Various JPEG Image Steganography Techniques: A Review

Priyanka Pal
Dept. of computer science
Radharaman institute of technology and science
bhopal, india
priyanka.cse25@gmail.com

Shubha Dubey
Dept. of computer science)
Radharaman institute of technology and science
bhopal, india
chaturvedishubha07@gmail.com

Abstract—Image Steganography is a technique of providing some hidden data into the cover or host image so that it can be transmitted in a secure manner. There are various Image Steganography techniques implemented with some advantages and limitations. Here in this paper a complete survey of all the Image Steganography technique their advantages and issues are discussed and analyzed, hence on the basis of their issue or limitations a new and efficient technique is implemented in future.

Index Terms—Steganography, Image Embedding, Image Extraction, Mosiac Images, Watermarking.

I. Introduction

Steganography is an art of writing for conveying message inside another media in a secret way that can only be detected by its intended recipient. There are security agents who would like to fight these data hiding systems by steganalysis, i.e. discovering covered secret messages and rendering them useless.

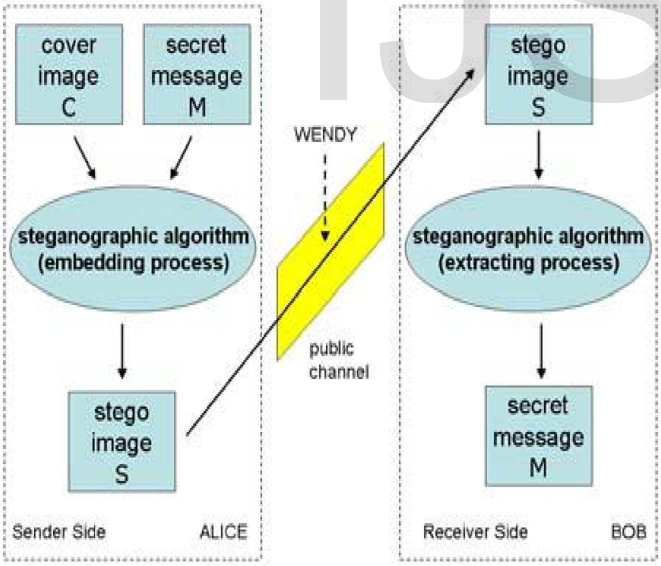

Figure 1: Basic steganographic model

Steganalysis is the art of detecting the message's existence, messge length or place of message where it is to be hidden in covered media and blockading the covert communication. In other words, steganography is the process of hiding a secret message within a larger one in such a way that someone cannot know the presence or contents of the hidden message [1].

