INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

REVIEW PAPER ON IMAGE STEGANOGRAPHY

Deepali V. Patil[1], Mr. Shatendra Dubey[2]
[1]Dept. of Computer Science & Engg.., NRI Institute of Information Science & Tech. Bhopal- 462021, India
deepalipatil86@yahoo.co.in
[2]Dept. of Computer Science & Engg.., NRI Institute of Information Science & Tech. Bhopal- 462021, India

Abstract— In this paper we study different Steganography techniques for encrypting the information. Steganography is a technique which allows *secreting* information or data into the image. This paper discusses the concept at the back of Steganography by exploring firstly what is the Steganography and the terms that are associated the Steganography. This paper explores the Steganography methods – image Steganography, audio Steganography, video Steganography, text Steganography that are used to embed the information in digital carriers. The two most important aspects of image based Steganography system are the quality of stego image and the capacity of the cover image. By reviewing this paper, researchers can enlarge a better Steganography technique to increase the M*SE, BER* and PSNR value by analyzing the existing Steganalysis techniques.

Keyword: Steganography, image-audio-video-text Steganography, MSE, BER and PSNR

I. INTRODUCTION

Introduction about Network Security

Network security is the set of tools designed to protect data and to stop from hackers. Nowadays the word Network Security is somewhat deceptive, because virtually all business, government and academic organizations have their interconnected networks. Such a collection is pronounced as Internet and therefore it called as Internet Security.

Introduction about Steganography and cryptography

Since the start of internet, one of the most important factors of Information Technology and Communication has been the security of information, for that two techniques are used cryptography and steganography

Steganography

Steganography is not truly a method of encrypting message but hiding them within something else to enable them to pass unobserved. The word steganography comes from Greek word where “Steganos” means “Covered” and “Graphy” means “Writing “The innocent files can be referred to as cover text, cover image or cover audio as suitable. After embedding the secret message it is referred stego medium.

Cryptography

Cryptography encodes information in such way that nobody can read it, except the person who holds the key. Cryptography comes from Greek word where “Crypto” means “Secret” and “Graphy” means “Writing”.

Need of Steganography and Cryptography

Encryption allows secure communication and it requires a key to read the information. An attacker is not able to remove the encryption but it is easy to alter the file and making it unreadable for the intended recipient. Steganography allows protected communication It cannot be removed and it requires significantly altering the

data in which it is embedded. The embedded data will be private until an attacker is able to find a way to detect it.

II. LITERATURE SURVEY

Following are the different technique which can be used for secure communication:

At these days and age, digital communication has become a fundamental part of communications. A plenty of applications are Internet based and in a few cases it is preferred that the communication made secret. For that to achieve this goal cryptography and steganography are used. In this paper, a variety of digital steganographic techniques are implemented which are able to producing a secret-embedded image that is indistinguishable from the original image to the human eye. A comparative analysis is made to demonstrate the effectiveness of the proposed methods. The effectiveness of the proposed methods has been estimated by computing Mean square error (MSE) and Peak Signal to Noise Ratio (PSNR). [1]

For the past decade, many steganographic techniques for images have been presented both in spatial and frequency domain.

1) LSB Substitution Method:

When hiding the information within images Least Significant Bit (LSB) method is used. In this scheme 8^{th} bit of each byte of the carrier file is substituted by one bit of the secret information. This technique is very simple.

2) Optimum Pixel Adjustment Procedure:

The distortion caused by LSB substitution method is minimized by the Optimal Pixel Adjustment Procedure (OPAP). After hiding of the secret data, the pixel value is adjusted in OPAP method. Due to this the quality of the stego image is improved without disturbing the hidden data.

3) Inverted Pattern Approach (IP)

The idea of processing secret message has been used by IP approach prior to embedding. In this method, before it is embedded each section of secret images is determined to be inverted or not inverted. Additionally, the bits are used to record the transformation which may be treated as secret key or extra data to be re-embedded.

