A Review of Image Steganography

[1]Miftah ul uroos,
Student, Department of
Electronics and Communication
Engineering, Swami Devi Dyal
Institute of Engineering and
Technology, Haryana, India

[2]Dimple Goyal,
Assistant Professor, Department
of Electronics of Communication
Engineering, Swami Devi Dyal
Institute of Engineering and
Technology, Haryana, India

[3]Muheet Ahmed Butt
Scientist "D"
PG Department of
Computer Sciences,
University of Kashmir,
Srinagar, J&K

[4]Majid Zaman
Scientist "D"
Directorate of IT and SS
University of Kashmir,
Srinagar, J&K

Abstract

In the modern age of Information Communication Technology where data security plays a key role in the propagation of information. Data hiding plays a very important role with the rapid growth of intensive transfer of multimedia content and secret communications. Steganography is the art of hiding information in ways that prevent unauthorized detection to a very large extent. The Steganography is used to transport information from one place to other place through a basic public channel medium in covert and concealed manner. Steganography furs the very existence of a message so that if successful it generally entices no doubt at all. Steganography means hiding a secret message (the embedded message) within a larger one (source cover) in such a way that an observer cannot detect the presence of contents of the hidden message as the distortion and noise are kept at a very low level. The proposed research review provides an insight of various stenographic techniques and also provides a comparative analysis of the research done in the field of steganography.

I.INTRODUCTION

Steganography refers to the data hiding. The main purpose of image steganography is to hide the data behind images. It means that it encodes the text in the form of image. The steganography is done when the communication takes place between sender and receiver. It is used to send the sensitive information with high security[15]. Nowadays in data transfer over the network, the security is the main issue concerned with this. In order to secure the data while transmission, steganography is used. Before the growth of the steganography, security of the data [17] was the main concern of research for the researchers. The number of techniques was developed in order to secure transmission. Steganography use algorithms for concealing the data. There are various types of steganography[13]. These are:

1. Text steganography.
2. Image steganography.
3. Audio steganography.
4. Video steganography.

In image steganography, the data is hiding behind the cover image. The data is hidden character wise behind the pixels of the image. The several aspects on which the steganography method depends are:

- Robustness
- Capacity
- Undetectability
- Invisibility

From the ancient times, steganography is used to hide the confidential data. The data was hidden on the back of wax, writing tables, stomach of rabbits or on the scalp of the slaves. And now a day, hacking is used for an unauthorized access of data. So, to keep the data confidential, sender uses different methods. The word steganography belongs to Greek language. In Greek the steganography stands for "covered writing". The first of all steganography was used in Greece. They use to enter the message on a wooden tablet and then apply wax on it to hide the written data.

In this modern time, where technology is developing at fast speed and each day new developments are made, security is of highest priority. The data needs to be kept secure and safe so that it could be accessed only by the authorized workers and any unauthorized user cannot have any access of that data. Data sharing is increasing as thousands of messages and data is being transmitted on internet everyday from one place to another. Hence the protection of data is prime concern of the sender. The need is that correct data should be sent but in a secret way that only the receiver should be able to understand the message. At first, technique of cryptography was invented to transmit secret messages over places. In cryptography the message was encoded in another message in a covered way such that only the sender and receiver knew the way to decrypt it. A cryptographic key was used to decode the message that was known only by the authorized persons. The limitation of cryptography was that illegitimate person came to know that the message had a hidden text in it and so the probability of message being decoded by illegitimate person increased. To overcome this limitation the method of steganography was introduced.

The technique of steganography is better than cryptography as in it the data is hidden in image. The image is then sent over internet. It had advantage over cryptography as now the illegitimate person does not come to know whether data is hidden in the image or not. The data could only be decrypted from image by the authorized person as he knows the phenomenon to decode it and had the authorized key with him that was required to decode the data. The security and the reliability of data transmission also improved with invention of steganography as now the other person could not alter the sent data.