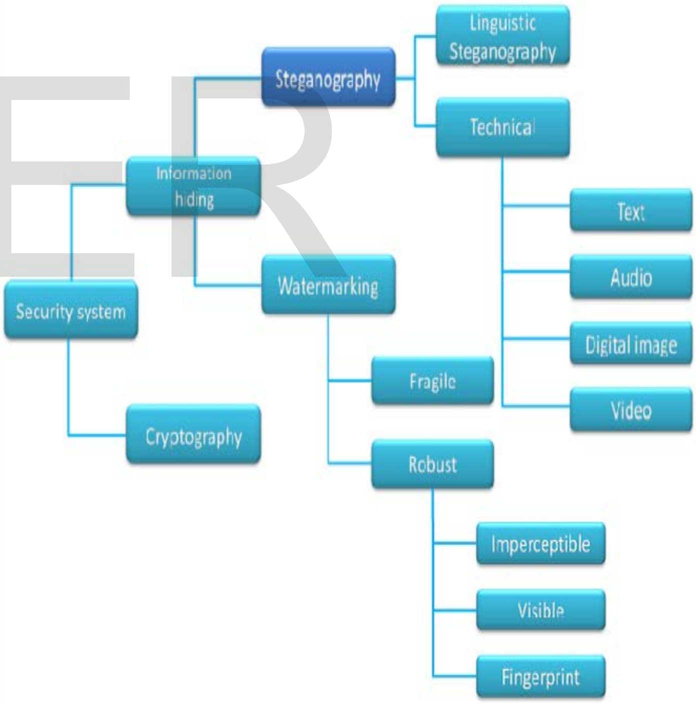

Figure 2: Steganography in security domain

While steganography can be achieved using any cover media, we are concerned with hiding data in digital images. The features expected of a stego-medium are imperceptibility and robustness, so that the secret message is known only to the intended receiver and also the stego-medium being able to withstand attacks from intruders. The amount of secret message embedded should be such that it doesn’t reduce the quality of the stego image. Steganography will hide the message so there is no knowledge of the existence of the message in the place [2].Secret message between two parties can also be communicated covertly using steganographic techniques, which hides the information without raising the attention of the third party. In addition to security-related application, other interesting applications such as hyperlink and metadata insertion are utilized to enrich the image content [3]. There is currently no more secured steganography system which can resist all steganalysis attacks such as visual attack, statistical attack (active and passive) or structural attack. Any steganographic system is expected to work with a high embedding capacity, imperceptibility, and stego image quality. To achieve all of these requirements we have used morphing for hiding image data. Morphing is a process of generating the intermediate images from the source image to the destination image. Source image gradually fade towards the destination image by generating intermediate frames. Intermediate images contain some part of the source and some part of the destination image. This feature helps to hide any source or destination image between the selected intermediate images by using morphed steganography.

Essentially, the information-hiding process in a steganographic system starts by identifying a cover medium's redundant bits (those that can be modified without destroying that medium's integrity) [4]. The embedding process creates a stego medium by replacing these redundant bits with data from the hidden message. Modern steganography‟s goal is to stay its mere presence undetectable, but steganographic systems, thanks to their invasive nature, leave behind detectable traces within the cover medium. Although secret content is not discovered, the very existence of it is: modifying the cover medium changes its statistical properties, thus eavesdroppers can notice the distortions within the resulting stego medium‟s statistical properties. The strategy of finding these distortions is named statistical steganalysis. The purpose of steganography is to hide the presence of communication while the purpose of cryptography is to make the communication incomprehensible by modifying the bit streams using secret keys. The advantage of steganography, over cryptography is that the attackers are not attracted towards communicating messages between sender and receiver while the encrypted messages attract the attackers. Steganalysis is a method of detecting the message hidden in a cover media and to extract it. Changes will be apparent in the statistical property of image if the secret message bits are inserted in image. The strength of the steganography is measured by steganalysis. RS steganalysis is one of the most reliable steganalysis which performs statistical analysis of the pixels to successfully detect the message hidden in the image. However, steganography method to detect the presence of secret message by RS attack/analysis is difficult in case of color images. Retention of visual quality of the image is also imperative. It is worth to note that genetic algorithm optimizes security and also the quality of the image.

II. STEGANOGRAPHY FOR MULTIMEDIA DATA COPYRIGHT PROTECTION SURVEY

In electronic commerce of multimedia contents, merchants sell products in electronic format. These contents can be copied very easily and without quality loss. When multimedia contents are sold to possibly dishonest buyers that may copy and redistribute them, an intellectual property rights problem arises which forces such contents to be protected. Copy prevention solutions have proven ineffective, so other solutions must be deployed. A failure example of one of such systems can be found. Copy detection is the most promising solution. It is based on hiding an imperceptible mark in the product before selling it. This mark will keep embedded in all copies and future recovery from illegal copies will allow proving ownership of the product (watermarking) or trace the dishonest user who has began redistribution (fingerprinting). To imperceptibly embed a mark in a product, copy detection techniques use steganography [5].

Steganography is the art of hiding a secret message within a larger one in such a way that third parties cannot discern the presence or contents of the hidden message.

There are two kinds of marks, depending on the information they carry: watermarks and fingerprints:

Watermark: The mark contains information about the owner of the content it is embedded in, so all copies carry the same embedded mark. Future retrieval of this mark allows ownership to be proved.

Fingerprint: The mark contains information about the buyer who has bought a certain copy of the product. In this way, all copies sold to different buyers carry a different embedded mark.

Later recovery of this mark from illegally redistributed copies allows the dishonest buyer who permitted redistribution of her copy to be identified. A copy detection scheme consists of two algorithms: mark embedding and mark recovery.

