A Survey & Applications of Various Image Steganography Techniques

Saurabh Paliwal
Department of Computer Science & Engineering
T.I.T.S
Bhopal, India
Saurabh.paliwal34@gmail.com

Prof. Rajesh Kumar Nigam
Department of Computer Science & Engineering
T.I.T.S
Bhopal, India
Rajeshrewa37@gmail.com

Abstract—Due to research is the ever-increasing need for harder-to-break encryption and decryption algorithms as the computer and network technologies evolve. We believe that by proposing the block-based encryption and decryption algorithm, it will help to reduce the relationship among image elements by increasing the entropy value of the encrypted images as well as lowering the correlation. Here in this paper a survey of all the existing Image Steganography techniques are discussed with their various advantages and limitations. Hence on the basis of their various advantages and limitations a new and efficient Image Steganography is implemented in future.

Index Terms— Steganography, Information Security, data hiding, Image Embedding, Image Extraction.

I. Introduction

The presence of computer networks has prompted new problems with security and privacy. Having a secure and reliable means for communicating with images and video is becoming a necessity and its related issues must be carefully considered. Hence, network security and data encryption have become important. The images can be considered nowadays, one of the most usable forms of information. Image and video encryption have applications in various fields including Internet communication, multimedia systems, medical imaging, telemedicine and military communication. The fast expansion of computer networks permitted to large multimedia data files, such as digital images, to be easily transmitted over the internet these multimedia data encryption is broadly used to make certain security but, most of the available encryption algorithms are used for text data. Digital steganography can conceal top secret data (i.e. secret files) extremely strongly by embedding them into some media data known as "vessel data." The vessel data is also referred to as "carrier, cover up, or replica data". In Steganography images used for vessel data. The embedding action put into practice is to substitute the "intricate areas" on the bit planes of the vessel image with the secret data. The most significant feature of Steganography is that the embedding capability is incredibly huge. For a 'normal' image, approximately 50% of the data might be disposable with secret data earlier than image damage becomes perceptible.

Due to large data size and real time constrains, algorithms that are good for textual data may not be suitable for multimedia data. In most of the ordinary images, the values of the neighboring pixels are strongly correlated (i.e. the value of any given pixel can be reasonably predicted from the values of its neighbors) [1]-[3].

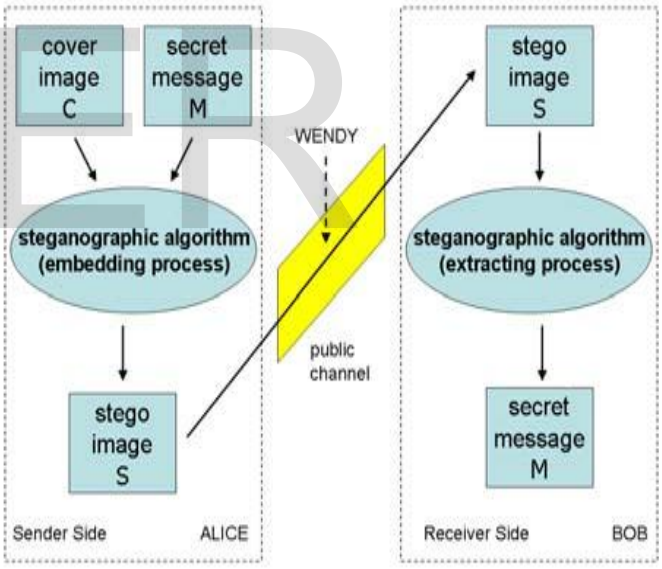

Figure 1: Basic steganographic model

In order to dissipate the high correlation among pixels and increase the entropy value, there are so many transformation algorithms that split the image into blocks and then shuffle their positions before it passing them. However, addition of encryption defect the use of image encryption technique as the fundamental need for security is to eradicate the suspicion of hidden data. Most of the available encryption algorithms are mainly used for textual data and may not be suitable for multimedia data such as images. For most data hiding

applications, a certain degree of compression is desired and is often constrained by acceptable image quality. Such manipulation is necessary to facilitate efficient information transfer and storage. In this [4] steganalysis process is used. The ambition of [5] steganalysis is to decide if an image or additional carrier contains an embed message. To enhance the protection and payload speed the embedder will acquire multicarrier embedding model in the [6] spread spectrum communication is explained. Since traditional encryption schemes are not well for modern multimedia requirement, many researchers have been constantly to explore better solutions for image and video encryptions. The approaches used of this research work are specially oriented towards analyzing since that no one method is proficient of achieving each and every one these goals, a group of processes is considered necessary to extent the variety of likely applications. The procedural challenges of data hiding are terrible. There is numerous data hiding and data extraction schemes are comes into existence. The key data hiding procedure is steganography. Many existing schemes under this category are found to simply accomplish reasonable or even low security and even low encryption speed.