4) IP method Using Relative Entropy:

In this, the relative entropy is calculated instead of finding the mean square error for inverted pattern approach,

5) The proposed Hiding Streams of 1s and 0s

The usual steganographic method uses few bits from the secret data to be embedded. But this method uses alternatively the 1s or 0s present for hiding. This is a creative steganographic approach where the hidden data is converted to binary. In this method the occurrence of 1s and 0s are calculated and placed in the pixels of the cover image. The occurrence of 1s is placed in the odd columns of the pixel and the occurrence of 0s is placed in the even columns. Benefits of this method are: 1) Implementation is simple. 2) Embedding capacity is large 3) Smaller key size.

6) Pixels Value Differencing (PVD)

Instead of the high capacity of the concealed information, Pixel Value Differencing can provide a high quality stego image. Means, the number of insertion bits is not independent on whether the pixel has edge area or smooth area. The difference between the adjacent pixels is more in edge area and it is less in smooth area.

7) The proposed mod method:

By subtracting any remainder obtained from dividing with 10 the embedding is done.

Benefits:

1. Provides high embedding capacity.
2. The quality of the image is retain.
3. In the difference between the adjacent pixels, the data is hidden
4. Also there is the key without which extraction of data is not possible.

8) The proposed MOD10 based method

In this method the data is hidden in the remainder obtained by dividing the gray value of the pixel by 10. This method has a key which determines whether the data is same as the remainder or 10-remainder. The key improves the quality of the stego image.

9) DCT

To hide information in the images many techniques are used in that one is transform domain techniques is used. A transform domain technique, DCT is used to hide messages in significant areas of the cover image. In discrete cosine technique, pixels are split into 8×8 blocks. Then, all blocks are DCT transformed each block encodes just one secret message bit.

Benefits:

1. This method is more robust to attacks, such as compression, cropping etc.
2. The quality of image is good, but embedding capacity is low.

In Image Encryption method, the function of Least Significant Bit (LSB) technique is to hide the information in image. In this approach firstly information is encrypted and then encrypted information embeds in image at LSB position. After embedding, it measures the values of entropy and correlation of stego image and original image. If both the values are same then the method is a safe one. To execute this, various vertical and horizontal blocks will be developed at the sender side, and it mixed with the encrypted image before sending it to the receiver. After sorting the secret information from the encrypted image the secret transformation table is reconstructed by the receiver. In this process only secret information is transfer in spite of transferring whole secret transformation table. Further the LSB technique is overwrite by the hidden data of binary representation within the encrypted image data randomly. Before and after the insertion process the values of the correlation and entropy are likely to be the same. The benefit of this is to negating the chance of the encrypted image being found and then increase the security level of the encrypted image. [2]

A latest steganography method is projected for data hiding. Least Significant Bits (LSB) technique is used to hide data within encrypted image data in the method. The LSB technique is overwrite by the hidden data of binary representation within the encrypted image data randomly. Investigational results illustrate that the values of correlation and entropy before the incorporation are alike to the values of correlation and entropy after the incorporation. Since the both values have unchanged, the method gives a good suppression for data in the encrypted image, and minimizes the chance of the encrypted image being found. After sorting the secret information from the encrypted image the secret transformation table is reconstructed by the receiver and hence the inverse of the transformation and encryption processes can reproduce the original image. [2]

Security, capacity and imperceptibility are the three main things which are covered in this topic. Hybrid data hiding scheme is utilized which implements LSB techniques with key-permutation method. Also optimal key permutation method is planned using genetic algorithm for best key selection. Here based on LSB substitutions the system has been planned, where random key is obtained and circulated to the communicating parties. The secret data is entrenched in the k LSBs of the Host image, where the value of k is below 3. The value of k is limited to 3 so that it will not raise the all possible keys permutations. Measuring the PSNR for each substitution, and selecting the one which having the maximum PSNR value for each substitution is the suitable method to achieve the best optimal result. But it takes very time and is not practical. To overcome this genetic algorithm is employed where genetic algorithm is a randomized search process, so that it offers superior image quality and big message capacity as well as boost the system protection. In this topic the system security has been recovered while growing the number of keys along with less estimated time. [3]