Steganography is one of the technique in which the data is hidden in the cover object with the use of secret key. The extractor should have secret key to extract the data. The secret key is designed in such a manner that it can't be find out by an unauthorized user.

In steganography systems following terms are used:

- Cover Media: The cover media is the medium in which message is embedded to hide the presence of secret data.
- Stego: The media through which the data is hidden.
- Secret data: The data to be hidden or extract.
- Steganalysis: The method by which secret data is to be extracted.

In image steganography, images are used as cover object.

The block diagram of basic steganography is shown below:

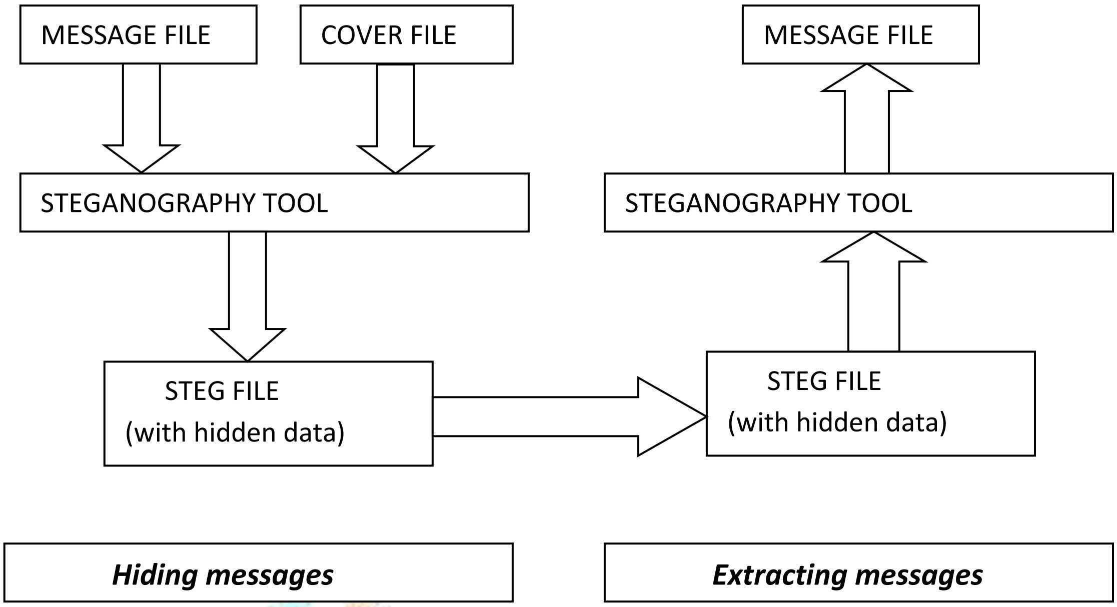

Figure: Block diagram of basic steganography

II.TECHNIQUES:

The various techniques for steganography are available. Some of them are as follows:

- LSB Technique.
- Distortion Technique.
- Masking and Filtering.
- Transform Domain Technique.

LSB technique: LSB stands for Least Significant Bit. This is a technique for image steganography which works on the Least Significant Bit value of the pixels. First the cover image is decomposed into bit planes and then LSB of bit planes is substituted with secret data. This substitution concept includes embedding at the minimum weighting bit as it will not affect the value of original pixel. This technique does not lead to any kind of distortion in the image while embedding data behind it. The value of least significant bit varies but this change is invisible to human eye. The LSB have many advantages such as the image does not depreciated or distorted and by using LSB one can encrypt large amount of data behind an image. It also poses some lacks and also it is less robust in nature, sometimes changes in image can lead to the data lost, hidden data can be revealed easily i.e. less secure. LSB transfers the data to the receivers end with security without allowing the illegitimate person to access the encrypted data.LSB is the popular and oldest method for hiding the message in a digital image. In LSB method we hide the message in the least significant bits (LSB's) of pixel values of an image. In this method binary equivalent of the secret message is distributed among the LSBs of each pixel.