II. Theoretical Background

Steganography is the art and science of covert communication by embedding a message into an innocuous looking cover media such as text, image, and video. In steganography, covert writing is established for two main reasons: protection against detection (data hiding) and protection against removal, which is in turn divided into watermarking and fingerprinting. The tremendously fast development of the internet technology brings more and more attention to the information security techniques, such as text encryption, image encryption, video encryption, etc. In other words, information security is an advantage that has a value like any other asset. As an advantage, information needs to be secured from attacks during transmission over wired or wireless networks. During the last two decades, the use of information brings more and more on using internet technology. So the authorized people can send and receive information from a long distance transmission using computer networks. To be secured, information needs to be hidden from unauthorized access (confidentiality), protected from unauthorized change (integrity), and available to an authorized entity, when it is needed (availability). Not only should information be confidential, when it is stored in a computer; there should also be away to maintain its confidentiality, when it is transmitted from sender to receiver [7].

Traditionally the information transmitted only text by using traditional encryption schemes, but nowadays also audio, image, and other multimedia types due to the widespread transmission over various communication networks. So it has been observed that the security of multimedia data is most important. The field of multimedia security has grown in the last decade to provide design insights for the protection of multimedia data and enhancement of digital media under a number of miscellaneous attack scenarios. In such a way, one natural question that arises is the security and confidentiality of a digital packet of multimedia information.

As a promising tool for the design of digital ciphers technique, DWT theory has been extensively used to especially develop image encryption algorithms. The simplicity of many transformation techniques and the well established DWT theory make it possible to approach practically good solutions to image encryption. The general design rules for image encryption systems have been presented. Finally, Examples of the current important image encryption techniques were presented. Moreover, the security of steganographic systems must be founded on the hypothesis that an attacker has full knowledge of the steganographic system embedding and extracting algorithmic procedures. Yet, he/she has no access to the stego key which must be as strong as possible in order to prevent attackers from extracting the secret information out of the cover [8].

III. Image Steganography

Image steganography has been the focus of a significant body of research because of the large amount of redundancy in an image file that could be potentially. Utilised to hide communication. An image is a collection of numbers that constitute different light intensities in different areas of the image. When dealing with images of greater bit depth, the image file size turn out too large to be sent over the Internet. Thus, some methods were introduced to reduce an image's file size so that it can be displayed in reasonable time and use less space during storage. These methods employs mathematical formulas to compress image data, leading to a smaller file sizes also known as image compression [9]. This numeric representation forms a grid and the individual points are referred to as pixels (picture elements). Greyscale images use 8 bits for each pixel and are able to display 256 different colours or shades of grey. Digital colour images are typically stored in 24-bit files and use the RGB colour model, also known as true colour. All colour variations for the pixels of a 24-bit image are derived from three primary colours: red, green and blue. Each primary colour is represented by 8 bits. Thus, in one given pixel, there can be 256 different quantities of red, green and blue.

Basically, the steganography process contains three main components: a message, a carrier file and a key as shown in Figure 2.

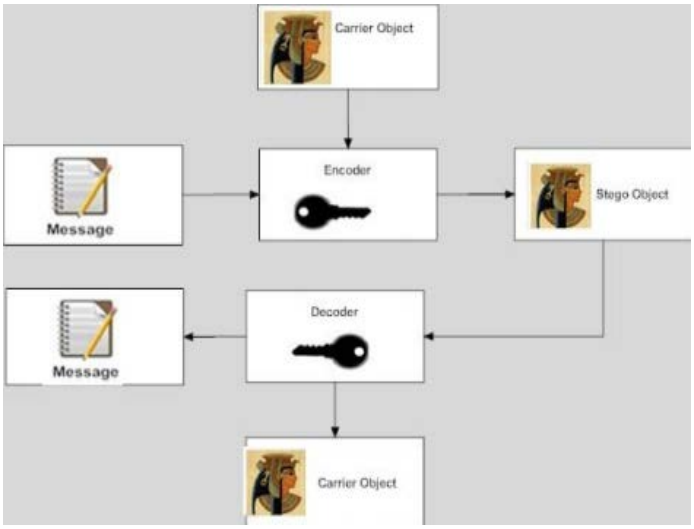

Figure 2: The Steganography Process

The message is the QR code file that is going to be embedded (hidden) in the carrier. The carrier file (image file) is the object that carries the message. The key is used to decode (extract) the hidden message from the carrier file. This process can be mathematically represented by:

$$y(k) = s(k) + \alpha\, w(k)$$

The message, w (k), and the carrier file, s (k), are independent from each other. They both have continuous values. Depending on the key, some of the values of the message, w (k), can have zero as its value. The parameter, "α" determines the value of the strength of the message, which can be changed depending on its perceptual characteristics, robustness properties etc. Typically it has values greater than zero, i.e. $\alpha>0$. If the decoder has access to the cover message, s (k), then it will be easy to know the hidden message by subtracting s (k) and y (k):

$$\alpha\, W(k) = y(k) - s(k)$$

On the other hand, if the decoder does not know the cover message, s (k), then a slightly more secure system for the sender and receiver would be to share a secret key that specifies the method of obtaining w (k). Even if an adversary suspects the usage of steganography, without the secret key, there will be no way of determining the pixels to target. The key in the steganography formula is comprised of the embedding methods and its applied algorithms which are used to embed and extract w (k).

IV. As Steganography with Cryptography, Watermarking and Fingerprinting

The embedded data- the message that one wish to communicate covertly - is normally hidden in an innocuous message, known as a cover object in which the stego-object is produced. A stego-key is used to manage the hiding process and retrieval of the embedded data between communicating covert parties. Digital media are increasingly equipped with distinguishable marks, which may encompass a hidden copyright notification or serial number to counteract copyright violation. Cryptography aims to keep the contents of a message secret, while steganography aims to keep the existence of a message undetectable [10]. Encryption ciphers secret information in a way that it becomes unreadable except for the intended recipient who can decode it. The encrypted message might grab eavesdropper's attention, since its protection means something valuable is keep confidential. Therefore, this security vulnerability can be significantly reduced by using steganography techniques so that it draws no special attention.

Steganography and Cryptography: Cryptography and Steganography are members of the spy craft family, both aiming at providing secret communication. Cryptography secretes only the meaning or contents of a message from an eavesdropper, but the encrypted message still exists and can be seen. Steganography, on the other hand, offers more secrecy than cryptography, since it hides the mere existence of secret message rather than only protecting the message contents [11].

A Cryptography system is jeopardized if a malicious attacker can read the contents of a secret message, while a steganographic system is jeopardized if the existence of the message is detect by an attacker. In other words, a stegonagraphic system is considered exposed even without decoding the message, if an attacker suspects the file carrying the secret message or the steganography method used for encoding the secret message. Hence, steganography can complement cryptography to avoid raising the suspicion of system attackers and not to substitute cryptography. Steganography is a branch of information hiding technology which encompasses applications for protection against detection and protection against removal such as copyright protection for digital media, watermarking, fingerprinting and data embedding. In these applications, information is hidden within a host data set, which is intentionally corrupted in a covert way, so that it could be sent secretly to an intended receiver.

Steganography and Watermarking: Steganography and watermarking are methods of data hiding and share common features. The goal of watermarking is to embed a unique signature to signify the origin or ownership of a digital media for the purpose of copyright protection, while the goal of steganography is to cover the existence of the communication taking place within a digital media. Watermarking is a mechanism used to prove that illegal copying or any minor modification of the watermarked file is done.

One of the main features of watermarking is known as ''robustness'', if someone knows that a digital mark exists (i.e. visible watermarking) and tries to remove the watermark from the watermarked media, he/she should consequently cause

distortions or destroys the original watermarked media. In order to take our discussion further, in the next section another technology, closely related to watermarking, called fingerprinting is discussed.

Steganography and Fingerprinting: Watermarking and fingerprinting are closely related to steganography and fall in same domain of information hiding. Both approaches share techniques that are used to imperceptibly convey information by embedding it into the cover file, yet the kind of embedding information is of a different algorithmic form. In watermarking, all copies of the carrier object are marked in the same way, while in fingerprinting different unique marks are embedded in distinctive copies that are supplied to different clients. These unique embedded marks should identify the redistribution of illegal copies providing a traitor-tracing functionality. A steganographic system is jeopardized, if an attacker suspects a specific file or steganography method even without decoding the message, while a successful attack on a watermarking or fingerprinting system would be the removal of the mark. The fundamental difference between the three technologies is the underlying philosophies of the cover file. In watermarking and fingerprinting, the information hidden inside the cover file may also be public knowledge and even visible sometimes, while in steganography the imperceptibility of the hidden information is critical. A successful attack on a steganographic system consists of an adversary detecting the existence of hidden information inside a file [12], while a successful attack on a watermarking or fingerprinting system would be removing the mark, and not its detection. Technically, steganographic methods are considered robust against modifications that may occur during transmission and storage, but not against modification of data. Watermarking and fingerprinting, on the other hand, have the additional notion of resilience against attempts to remove hidden data. In these applications, the embedded information should be robust against possible attempts to remove it, since they provide proof of ownership of digital data [13]. Thus, steganography's underlying philosophy is protection against detection, while watermarking and fingerprinting underlying philosophy is protection against removal.