In this paper, Discrete Wavelengths Transform (DWT) is used to embed the secret message in frequency domain through steganography method. Haar-DWT is the frequency domain transform. It includes horizontal and vertical operation. Initially the pixels are scanned from left to right in horizontal direction which make the plus and minus operations on nearest pixels and then accumulate the addition on the top and the subtraction on the bottom. The advantage of this technique is to diminish the extra data in the stego-image as well squeeze the size of key matrix as far as possible. [4]

In this paper, spread spectrum image steganography (SSIS) technology is shown which the part of latest digital steganography is. Here image renovation, error-control coding, and those similar to spread spectrum communication, are bring together within the SSIS structure and the behavior of the system is illustrated. Primary concept of this system is to embed the hidden information within noise along with addition to a digital cover image. This system may be extended to audio signals and color imagery. [5]

Spread-Spectrum Image Steganography (SSIS) is the science of communicating in a hidden manner. This new method is proposed here according to the discussion of steganographic communication theory which hides and then recovers messages of significant length within digital imagery as well as maintains the original

image size and dynamic range. The hidden messages can be improved using proper keys without any knowledge of the original image. This process embeds the message which can be in type of text, imagery, or any other digital signal. [5]

Here by means of Steganography method, new algorithm is generated to hide data inside image. Also the use of bitmap image is implemented to hide the data. Pixels are used to embed the data inside the image. There are two stages are. The first is to come up with a new Steganography algorithm in order to hide the data inside the image and the second stage is to come up with a decryption algorithm using data retrieving method in order to retrieve the hidden data that is hided within the stego -image. Benefit of this method is SIS maintains privacy and accuracy of the data. [6]

Binary codes and pixels are used inside an image to plan this algorithm. To exploit the storage of data, the zipped file is used inside the image before it is transform to binary codes, so that the steganography Imaging System (SIS) is built by using the projected algorithm. Then to check the feasibility of the planned algorithm, the testing is done. While testing the PSNR (Peak signal-to-noise ratio) is taken for each of the images and different sizes of data are also stored inside the images. So this new steganography algorithm is much capable to hide the data inside the image based on the PSNR value of each images as the stego image has a higher PSNR value. [6]

In this paper, an extremely capable steganography code of behavior is planned. It is supported by on hamming codes, the embedding and the retrieval algorithm having the similar computational rate. Product code of two hamming codes is used by this method to improve the embedding rate. [7]

Here the two dissimilar plans are investigated. Firstly design is done by using blind watermarking scheme. Secondly the design is done for steganography to achieve perfect security is achieved, it means the relative entropy among stego data and cover data leans to zero. Also here investigation of information is embedded in the circumstance of digital watermarking. Design of information embedding process is done for digital watermarking so that the embedded information will not be tearing down by consequent processing. That's why attractive digital watermarking technology is created for steganography. Also this system is beneficial because the performance of the schemes is compared relating to embedding distortion, rate and security.

Steganography is the skill of message communication by embedding it into multimedia data. It is preferred to exploit the quantity of hidden information (embedding rate) while defending security against recognition by illegal parties. Cachin has anticipated a proper information-theoretic steganography model. When the values of the stego data and cover data are equal then steganographic method is entirely safe, it means the relative entropy among stego data and cover data leans to zero. Also the stego data should appear as a "typical image" for image data. In this topic, a soundless communication channel is understood. The stego image has been stored in the popular JPEG format by these two dissimilar plans. [8]

The main purpose of this practice describes the steganographic method to reduce the visually plain and numerical dissimilarity among the cover data and stego-image while increasing the amount of the payload. Here gray scale image (I0) is considered having measurement M*N where M and N are rows and columns of intensity level. Message to be embedded is taken in account. ASCII codes are used in which every letter in the message is transformed. Henon map has been taken in account to generate schaotic sequence. By taking average value of these sequences as threshold value, they are transformed into binary. Every bit of the transformed message is XORed bit is once more XORed through the LSB of the pixel of the image selected as the cover image. The benefit of this algorithm is to give security and keeps confidentiality of the secret message. [9]