A general mark embedding procedure is depicted in Figure 2.1. It consists of an algorithm that takes as input the original object X, the mark M to be embedded and a secret key K only known to the merchant, and generates the marked object X0 as output.

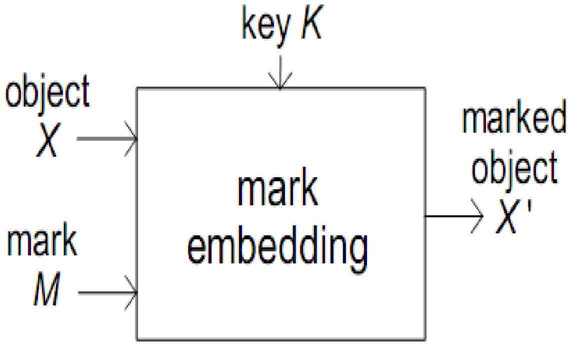

Figure 2.1: Mark embedding procedure.

A general mark recovery procedure is depicted in Figure 2.2. It takes as input a (probably) marked object ^ X, the secret key K and possibly other information depending on the specific algorithm. The procedure generates as output a Boolean value indicating whether a mark has been found or not, and depending on the scheme, the recovered mark ^ M.

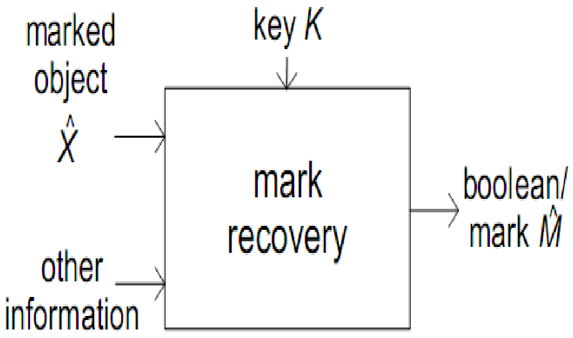

Figure 2.2: Mark recovery procedure.

III. Different Criteria for Evaluation of Image Steganography

The image steganography have different strong and weak points and it is important to ensure that one uses the most suitable algorithm for an application. All steganographic algorithms have to comply with a few basic requirements. The most important requirement is that a steganographic algorithm has to be imperceptible. The authors propose a set of criteria to further define the imperceptibility of an algorithm. These requirements are as follows:

- **Invisibility –** The invisibility of a steganographic algorithm is the first and foremost requirement, since the strength of steganography lies in its ability to be unnoticed by the human eye. The moment that one can see that an image has been tampered with, the algorithm is compromised
- **Payload capacity –** Unlike watermarking, which needs to embed only a small amount of copyright information, steganography aims at hidden communication and therefore requires sufficient embedding capacity.
- **Robustness against statistical attacks –** Statistical steganalysis is the practice of detecting hidden information through applying statistical tests on image data. Many steganographic algorithms leave a ‘signature’ when embedding information that can be easily detected through statistical analysis. To be able to pass by a warden without being detected, a steganographic algorithm must not leave such a mark in the image as be statistically significant.
- **Robustness against image manipulation –** In the communication of a stego image by trusted systems, the image may undergo changes by an active warden in an attempt to remove hidden information. Image manipulation, such as cropping or rotating, can be performed on the image before it reaches its destination. Depending on the manner in which the message is embedded, these manipulations may destroy the hidden message. It is preferable for steganographic algorithms to be robust against either malicious or unintentional changes to the image.
- **Independent of file format –** With many different image file formats used on the Internet, it might seem suspicious that only one type of file format is continuously communicated between two parties. The most powerful steganographic algorithms thus possess the ability to embed information in any type of file. This also solves the problem of not always being able to find a suitable image at the right moment, in the right format to use as a cover image.
- **Unsuspicious files –** This requirement includes all characteristics of a steganographic algorithm that may result in images that are not used normally and may cause suspicion. Abnormal file size, for example, is one property of an image that can result in further investigation of the image by a warden.