V. Literature Survey

In this study [14], author had a survey on audio steganography modern examine the suggestion of hiding messages and data inside other pieces of data can be useful in many existent world applications together with encryption and some extra code-writing techniques. Data hiding techniques are a novel type of expertise in secret way of communication over insecure channel. Multimedia objects like audio are the most used in this day's information hiding methods. Audio file due to its far above the ground level of being without a job and high data transmission rate can generate a good hiding standard. Due to that, some essential perceptions of audio steganography and HAS together with Phase Coding, Least Significant Bit (LSB) Coding, Echo data hiding and Spread Spectrum (SS) were wrapped. Two widespread techniques of MP3 steganography were offered embedding during and after compression. A number of formats such as MP3 have been used in audio data steganography. Variety of techniques has been created for embedding data in digital audio.

In this part of writing additionally [14] to extra stress on MPEG-1 layer III (MP3) steganography. A variety of techniques have been talk about for civilizing imperceptibility, forcefulness and competence along with systematic information about limitations and strong points of these methods. For each method based on the disadvantages, author had to conveyed finish and tried by commencing a recommended technique can documents to the enhanced consequence. On the other hand, in embedding after compression move towards accomplishment can be accomplished if the decoding and encoding procedure do not execute during the embedding development. So the safety measures of hidden information is the most excellent in view of the fact that they pass through during communication over insecure channel using the process which set in data after compression.

In this description author [15] suggest new methods are used for addressing the data-hiding method and estimate these techniques in glow of three applications: copyright protection, tamper proofing, and augmentation data embedding and data tracking and corrupting is rapidly developing in communication. So we have to security device the data from the followers. Hence we necessitate a skillful and enthusiastic and save from harmed data hiding proposals to secure from these attacks and origin system. In this proposed system author [15] is to meet the expense of a good quality extraction method which determined the blindly enhancement of data the blindly extraction technique is calculated. This method uses the M-IGLS algorithm for the withdrawal. Blindly extraction represents the original host and the embedding delivery services are not requiring being familiar with that. At this point, the hidden data embedded to the host signal passing through multicarrier SS (Spread Spectrum) embedding method. The hidden data is taken out from the digital multimedia data like audio, video or image. The data is established by way of DCT transform by multicarrier SS (Spread Spectrum) embedding method. The extraction algorithm used to process will meet the expense of high signal to noise fraction and it will accomplish the opportunity of fault progression identical to disreputable host and embedding carriers extract the hidden data from digital multimedia data is Multicarrier Iterative Generalized Least Squares (M-IGLS).

As a Steganography approach the perceptual quality of the host audio signal was not to be degraded. In the proposed technique [16], first the secrete data is embedded into the image and that image is embedded into the audio. Initially, for the reason that the size of the information is usually to a certain extent small contrasted to the size of the data in which it must be secreted to the

cover text, electronic media is much easier to work with the purpose of hide data and take out messages. Secondly, extraction itself can be computerized when the data is electronic, in view of the fact that computers can proficiently influence the data and accomplish the algorithms required to get back the messages. Electronic data also frequently includes redundant, avoidable and unobserved data spaces which can be influenced with the intention of hide messages. The most important objective of this paper was author has to find a way to going on research so that an audio file can be used as a host media to hide textual message without affecting the file structure and content of the audio file a process of embedding text-based data into a host audio file using the method of bit modification has been presented [16] in which the data field is edited to embed intended data into the audio file. Because dreadful conditions in the perceptual quality of the cover object may show the ways to a perceptible transform in the cover object which may leads to the disappointment of purpose of steganography. The two most important criteria for doing well steganography are that the stego signal consequences from embedding is perceptually impossible to differentiate from the host audio signal, and the embedded message is make progressed correctly at the receiver. In analysis cases the text-based data has been effectively embedded to the audio file to create in your mind in what amount the objective has been accomplished.

There are frequent proposed protocols to hidden data in channels containing pictures, video & audio and even typeset text. A process of embedding text-based data into a host audio file using the method of bit modification has been presented in this paper. U. Mourya Vardhan et. al. [17] try to developed a procedure has been in which the data field is prepare for publication to embed be going to data into the audio file. In this paper, secret communication through audio, i.e., embedding textual information in an audio file steganography. To keep on with this, the header section of the header section may show the ways to a altered form of complete audio file. Through this technique the perceptual quality of the host audio files not degraded and not be detected.

