A Survey on Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture

Honey Mol M
M.Tech student
Department of Computer Science and Engineering
Mohandas College of Engineering
Anad, Trivandrum

Prof.Mrs.Reji P.I
Department of Computer Science and Engineering
Mohandas College of Engineering
Anad, Trivandrum

Abstract— **Many of the binary image steganographic techniques only consider the flipping distortion according to the HVS(Human Visual System), which will be not secure . Here, a binary image steganographic scheme is to minimize the embedding distortion on the texture . To extract the complement, rotation, and mirroring-invariant local texture patterns (crmiLTPs)from the binary image . The weighted sum of crmiLTP changes when flipping one pixel is then used to measure the flipping distortion corresponding to that pixel. By testing on simple binary images and the new image data set, the results shows that the proposed scheme can well describe the distortions on both visual quality and statistics.This scheme generates the cover vector by dividing the scrambled image into super pixels. Experimental results show that the proposed scheme can achieve statistical security without degrading the image quality or the embedding capacity. In this paper describes survey on image steganographic techniques and steganographic techniques used with different cryptographic algorithms, to provide extra layer of Security.**

***Keywords*— Binary image, steganography, complement,rotation, and mirroring-invariant local texture pattern(crmiLTP), flipping distortion measurement**

I. INTRODUCTION

The word "Steganography" is a Greek word which means that "covered" OR Steganography is an art and science of encapsulating secret information behind the cover medium. Cover medium, in the sense that multimedia content like digital images, audio files or video files. The aim of data hiding is to hide the existence of communication.

Nowadays, computers and internet has become important parts of our life. Information security is the most important concern in any communication. There are several security attacks related to information security and many of techniques has been implemented to prevent such type of attacks. Data hiding is related field to information security. Data hiding can be achieved by using Digital Steganography. Digital Steganography is art of encapsulating secret messages behind the innocent looking digital media.

In the spatial domain, message bits are embedded by directly flipping pixel values in a binary image. Unlike grayscale images, a pixel in binary images uses two states: black (1) and white (0). As a result, distortions on binary images are easily detected by human eyes. To deal with this problem, steganographic schemes suggest constraining the embedding to the portions of images that are difficult to be noticed. Some scheme uses the boundary to find more suitable pixels for embedding message bits, whereas the others divided the cover image into overlapped or non overlapped blocks and found the most suitable flipping location in each block. By employing 2×2 size blocks and double processing, the scheme presented in used nearly all the shifted edges to embed message bits and hence achieved a large payload. Matrix embedding is commonly employed to achieve a high embedding efficiency. Filler used a practical near optimal matrix embedding, syndrome-trellis code (STC), to embed near the capacity distortion bound with respect to the specified distortion measurement. Prior works also supported the priority of STC.

The mentioned scheme measures the embedding distortion according to the human visual system. Therefore, the yielded stego images present high visual qualities and usually cannot be differentiated from the cover images by human eyes. The adversary may reveal the secrets with the assistance of steganalyzers. To make a steganographic scheme secure, an proper way is to model the image statistic and decrease the embedding impact on that model .Noting that binary images commonly represent the texture here uses the texture model to measure the embedding distortion. Broadly speaking, there are three types of methods describing the texture: geometry based , statistic based, and model based methods. In the proposed measurement, the first and second types are joined to explain the texture with respect to both spatial structure and statistical distribution. That is, first extract the local texture pattern (LTP) as the texture primary. The histogram of LTPs is then used to describe the texture distribution. The LTP is motivated by the concept of the local binary pattern (LBP) , which has been successfully applied in texture classification , face detection , steganalysis etc... Since binary images has different visual appearance compared with grayscale images, an extension of the LBP, the complement, rotation, and mirroring-invariant local texture pattern (crmiLTP), is developed to be better applied in binary image

steganography. The texture region is more suitable for steganography.So, it is expected that a good stego system can be achieved in the texture model.

Here, a spatial domain based binary image steganographic scheme is proposed. The scheme reduces a novel flipping distortion measurement which considers both Human Virtual System and statistics. This measurement uses the weighted sum of crmiLTP changes to measure the flippability of a pixel. The weight value corresponding to each crmiLTP is set according to that pattern's sensitivity to the embedding distortion. To calculate the sensitivity, a collection of generalized embedding simulators are organized to yield stego images with different distortion types and strengths. In the embedding phase, STC is employed to reduce the flipping distortion. To delete the unexpected flipping incurred by STC, the concepts of scrambling and superpixels are used to guarantee that flippable elements occupy usually in a cover vector. By incorporating the new distortion measurement with the STC framework, the proposed steganographic scheme presents a better performance compared with other works.

II. LITERATURE SURVEY

[1]Yu-Chee Tseng,Yu-Yuan Chen, and Hsiang-Kuang Pan proposed in, "A secure data hiding scheme for binary images", enhancement in the image hiding quality and hiding capacity, author presented a novel scheme which can hide a some amount of data by changing number of bits in the original binary image using secret keys as binary matrix and an integer weight matrix. The operator XOR is used so that the keys are not compromised. Another function of the weight matrix is to intensify the data-hiding capacity.