IV. Literature Survey

In this paper [6], author has proposed a new method based on tunable visual image quality and data lossless method in spatial domain based on a genetic algorithm (GA). The most important proposal of that technique is modeling the steganography difficulty as a search and optimization problem. Here author has make an effort to get best place for embedding modified secret data in host image to accomplish high level of protection. The process of embedding is achieved in two most important steps; initially they modify secret bits and then to embed it into host image. Due to hosting image in different places in defined by order of scanning host pixels and starting point of scanning and best LSBs of each pixel. However several techniques have been suggested for image steganography, restricted studies have been done on metaheuristic-based image steganography and these efforts could not present logical reasons for benefit of their techniques. An experimental result shows that in comparison with existing accepted steganography methods, demonstrate that the proposed algorithm not only accomplishes high embedding capacity but also improves the PSNR of the stego image.

Here author [7] has presents the application of wavelet transform and genetic algorithm (GA) in a new steganography method. Here they try to provide work for a GA based mapping function to embed data in discrete wavelet transform (DWT) coefficients in 4 * 4 blockson the wrap image. The optimal pixel adjustment process (OPAP) is useful after embedding the message. Here they try to utilize the frequency domain to get better the strength of steganography and then they implement GA and OPAP to obtain an optimal mapping function to condense the difference error between the cover and the stego-image, consequently improving the hiding capacity with low distortions. An experimental result shows that in comparison reveal that the new method do better than adaptive steganography technique based on wavelet transform in expressions of PSNR and capacity, 39.94 dB and 50% correspondingly.

A new morphed steganographic algorithm is proposed [8] in this paper. Basically the image security is a difficult problem in now-a- days. So here author using Steganography technique for hiding secret data in cover medium. The Least Significant Bit is a typical Steganographic technique that has several restrictions. The drawbacks are less capability to hide from view data, reduced stego image quality, and imperceptibility. Here author has to focuses on these drawbacks and new steganographic algorithm is proposed based on the morphing conception is being used for image steganography to overcome these drawbacks. The PSNR and standard deviation are well thought-out as determine to get better stego image quality and morphed image selection, correspondingly. The stego keys are produced during the morphed steganographic embedding and extracting procedure. Stego keys are employed to embed and remove the secret image. As compare on experimental results with existing method which is based on hiding capacity and PSNR using proposed algorithm accomplishes an enhance in hiding capacity, stego image quality, and imperceptibility. The experimental results were compared with state of the art steganographic techniques.

In this proposed work [9], here they studied the steganographic standard of data hiding in usual digital images. This proposed system presents a new method to increase the data hiding capacity and the imperceptibility of the image after embedding the secret message. In proposed work Optimal Pixel Adjustment Process also useful to minimize the error difference between the wrap and stego image. By this effort best effects have been acquired as compared to offered efforts. The proposed steganography model decreases the embedding error and presents higher embedding capacity. Detection of message survival will be very inflexible for those stego images that manufactured using the proposed technique. Experimental result shows the highest embedding capability and security against Reversible Statistical attack.

Chen and Lin [10] propose a new steganography technique which embeds the secret messages in frequency domain to show that the PSNR is still a satisfactory value even when the highest capacity case is applied. By looking at the results of simulation, the PSNR is still a relaxed value even when the highest capacity is applied. This is due to the different characteristics of DWT coefficients in different sub-bands. Since, the most essential portion (the low frequency part) is kept unchanged while the secret messages are embedded in the high frequency sub-bands (corresponding to the edges portion of the image), good PSNR is not a imaginary result. In addition, corresponding security is maintained as well since no message can be extracted without the “Key matrix” and decoding rules.

Amitav Nag, Sushanta Biswas, Debasree Sarkar and Partha Pratim Sarkar [11] present a technique for image steganography based on DWT. This paper presents a novel technique for Image steganography based on DWT, where DWT is used to transform original image (cover image) from spatial domain to frequency domain. First, two dimensional Discrete Wavelet Transform (2-D DWT) is performed on a gray level cover image of size M × N and Huffman encoding is performed on the secret messages/image before embedding. Then each bit of Huffman code of secret message/image is embedded in the high frequency coefficients resulted from Discrete Wavelet Transform. Image quality is to be improved by preserving the wavelet coefficients in the low frequency sub-band also.