For example data bits 01100101 are tried to hide into an 8 bit color image[16]. According to this technique 8 consecutive pixels from top left corner of the image are selected. The binary equivalent of those pixels may b like this

00100101 11101011 11001010 00100011

11111000 11101111 11001110 11100111

Now each bit of data 01100101 are copied serially (from left hand side) to the LSB‟s of equivalent binary pattern of pixels, resulting the bit pattern would become

00100100 11101011 11001011 00100010

11111000 11101111 11001110 11100111

The problem with this technique is that it is very vulnerable to attacks such as image compression and quantization of noise.

a) Advantages of LSB

- Less suspicious to human eyes.
- Simple to implement and many techniques uses this method.
- High perceptual transparency.
- 100% chances of insertion.

b) Disadvantages of LSB

- Three weakness- Robustness, Tamper and Resistance.
- Extremely sensitive to any kind of filtering.
- Scaling, Rotation, Cropping, adding extra noise lead to destroy the secret message.

Distortion Technique: Distortion technique encrypts the data by distorted it. In this original cover image is decoded into encrypted or distorted cover image. In this technique the receiver applies a function on encrypted or distorted image in order to decrypt it. In this steganography is applied by making distortions in image. This technique performs a sequence of alterations in cover image. Then this sequence is applied for the purpose of comparing the encrypted message with forwarded message. The data is encrypted behind randomly selected pixels. In case when the encrypted image vary from original image then bit "1" is used else bit "0" is used. In this cover image is send to the receiver which is a barrier in the security provided by this technique. It is a rule that the cover image should always used for once while steganography if any cover image is used more than once in steganography then it will easy for the illegitimate person to attack the image for accessing the encrypted data behind the image.

Masking and Filtering: This technique works in the same way as the technique of watermarking. In this case data is not hidden behind any image. Instead of hiding, data is attached or inserted on such space which is secure from attackers. In this technique, watermarking is used for securing the data. This method facilitate the user with the feature of robustness, compression is done because data is embedded on a secured surface and visible to everyone. The limitation of this system is that it is meant for only gray scale images.

Transform Domain Technique: This technique possesses much complexity as compare to other techniques. It performs steganography by hiding the data behind the image. It uses many algorithms to encode the data. Some transformations are also used for steganography. As it is clear from the name of the technique that number of transformation domains is used for embedding the data and then further algorithms are used for encryption. The data is embedded in frequency domain. It is much preferable technique of embedding the data in comparison of time domain. This technique hides the data in that images which are safe from attackers and there is no need of data compression in this technique.

In image steganography, data hiding method can be classified into different categories

- Spatial domain steganography
- Frequency domain steganography
- Adaptive domain steganogarphy

Spatial domain steganography: In spatial domain steganography, cover image and secret data are modified by using LSB and level encoding. The cover image is first decomposed into bit planes and then LSB of bit planes is replaced with secret data. LSB substitution is the mostly used steganographic technique. This substitution concept includes embedding at the minimum weighting bit so that it will not affect the value of original pixel. The only drawback of the LSB insertion is the simplicity of extraction process. Thus, an illegitimate person can easily extract the data.

Frequency domain steganography: In frequency domain steganography, secret data is hidden in significant areas of covered image, which makes data invigorate to attacks such as compression, cropping or image processing methods than LSB approach. This provides an improved security level to steganography technique and lead to the development of algorithms. The various transforms include DCT, DWT and DFT. Wavelet Transform (WT) converts spatial domain information to the frequency domain information. Wavelets are used in image because wavelets separately partition the high frequency and low frequency information pixel by pixel. This method mainly addresses the capacity and robustness of the data hiding system.

Adaptive steganography: This steganography method is a special case of two methods, that are, spatial domain and transform domain steganographic methods. It is also known as “Statistics Aware Embedding and Masking”. Global features of images are used before embedding secret data in coefficients of DCT or DWT. This statistics will decide where changes can be made.

