had mainly used for encryption the text or data by using ASCII codes of the data which is to be encrypted. The secret key is used to modify the contents of another string and then the modified string is became a key to encrypt or decrypt the data. Therefore, it can be said that it was a symmetric encryption algorithm because it has used the single key cryptography (encryption / decryption) by slightly altering it. This algorithm drives only then when the input text length and key length would be the same [8].

Dey, Somdip(2012) In this article the researchers has presented an innovative cryptographic technique named SD-AREE which was used to rule out terms that are monotonous, in the message, when it has to be encrypted, so that it can develops an impossible way that nobody can even predict the original message from the encrypted message. In modern era, the cryptography hackers usually try to break a cryptographic algorithm or they may try to retrieve the key. This key is needed in order to encrypt a message (data), by examining the insertion or presence of dreary bits / characters (bytes) in the message as well as the encrypted message in order to find out the encryption algorithm or the key which has been used for it. Therefore it must be a good encryption method in order to reject the tedious terms such that there should be no trace of repetitions can be traced. That is why, they have applied SD-AREE cryptographic method in order to reject the repetitive terms from the message, which had to be well encrypted. It is a adapted Caesar Cipher Technique along with progressive bit-manipulation cryptographic technique [9].

Rishav , Jeeyan , Debanjan (2012) designed a innovative method in which they hide their secret message in a cover file a nd cover file may be any text file , Microsoft word file or any black and white space character file any for hiding. Firstly the secret message has been encrypted by using a modified Widespread Vernam Cipher Method (MGVCM) which was proposed by Nath et**.** al**.** in order to hiding the secret message which exists inside any ASCII file, they had proposed a different technique in which the bits of each character of secret message file had been inserted on behalf of eight randomly selected blank space characters of the given cover file [10].

Xing Tang et al (2013) present a promising algorithm for information hiding in Word document, which by changing the RGB values of character and underline. For the time being, A new system called text information hiding system based on RGB is implemented. The structure, mechanism and process of the system are described in detail. The comparisons of investigational results exhibits that the algorithm has an outstanding performance in visual. Furthermore, the system expands the capacity of hidden and get betters results in the imperceptibility of carrier document [11].

Juneja, Mamta, and Parvinder S. Sandhu (2013) the paper proposed a new technique for information security. It invented an algorithm called enhanced steganography algorithm. In this algorithm a information message is first embedded then embedded message bit is set into the LSBs of nonadjacent and random pixel locations in edges of images. No original cover image is required for the extraction of the secret message. Author developed this method for the purpose of implementing a new enhanced data hiding method based on LSB .The principal point of this paper is to propose a solution that is robust, effective and to make it very hard for human eye to predict and detect the existence of any surreptitious information inside the host image. This has been achieved by using those bits for data storage that are on edges and using blue component of color image to which human eye is least perceptive. The proposed solution has not only achieved what was required

but has also increased the data hiding capacity of the host image by utilizing all the pixels [12].

Devi, Kshetrimayum Jenita(2013) In this paper author developed an algorithm of an image based steganography that is a combination of Least Signicant Bits (LSB) techniques and pseudo random encoding technique . In the LSB approach, the bits of LSBs of cover image is replaced by the message file bits in this manner that cover image property remain same. But this method is somewhat difficult because it is very challenging to differentiate between both the images. The LSB-based technique is the most interesting one because it is very difficult to differentiate between the cover-object and stego-object in that situation in which few LSB bits of the cover object are exchanged. In Pseudo-Random technique, a random-key is mainly used as the pit for the Pseudo-Random Number Generator is needed in the embedding process. Both the methods generally used a stego-key while embedded messages inside the cover image. A stego-key is used by both the techniques while message is embedding within the cover image. By using the key, the chance of getting attacked by the attacker is reduced [13].

Ramaiya and Manoj et al. (2013)presents a exclusive technique for Image steganography. This technique is based on the three important method (i)Data Encryption Standard (DES) (ii)strength of S- Box mapping (iii) Secrete key. For preprocessing of secrete image two unique S-boxes with embedded function steganography algorithmis used. By using this preprocessing method no one can extract the information message without prior knowledge of mapping rules and secret key. Moreover the proposed scheme is not only able to shuffle data but it also changes the pixel intensity value which increases safety of algorithm [14].