J. K. Mandal et al. present another GA-based algorithm termed DEGGA. Focus in this method is on large amount of hidden data and the results are compared with another method by Ran- Zan et al. [12]. In Mandal method, large volume of message/ image is embedded in spatial domain using 3 x 3 masks from the source image. Four bits of the secret message / image is embedded per byte of the source image onto the rightmost 4 bit of each pixel. Mutation is applied on the embedded image. Also, a method of bit handling is applied to keep the fidelity high. In the process of embedding dimension of the secret message / image followed by the content of it. Reverse process is followed during decoding. Genetic algorithm is used to enhance a security level. Various statistical parameters computed that are compared with the Ran- Zan et al. method shows that proposed DEGGA obtained better results in terms of PSNR. Proposed method use gray scale image for secure message transmission. An authenticating image of size m x n is chosen as secret message. The size of the host image is p x q. Input: Host image of size pxq, authenticating image of size pxq. In follow, embedding algorithm is listed. Output of algorithm is embedded image of size pxq. The purpose is inserting the authenticating image (secure message) bitwise into the source image [13].

V. Conclusion

Although only some of the main image steganographic techniques were discussed in this paper, one can see that there exists a large selection of approaches to hiding information in images. GA utilized to acquire an optimal mapping function to lesser the error difference between the cover and the stego image and use the block mapping method to preserve the local image properties. As, also to increase the hiding capacity of the algorithm in comparison to other methods.

References

[1] Masoud Nosrati, Ronak Karimi, Mehdi Hariri. Embedding Stego-Text in Cover Images Using linked List Concepts and LSB Technique. World Applied Programming, Vol (1), No (4), October 2011. 264-268.

[2] Masoud Nosrati, Ronak Karimi, Mehdi Hariri. An introduction to steganography methods. World Applied Programming, Vol (1), No (3), August 2011. 191-195

[3] Tew, Y., & Wong, K. (2014, Feb). An overview of information hiding in H.264/AVC compressed video.IEEE Transactions on Circuits and Systems for Video Technology, 24(2), 305 - 319.

[4] R.J. Anderson and F.A.P. Petitcolas, “On the Limits of Steganography”, J. Selected Areas in Comm., vol. 16, no. 4, 1998, pp. 474–481.

[5] S. Katzenbeisser and Fabien A.P. Petitcolas. Information Hiding:techniques for steganography and digital watermarking. Artech House. ISBN 1-58053-035-4. 2000.

[6] Hamidreza Rashidy Kanan , Bahram Nazeri, "A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm" Expert Systems with Applications 41 (2014) 6123–6130

[7] Elham Ghasemi, Jamshid Shanbehzadeh, and Nima Fassihi, "High Capacity Image Steganography Based on Genetic Algorithm and Wavelet Transform"

[8] Anant M.Bagade* and Sanjay N.Talbar, "A High Quality Steganographic Method Using Morphing" J Inf Process Syst, Vol.10, No.2, pp.256~270, June 2014.

[9] Jyoti, Md. Sabir, "More Secured Steganography Model with High Concealing Capacity by using Genetic Algorithm, Integer Wavelet Transform and OPAP" International Journal on Recent and Innovation Trends in Computing and Communication, ISSN 2321 – 8169 Volume: 1 Issue: 4 MAR 2013.

[10] Po-Yueh Chen and Hung-Ju Lin, "A DWT Based Approach for Image Steganography", International Journal of Applied Science and Engineering 2006. 4, 3: 275-290.

[11] Amitav Nag, Sushanta Biswas, Debasree Sarkar and Partha Pratim Sarkar, "A novel technique for image steganography based on DWT and Huffman encoding", International Journal of Advances in Image Processing, Vol. 2, Special Issue 1, Part 2, 2011.

[12] Ran-Zan Wang, Chi- Fang Lib, and Ja- Chen Lin, "Image hiding by optimal LSB substitution and Genetic algorithm", 2001 Pattern Recognition Society. Published by Elsevier Science Ltd

[13] J. K. Mandal, A. Khamrui. A Data Embedding Technique for Gray scale Image Using Genetic Algorithm (DEGGA). International Conference on Electronic Systems (ICES-2011).