III.APPLICATIONS:

The main application fields of steganography are:

- Copyright Protection
- Feature Tagging
- Secret Communication
- Use by defence
- Digital Watermarking
- Intelligence services
- Steganography printers
- Web based applications

IV.Literature Survey

Rutuja Kakade, et al [1] introduced a new steganography technique that can be applied to secure the data during transmission. Also the data can be added in QR code for the ease of access of sending information.

The various techniques of steganography used are the DWT technique and LSB steganography. The data to be steganographed had been encrypted using AES algorithm to improve the security.

Marwan Ali Albahar, et al [2]gave two solutions in data security field for ensuring that only legitimate receivers will have access to the intended data: steganography and cryptography. These solutions provided a high level of security. With the exponential growth of challenges in the field of computer security, the use of Bluetooth technology is expanding rapidly to expose many of these challenges on the surface. One of these challenges is the MITM attack during Bluetooth pairing process. It introduced a novel method based on steganography to secure the pairing process and prevent MITM attacks.

Sujarani Rajendran, et al [3] proposed a new symmetric key based image hiding technique. Pseudo random keys are generated by using 1D logistic map and those keys are used for choosing the pixel position of cover image randomly for hiding the secret image. The main security part of the projected method is the selection of pixel position in the cover image. Peak Signal Noise Ratio (PSNR) and Mean Square Error (MSE) measures are used for comparison and the result analysis showed that the proposed scheme provided efficient level of security.

Vijay Kumar Sharma, et al [4] reviewed the steganographic techniques and their uses and attacks on these. The steganography is commonly known as covert writing and mainly used in hidden communication. A reliable internet communication is free from the attacks if steganography is used.

Vandana Yadav, et al [5] used new technique for steganography in a HSI color cover images, which hides secret message in the edges of the carrier images using 2-bit LSB substitution for embedding. To get true edges, canny edge detection technique has been used. The amount of data to be embedded plays an important role on the selection of edges. The main advantage of using HIS color mode is that it produced a image with a significantly large file size hence we hide large amount of confidential message. The proposed technique had better and higher embedding capacity.

Mirza Abdur Razzaq, et al [8] blended security technique using encryption, steganography and watermarking. It comprised of three key components: (a) the original image has been encrypted using large secret key by rotating pixel bits to right through XOR operation, (b) for steganography, encrypted image has been altered by least significant bits (LSBs) of the cover image and obtained stego image, then (c) stego image has been watermarked in the time domain and frequency domain to ensure the ownership. The proposed approach is efficient, simpler and secured and it provided significant security against threats and attacks.

Wid A. Awadh, et al [10] presented a new text steganography approach for hide loaded secret English text file in a cover English text file to ensure security of data in cloud computing. The proposed approach improved data security, data hiding capacity, and time.

Mandeep Kaur, et al [11] used three different techniques such as Huffman encoding, Deoxyribonucleic acid and State Transition. Initially, Huffman is applied over the text for the compression, and then Deoxyribonucleic acid is applied over the compressed data for the encryption and lastly State Transition algorithm has used for updating the location in the image. The application of these algorithms provided high security in comparison with the traditional algorithms. The implementation of these algorithms is done with respect to message bits. Total three images are used for the evaluation of traditional and proposed techniques in which the message bit varies from fifty to hundred. The simulation analysis concluded that the proposed method is efficient, more secure and proficient in comparison with other techniques such as LSBs, LF-DCT and MF-DCT. The parameters PSNR and MSE are used for the evaluation of their performance.

Muhammad Zaheer, et al [12] proposed security and payload capacity enhancement of an image steganography system for an audio message by using compressed sensing theory. However, in order to utilize compressed sensing, the audio message is first converted to an equivalent grayscale image which is sparsified using 2D-DCT and thresholding. The sparsified image is further compressed using the proposed compressed sensing algorithm which not only enhanced the security but also improved the payload capacity; without losing imperceptibility of the system. The compressed image is embedded in chaotically chosen pixels of the cover image. At receiver the compressed sensing reconstruction algorithm is used to reconstruct the grayscale image which is then converted back to the audio message. The proposed system is highly imperceptible, secure and robust against various image processing attacks. It reconstructed secret audio message with high PSNR value.