Paul, Manas, and Jyotsna Kumar Mandal(2013) In this paper, Author design an algorithm named Spiral Matrix Based Bit Orientation Technique (SMBBOT). This algorithm works as follows (i) convert input plain text into binary bit stream. (ii) In encryption process encryption binary input stream is cut like that it could be converted into variable size blocks. These blocks of bits are taken from MSB to LSB so as to fit into a square matrix of an appropriate order following the concept of Spiral matrix. The square matrix usually splits into 2x2 sub-matrices. Bits are generally taken column-wise from all 2x2 sub-matrices in order to construct the encrypted binary string. Cipher text is mainly generated from the encrypted binary string. The arrangement of the values of block length and the number of blocks of a particular session which mainly generates the session key especially for SMBBOT. For decryption algorithm a cipher text may be considered as the binary bit string. Handling the session key information what happens that the binary string is broke down in the predefined blocks. These Bits blocks are then taken from MSB to LSB in order to fit column-wise into 2x2 square matrices. Using the respective sub-matrices a single square matrix with suitable order is formed. The decrypted binary string is made after fetching the bits from square matrix which is following the reverse concept of Spiral Matrix. The plain text is then regenerated from the decrypted binary string. A comparative analysis of SMBBOT with the existing as well as industrially accepted TDES and AES has been prepared] [15].

III. COMPARARTIVE STUDY

In most of the research work, the authors have tried to implant some secret message within any cover file in an encrypted form so that no one will be able to pull out the actual secret message. Some standard steganographic method uses the DCT method , S box method and some uses LSB method used in the cover file. Here, I have experimentally evaluated image steaganography using DES Algorithm and taken this as a base algorithm for my future works.

3.1 Evaluation method and experimental result of image steganography using DES Algorithm

Encryption plays an important part in information security. Therefore, it is necessary to evaluate the performance of encryption and decryption algorithms. The evaluation is doneon PSNR . I analyzed the image steaganography using DES Algorithm (2012)on PNSR Value . In this section, I analyzed the experimental results of image steaganography using DES Algorithm (2012)

IV. RESULT ANALYSIS

The aim is to hiding of a secret image into a cover image so that the cover image and the stego image are almost the same with sparse and undetectable difference to the observer.

Image Steganography using DES (2012) Steganography technique because without knowing the secrete keys, S-box mapping function, the extraction of secrete image from the stego image is impossible. Moreover quality of cover image is also not degrading due to variation in one LSB of each pixel which reflects only 0 – 1 difference pixel value. Additionally the proposed scheme is capable of not just scrambling data but it also changes the intensity of the pixels which contributes to the safety of the encryption.

A. Peak Signal to Noise Ratio (PSNR):

The measurement of the quality between the cover image f and stego-image g of sizes N x N (for 8 bit gray level) is defined by PSNR as:

$$PSNR = 10 \times \log (2552 / MSE)$$

$$\text{Where MSE} = \sum_{N=0}^{N-1} \sum_{N=0}^{N-1} (f(x,y)g(x,y))^2/N^2$$

Where f(x,y) and g(x,y) signify the value of pixel at the position (x, y) in the respective cover-image as well as the stego-image respectively. The unit PSNR is dB. PSNR is representative of the quality of image i.e. the higher the PSNR, lower in the variation between cover image as well as stego image and vice – versa.

TABLE 1: CAPACITY & PSNR

Name of the image	Size(in pixels)	Capacity	Existing algorithm
Rima	64*64	25%	60.511
Jose	64*64	25%	57.812
flower	64*64	25%	58.42
flylib	64*64	25%	54.726
Tulips	64*64	25%	51.644
Koala	64*64	25%	51.611

Figure and graphs shows the result analysis on multiple images

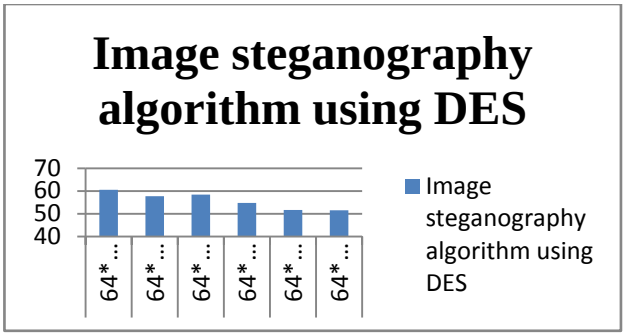

Figure 4.2: Graph of Image steganography using DES results on images

IV.CONCLUSION

In image steganographic algorithm based on DES (2012) author use the strong point of S-box mapping then use a secret key for secret image encryption it improves security as well quality image quality compare to existing algorithms. Steganography, particularly combined with the cryptography could be a powerful tool that permits to communicate secretly Because the speedy development in digital technology and net, steganography have progress lots over past years.All of the given ways of steganography showed their work on embedding strategy and provides no thought to the preprocessing stages, like cryptography of secrete image, as they rely heavily on the standard cryptography algorithms that clearly aren't tailored to steganography applications wherever flexibility, strength and security area unit needed. The analysis stimulates that the steganographic capability and stego image physical property area unit the foremost vital aspects of image steganographic systems. Primarily, either increasing the steganographic capability whereas maintaining the physical property (stego image quality) or enhancing the physical property whereas maintaining the steganographic capability represents a major contribution.