Ross J. Anderson and Fabien A.P. Petitcolas disagreed that each steganographic approach will have its restrictions; they projected information theoretic approach for ideal confidentiality. Here we simplify about steganography and its behavior. We compare it with the allied regulations of cryptography and traffic security, present a unified terminology consent at the first international workshop on the subject, and summarize a amount of approaches—several of them widen to cover encrypted copyright characters or consecutive numbers in digital audio or video. Then numbers of attacks are presented, some new, on such information hiding formats. This directs to a conversation of the terrifying barriers that lounge in the mode of a common theory of information hiding systems. Though, theoretical deliberations direct to suggestions of practical value, such as the use of similarity checks to intensify secrecy and offer public key steganography. Lastly we illustrate that

public key information hiding schemes be present, and are not essentially controlled to the case where the warden is inactive. [10]

An extremely diverse method of steganography is anticipated by Mohammed A.F. Al Husain. He considers the pixels of image to map with English letters and special characters. [11]

In this paper, Ran-Zan Wang and Yeh-shun Chen go with the two way block matching for image in image steganography. [12]

Writers in [13] correspond to a dual layered embedding process for executing plus minus steganography with binary covering codes and wet paper codes for hiding the messages in the LSB plane and second LSB plane correspondingly.

It is establish that the hidden unusual information amend the primary figures of natural images [14]. But the bytes delivering the image features and embed in the other bytes has not been touched then the difficulty can be work out. Author in [15] is planned a steganographic code of behaviour depend on hamming code.

In this topic by means of two square reverse chippers, a text steganography is planned. Two steps for encryption are explained here. Firstly, by means of algorithm, a first step cipher is obtained. Then it is separated into 2-2 characters after receiving the first step cipher. Further switching the 2-2 characters positions, final cipher is achieved. The cover image is separated into bytes. Here the plus point is to offer two level security-cryptography and steganography. This algorithm is much superior in terms of disturbance anticipation in comparison with LSB technique.

Here method for safe communication is shown by the authors by means of together cryptography and steganography technique. They considered the image to use steganography as the carrier. They have also encrypted the confidential information by their personal substitution cipher named two square reverse. Then the cipher text of the secret information is embedded into the carrier image. The selection of byte is made based upon the bit prototype of the secret information. That's why the embedded positions are reliant on the secret message, so the interloper having the complication to situate the bits. Furthermore the consequential image will be submitted to the receiver where the reverse operation is done by receiver as like as the sender to obtain the secret information. [16]

Now a day the internet has been broadly used worldwide. Occasionally, it is necessary to maintain the information undisclosed and protected without catching the interest of illegal person. In this paper, writer implemented Steganography technique as well cryptography technique for safe communication. They encrypt the undisclosed message by means of new cipher algorithm entitled twelve square substitution cipher algorithm and then the cipher text has been embedded in the carrier image in 6th and 7th bit locations or 7th and 8th bit locations or 6th and 8th bit locations having dissimilar pixels (bytes) of the carrier image based on index variable values. After this the receiver collect the resulting image and the cipher text from the assumed positions should be recovered by the receiver and then decrypt by using the twelve square cipher algorithms to acquire the secret message. It is a power pack approach because the embedding locations are different in all pixels [18]

III. RESEARCH SCOPE

Although LSB technique is simple, the disadvantage is it causes noticeable distortion when the number embedded bits for each pixel exceeds three. There are several adaptive methods for steganography have been proposed to reduce the distortion caused by LSBs substitution [1]. While human perception is less sensitive to subtle changes in edge areas of a pixel, it is more sensitive to changes in the smooth areas size. [1]

In Image Encryption approach, it provide lower payload. [2] When key size is large then it required huge computational time [3]. For providing more payloads, compress key size. [4] This method could be extended to colour imagery and audio signals [5] Here only bitmap (bmp) image will be used to hide the data.[6] To improve system security extension of HPDM(Histogram Preserving Data Mapping)will be used. [7] Chaos system is highly sensitive [8] and can be extendable to send secret images in cover image, also for audio and video carrier files. [9]

But disadvantage is Table1 and Table 2 is divided in to alphabets where 'q' is missing also digits are not included. In future this approach can be extendable to send secret image in cover image. This approach can be extendable to audio and video carrier files. [16]

A method for steganography using six square substitution ciphers which includes only alphabets in lower case [17]

A method for steganography using twelve square substitution ciphers which includes both alphabet and digit but the alphabet 'q' and some special character 'space' is missing. [18]

IV. CONCLUSION

In the past few years, the steganography is interested topic for image cover media. This paper provide an overview of steganography and introduce some techniques of steganography which help to embed the data. These techniques are more useful for detecting the stego images as well as the image media relating to security of images and embed the data for complex image area and you can easily estimate the high embedding rate by using the quantitative steganalytic technique.