Saher Manaseer, et al[14] worked with a new technique to embed the secret message into colored images. Two versions of the proposed algorithm, named standard LSB and Condition Based LSB respectively, were used. The experiment measures PSNR (Peak Signal to NOISE Ratio) and MSE (Mean Squared Error) for the two versions showed that the standard LSB version outperforms the second proposed version.

Brij Mohan Kumar, et al [6] presented a cryptography based technique to authenticate the images and is used to prevent image forgery. While steganography has been around for centuries, the Digital Revolution has sparked a renewed interest in the field. It focused specifically on the techniques employed in hiding information in digital image files.

Harini .V, et al [7] proposed a method to enhance the security by embedding data in colour images. The cover image is first converted to any one plane process and encrypted by using Chaos encryption. Adaptive LSB replacement algorithm is used for hiding the secret message bits into the encrypted image. In the secret data extraction module, the secret data will be extracted by utilizing significant key for choosing the image pixels to extract the data. The technique is particularly helpful in applications such as medical and military imaging. The proposed methodology provided better performance in terms of number of slices, number of IOBs and is implemented in FPGA (field programmable gate array). The design architecture when implemented on FPGA Spartan III offers high processing speed, which gave an impulse for the researchers to a very fast, programmable & cost effective hardware solution in the area of Secure Communication.

Mr. Jayesh Sharma, et al [13] reviewed different security and data hiding techniques that are used to implement a steganography such as LSB, ISB, MLSB etc.

V.COMPARATIVE STUDY

RESEARCHERS	TITLE	TECHINIQUES USED	EFFICIENCY LEVEL

1. Rutuja Kakade, et al.	“Image Steganography and Data hiding in QR code”	LSB based steganography, DWT technique, with AES algorithm.	High security, temper resistance, ease of access of sending information (due to addition of QR code).
2. Sujarani Rajendran, et al.	“Chaotic Map Based Random Image Steganography using LSB Technique”	LSB based steganography with 1D logistic map.	Efficient, highly secure, high PSNR, low RMSE.
3. Vijay Kumar Sharma, et al	“A Study of Steganography based data hiding techniques”	Cryptography, Steganography, Watermarking.	High hiding capacity, high security level.
4. Vandana Yadav, et al.	“A new approach for Image Steganography using Edge Detection Method for Hiding Text in Color Images using HSI Color Model”	Edge Detection, 2-bit LSB, with HSI color model.	Better and higher embedding capacity.
5. Brij Mohan Kumar, et al.	“An Introduction to Steganographic Techniques in the field of Digital Image Processing”	LSB based steganography, DCT (Direct Cosine Transform) algorithm.	Temper resistant.
6.Harini.V, et al	“FPGA Implementation of Secret Data Sharing through Image by using LWT and LSB Steganography Technique”	Chaos encryption, Adaptive LSB, LWT (Lifting Wavelet transform).	High processing speed, cost effective hardware.

7. Mirza Abdur Razzaq, et al.	“Digital Image Security: Fusion of Encryption, Steganography and Watermarking”	Encryption, LSB, Watermarking.	Efficient, simpler and secured.
8. D. Suneetha, et al.	“A Novel Algorithm for Enhancing the Data Storage Security in Cloud through Steganography”	LSB based steganography.	High data storage security in cloud.
9. Wid A. Awadh, et al.	“Using Steganography for secure data storage in cloud computing”	Text steganography.	Improved data security, data hiding capacity and time.
10.Mandeep Kaur, et al.	“Hybrid approach for improving data security and size reduction in Image Steganography”	LSB based steganography, LF-DCT, MF-DCT.	Efficient, more secure, proficient, high PSNR, low MSE.
11.Muhammad Zaheer, et al.	“Compressed Sensing Based Image Steganography System for secure transmission of Audio message with Enhanced Security”	2D-DCT, thresholding, LSB based steganography.	Highly imperceptible, secure and robust against various image processing attacks, high PSNR.