V. FUTURE WORK

Now a day, image steganography is broadly used in steganography field. So there is much of work to do and algorithm Time Complexity can be reduced. We can use efficient Stegnography algorithm with other cryptographic algorithms and steganographic algorithms which can decrease the space and time complexity and augment the level of security.

REFERENCES

[1] Thorsten Holz Frederic Raynal, “Detecting Honeypots and other suspicious environments,” in Proceedings of IEEE Workshop on Information Assurance and Security United States Military Academy, West Point, **NY** 2005.

[2] Abed, Fadhil Salman, and Nada Abdul Aziz Mustafa. "A Proposed Technique for Information Hiding Based on DCT." Int. J. Adv. Comp. Techn. 2.5 (2010): 140-152.

[3] Nath, Asoke, Sankar Das, and Amlan Chakrabarti. "Data Hiding and Retrieval." Computational Intelligence and Communication Networks (CICN), 2010 International Conference on. IEEE, 2010.

[4] Nath, Joyshree, and Asoke Nath. "Advanced Steganography Algorithm using encrypted secret message." International journal of advanced computer science and applications 2.3 (2011).

[5] Das, Debanjan, et al. "An integrated symmetric key cryptography algorithm using Generalised Modified Vernam Cipher method and DJSA method: DJMNA symmetric key algorithm." Information and Communication Technologies (WICT), 2011 World Congress on. IEEE, 2011.

[6] Abed, Fadhil Salman. "A Proposed Encoding and Hiding Text in an Image by using Fractal Image Compression." International Journal on Computer Science and Engineering (IJCSE) 4.01 (2012): 1-13.

[7] Niemiec, Marcin, and Lukasz Machowski. "A new symmetric block cipher based on key-dependent S-boxes." Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2012 4th International Congress on. IEEE, 2012.

[8] Mathur, Akanksha. "A Research paper: An ASCII value based data encryption algorithm and its comparison with other symmetric data encryption algorithms." International Journal on Computer Science and Engineering (IJCSE) 4.9 (2012): 1650-1657.

[9] Dey, Somdip. "SD-AREE: An Advanced Modified Caesar Cipher Method to Exclude Repetition from a Message." International Journal of Information and Network Security (IJINS) 1.2 (2012): 67-76.

[10] Ray, Rishav, et al. "A new Challenge of hiding any encrypted secret message inside any Text/ASCII file or in MS word file: RJDA Algorithm." Communication Systems and Network

Technologies (CSNT), 2012 International Conference on. IEEE, 2012.

[11] Tang, Xing, and Mingsong Chen. "Design and implementation of information hiding system based on RGB." Consumer Electronics, Communications and Networks (CECNet), 2013 3rd International Conference on. IEEE, 2013 of Standards and Technology, Gaithersburg, September 2011.

[12] Juneja, Mamta, and Parvinder S. Sandhu. "An Improved LSB Based Steganography Technique for RGB Color Images." International Journal of Computer and Communication Engineering 2.4 (2013).

[13] Devi, Kshetrimayum Jenita. “A Sesure Image Steganography Using LSB Technique and Pseudo Random Encoding Technique”. Diss. National Institute of Technology-Rourkela, 2013.

[14] Paul, Manas, and Jyotsna Kumar Mandal. "A Novel Symmetric Key Cryptographic Technique at Bit Level Based on Spiral Matrix Concept." arXiv preprint arXiv:1305.0807 (2013).

[15] Wenjie Lin, David Lee,” Traceback Attacks in Cloud—Pebbletrace Botnet”, 32nd International Conference on Distributed Computing Systems Workshops (ICDCSW), Macau 2012 ,june 18-21,pp 417- 426.

[16] Hisham A. Kholidy, Abdelkarim Erradi, Sherif Abdelwahed, Fabrizio Baiardi,”HA-CIDS: A Hierarchical and Autonomous IDS for Cloud Systems” In Fifth International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN), Madrid June 5-7Vol 2,pp. 179-184 , 2013.

[17] Ramaiya, Manoj Kumar, Naveen Hemrajani, and Anil Kishore Saxena. "Security improvisation in image steganography using DES." Advance Computing Conference (IACC), 2013 IEEE 3rd International. IEEE, 2013.

[18] Sheng-Wei Lee, Fang Yu,”Securing KVM-based Cloud Systems via Virtualization Introspection”, 47th Hawaii International Conference on System Science, Waikoloa, HI, Jan 6-9,pp 5028 – 5037, 2014.