In this paper [17] the main goal of author was embedding of text into audio as a case of steganography. The two major criteria for doing well steganography are that the stego signal resulting from embedding is perceptually interchangeable from the host audio signal, and the embedded message is re-concealed in the approved manner at the receiver side.

Hamidreza Rashidy et. al's proposed a new way of providing Secrete Information hiding technique using Genetic Algoithm [18]. The main idea of the proposed technique is modeling the steganography problem as a search and optimization problem. Experimental results, in comparison with other currently popular steganography techniques, demonstrate that the proposed algorithm not only achieves high embedding capacity but also enhances the PSNR of the stego image.

VI. Conclusion

The discussion highlighted requirements and limitations of existing techniques for digital copyright protections such as cryptography, steganography, watermarking and fingerprinting. For instance, the key generation technique used in cryptography and the dependence of the watermarking technique on the structure and format of the text compromises their efficiency. Therefore, the review of various techniques research was identified, which was to develop the above stated framework in order to provide a tool that fulfils the security and performance expectations of a steganographic system. Here in this paper the Various Steganography techniques are analyzed with different issues.

References

[1] S. P. Nana'vati., P. K. panigrahi. "Wavelets: applications to image compression- I," joined of the scientific and engineering computing, vol. 9, no. 3, 2004, pp. 4-10.

[2] Raftael C., gonzales, e. Richard, and woods, "Digital image processing," 2nd ed, Prentice hall, 2002.

[3] A.L. Vitali, A. Borneo, M. Fumagalli and R. Rinaldo, "Video over IP using standard compatible multiple description coding," Journal of Zhejiang University-Science A, vol.7, no.5, 2006, pp.668-676.

[4] S. Lyu and H. Farid, "Steganalysis using higher-order image statistics," IEEE Trans. Inf. Forensics Security, vol. 1, no. 1, pp. 111–119, Mar.2006.

[5] G. Gul and F. Kurugollu, "SVD-based universal spatial domain image steganalysis," IEEE Trans. Inf. Forensics Security, vol. 5, no. 2, pp.349–353, Jun.2010.

[6] M. Gkizeli, D. A. Pados, and M. J. Medley, "Optimal signature design for spread-spectrum steganography," IEEE Trans. Image Process., vol.16, no.2, pp. 391–405, Feb. 2007

[7] S. Li, Analyses and New Designs of Digital Chaotic Ciphers, Ph. D. Thesis, School of Electronics & Information Engineering, Xi an Jiaotong University, Xi an, China, June 2003.

[8] Cox, I. J., Miller, M. L., Bloom, J. A., Fridrich, J. and Kalker, T., 2008. Digital Watermarking and Steganography-Second Edition, Burlington, MA, USA, Elsevier Inc.

[9] Schneider, G.M. and Gersting, J.L., Invitation to computer science. Course Technology. 2004.

[10] Wang, H. and Wang, S., Cyber Warfare: Steganography vs. Steganalysis. 2004.

[11] Lou, D.-C. and Liu, J.-L., Steganographic Method for Secure Communications, Computers and Security, pp.449-460. 2002.

[12] Artz, D., Digital Steganography: Hiding data within data, IEEE Internet Computing 5(3), pp.75-80. 2001.

[13] Katzenbeisser, S. and Petitcolas, F., Information Hiding Techniques for Steganography and Digital Watermarking, Artech House. 2000.

[14] Mohsen Bazyar and Rubita Sudirman, "A Recent Review of MP3 Based Steganography Methods" International Journal of Security and Its Applications Vol.8, No.6 (2014), pp.405-414.

[15] Ch. Anusha , V. Sireesha, " Eliminating Hidden Data from an Image Using Multi Carrier-Iterative Generalized Least Squares" International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064, 2014.

[16] Budda Lavanya, Yangala Smruthi, Srinivasa Rao Elisala, "Data hiding in audio by using image steganography technique, "International Journal of Emerging Trends & Technology in Computer Science ISSN 2278-6856, 2013.

[17] U. Mourya Vardhan, A. Srinivasa Rao, "Imperceptible Data Transmission "International Journal of Technological Exploration and Learning, Volume 1 Issue 2, 2012.

[18] Hamidreza Rashidy Khan, Bahram Nazeri," A Novel Image Steganograogy Scheme with high embedding capacity and tunable visual image quality based on Genetic Algorithm", Expert Systems with Applications, Elsevier, 2014.