VI.Conclusion

The main objective of image steganography is to conceal the secret data using cover images. So the fundamental requirement of this research is that the hidden data carried by stego-image should be invisible to undesired user. There are different techniques that are used in image steganography. LSB is a technique in image steganography which works on the Least Significant Bit value of the pixels. Distortion technique encrypts the data by distorted it. In this original cover image is decoded into encrypted or distorted cover image. In Transform Domain technique, the data is embedded in frequency domain. It is much preferable technique of embedding the data in comparison of time domain. Since, sometimes there is the restrictions imposed on availability of encryption services by various governments, therefore in that case steganography is the better option.

REFERENCES

[1] Rutuja Kakade, Nikita Kasar, Shruti Kulkarni, ShubhamKumbalpuri, SonaliPatil, “Image Steganography and Data hiding in QR code”, IRJET, Vol 04, 2017.

[2] Marwan Ali Albahar, OlayemiOlawumi, KeijoHaataja, PekkaToivanen, “A novel method for Bluetooth pairing using Steganography”, IJITS, No. 1, Vol 09, 2017.

[3] Sujarani Rajendran, Manivannan Doraipandian, “Chaotic Map Based Random Image Steganography using LSB Technique”, IJNS,Vol 19, No.4, 2017.

[4] Vijay Kumar Sharma, Dr. Devesh Kr Srivastava, Dr. PratisthaMathur, “A Study of Steganography based data hiding techniques” , IJERMT,Vol 6, 2017.

[5] Vandana Yadav, Sanjay Kumar Sharma, “A new approach for Image Steganography using Edge Detection Method for Hiding Text in Color Images using HSI Color Model”, IJSRSET, Vol 03, 2017.

[6] Brij Mohan Kumar, Prof. Y.S Thakur, “An Introduction to SteganographicTechiniques in the field of Digital Image Processing”, IJESC, Vol 07, 2017.

[7] Harini.V, Vijayaraghavan, “FPGA Implementation of Secret Data Sharing through Image by using LWT and LSB Steganography Technique”, IJESC, Vol 07, 2017.

[8] Mirza Abdur Razzaq, Mirza Adnan Baigh, Riaz Ahmad Shaikh, Ashfaque Ahmad Memon, “Digital Image Security: Fusion of Encryption, Steganography and Watermarking”, IJACSA, Vol 08, No. 5, 2017.

[9] D. Suneetha, Dr. K. Kirankumar, “A Novel Algorithm for Enhancing the Data Storage Security in Cloud through Steganography”, ACST,Vol 10, No. 9, 2017.

[10] Wid A. Awadh, Ali S. Hashim, “Using Steganography for secure data storage in cloud computing”, IRJET, Vol 04, 2017.

[11] Mandeep Kaur, Rupinder Kaur Randhawa, “Hybrid approach for improving data security and size reduction in Image Steganography”, IRJET, Vol 04, 2017.

[12] Muhammad Zaheer, I.M Qureshi, ZeeshanMuzaffar, Laeeq Aslam, “Compressed Sensing Based Image Steganography System for secure transimission of Audio message with Enhanced Security”, IJCSNS, Vol 17, No. 7, 2017.

[13] Mr. JayeshSurama, et al, “ Steganography Techniques”, IJEDR, Vol 05, 2017.

[14] SaherManaseer, AsmaaAljawawdeh, DuaAlsoudi, “A New Image Steganography Depending on Reference and LSB”, IJAER, Vol 12, No. 9, 2017.

[15] Divya Suryawamshi, Meetali Salvi, Soumya Pandey , “Image Steganography for criminal cases”, IJEDR, Vol 05, 2017.

[16] Mamta Yadav, Amita Dhankar, “Image Steganography Techniques: A Review”, IJIRST, Vol 2,2015.

[17] Khan, Qamar Rayees, et al. "Integrity Model based Intrusion Detection System: A Practical Approach." International Journal of Computer Applications 115.10 (2015).