REFERENCES

[1] R. Amirtharajan, R. Akila and P. Deepika Chowdavarapu: A Comparative Analysis of Image Steganography, IJCA, Vol 2, (2010), 975-8887

[2] Aman Jantan and Mohammad Ali Bani Younes: A New Steganography Approach for Image Encryption Exchange by using the LSB insertion, International Journal of Computer Science and Network Security, Vol 8 (2008), 247-254.

[3] M. Mhamed, M. Bamatraf and Fadwa Al-afari: Data Hiding by LSB Substitution Using Genetic Optimal Key-Permutation, International Arab Journal of e-Technology, Vol. 2 No. 1, 2011.

[4] Po Yuch Chen and Hung Ju Lin: A DWT Based Approach for Image Steganography, International journal of Applied Science and Engineering, Vol.4, (2006), 275-290.
[5] Charles G. Boncelet and Lisa M. Marvel: Spread Spectrum Image Steganography, IEEE Transactions on Image Processing, Vol. 8, (1999),1075-1083.

[6] Rosziati Ibrahim and Teoh Suk Kuan: Steganography Algorithm to Hide Secret Message inside an Image, Computer Technology and Application Vol. 2, 102-108.

[7] H. Rifa-Pous and J. Rifa: Product Perfect Codes and Steganography, Digital Signal Processing, Vol.19, (2009), 764-769.

[8] Joachim J. Eggers, R.Bauml and Bernd Girod: A Communications Approach to image steganography, Proc. of SPIE Volume 4675, San Jose, Ca, 2002,1-12.

[9] Bhavana. S and K. L. Sudha: Text Steganography using LSB Insertion Method along with Chaos Theory, ISRO,E.33011/74/2011-V

[10] Ross J. Anderson and Fabian A.P. Petitcolas: On The Limits of steganography, IEEE Journal of selected Areas in communication, Vol.16, No.4, 1998, pp. 474-481.

[11] Mohammed A.F Al-Husainy: Image Steganography by mapping Pixels to letters, Journal of Computer science, Vol.5, No.1, 2009, pp. 33-38.

[12] Ran-Zan Wang and Yeh-Shun Chen, "High Payload Image Steganography Using Two-Way Block Matching", IEEE Signal Processing letters, Vol. 13, No.3, 2006, pp.161-164

[13] Weiming Zhang, Xinpeng Zhang and Shuozhong Wang, "A Double layered Plus-Minus One data Embedding Scheme", IEEE Signal Processing Letters, Vol. 14, No.11, 2007. pp. 848-851.

[14] Alvaro Martin, Guillermo Sapiro and Gadiel Seroussi, "Is Steganography Natural", IEEE Transactions on Image processing, Vol. 14, No. 12, 2005. pp. 2040-2050.

[15] H. Rifa-Pous and J. Rifa, "Product Perfect Codes and Steganography", Digital Signal Processing, Vol.19, 2009, pp. 764-769.

[16] Gandharba Swain, Saroj Kumar Lenka: A Technique for Secure Communication using Message Dependent Steganography, Special issue of IJCCT, Vol. 2, No. 12,2010.

[17] Gandharba Swain, Saroj Kumar Lenka: Better Steganography using the Six Square Cipher Algorithm, (ICAET-2010), Chennai, India, 2010, 334-338.

[18] Gandharba Swain, Saroj Kumar Lenka: Steganography using the Twelve Square Substitution Cipher and Index Variable , IEEE transactions on Image Processing, 2011, 84-88.