[2]S.-C. Pei and J.-M. Guo proposed in, "Hybrid pixel-based data hiding and Blockbased Watermarking for error-diffused halftone images" that digital halftoning is a technique for improving graylevel images into two-tone binary images. These images can favour the original images when observing from a distance by the human visual system. Techniques in the first classification embeds invisible binary data into halftone images, which further can be recovered by scanning and applying some extraction algorithms. Methods in the second category embed hidden visual patterns into two or many halftone images so that it can be recognised directly when the halftone images are covering each other. Author is using a composite method of combining noise- balanced error diffusion (NBEDF) data hiding and kernels-alternated error diffusion (KAEDF) watermarking into one or many error-diffused images.

[3]T.-Y. Liu and W.-H. Tsai in, "A New Steganographic method for data hiding in Microsoft Word document by change tracking technique" proposed, the basic idea of technique is to degrade the contents of a cover document D to arrive at another document D' by embedding a secret M message in D during the transformation process. The degradation initiates errors into the degenerated document D' such that the degraded document appears to be a introductory work by a virtual author A'. A stegodocument is then produced from D' by revising D' back to D with the changes being found, making it appear as if author A is correcting the errors in D'. On the other hand, by making use of the change tracking data in the stegodocument , a recipient B of S can easily recover the original document D as well as the degenerated document D' from both of which the embedded information can be extracted. In the embedding place the message bits are embedded using Huffman code alongwith Message Embedding by Text Degeneration and Revision algorithm. The change tracking information comprised of the stegodocument S allows simple recovery of the original document D and the degenerated document D', from both of which the embedded message can be extracted using message extraction algorithm.

[4] H. Yang and A. C. Kot in , "Pattern-based data hiding for binary image authentication by connectivity-preserving" proposed, Evaluation of the "flippability" of a pixel to gain good visual quality of the watermarked image. Handling the "uneven embeddability" of the image by embedding the watermark only in "embeddable" blocks. Study of the features in flipping pixels in binary images to attain blind watermark extraction. Exploring different ways of separating the image to achieve larger capacity. Examination on how to locate the "embeddable" pixels in the watermarked image to assimilate cryptographic signature to achieve higher security. A novel blind data hiding scheme based on connectivity-preserving of pixels in a local neighborhood for binary images authentication was proposed. A window of size 3x3 is hired to assess the "flippability" of a pixel in a block. The "uneven embeddability" of the host binary image is handled by embedding the watermark in those "embeddable" blocks based on the three transition criteria. A smaller block size is chosen in order to increase the data hiding capacity.

[5] E. Dagar and S. Dagar present the steganography technique for color RGB images to improve the security level of data transfer through the internet. 24 bit RGB image is utilized as cover image to embed secret data in red, green and blue pixels. X-Box mapping is used and several boxes contain 16 different values. Here "X" represent any integer number from 0 to 9. After this values saved in X-Boxes are mapped with LSBs of carrier image. It is very difficult for the attacker to extract the secret information because they make use of mapping. Thus this mapping provides high level of security to hidden information. PSNR value is also calculated and it has high PSNR value which leads to greater stego image quality.

[6]G. Prashanti and K. Sandhyarani have done survey on recent achievements of LSB based image steganography. In this survey authors discuss the improvements that enhance the steganographic results such as high robustness, high

embedding capacity and un-detectability of hidden information. Along with this survey two new techniques are also proposed. First technique is used to embed data or secret messages into the cover image and in the second technique a secret gray scale image is embedded into another gray scale image. These techniques use four state table that produce pseudo random numbers. This is used for embedding the secret information. These two methods have greater security because secret information is hidden on random selected locations of LSBs of the image with the help of pseudo random numbers generated by the table.

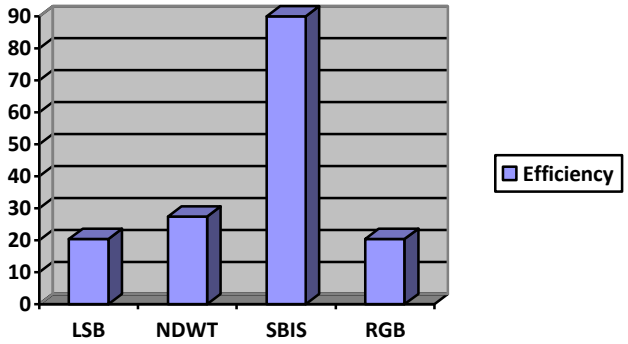
[7]Savita Goel proposed a new method of embedding secret messages in cover image using LSB method using different progressions. Authors compare the quality of stego image with respect to cover image using number of image quality parameters such as Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), histograms and CPU time, Structure Similarity (SSIM) index and Feature Similarity Index Measure (FSIM). Their study and experimental results shows that their proposed method is fast and highly efficient as compared to basic LSB methods.

[8]Della Baby proposed a "Novel DWT based Image Securing method using Steganography". In their work new steganography technique is prosed in which multiple RGB images are embedded into single RGB image using DWT steganographic technique. The cover image is divided into 3 colors i.e. Red, Green and Blue color space. These three color spaces are utilized to hide secret information. Experimental results obtained using this system has good robustness. Value of PSNR and SSIM index have been used by authors to compare the quality of stego image and original cover image. Proposed method has good level of PSNR and SSIM index values. Authors have found that their experimental results are better than existing approaches and have increased embedding capacity because of data compression. So security is high with less perceptible changes in stego image.

[9]M. Nusrati have done study on heuristic genetic algorithm based steganographic method for hiding secret information in a cover image. This method optimally find the appropriate locations in cover image to embed the secret information by focusing on the "before embedding hiding techniques". It tries to make least changes in the bits which lead to minimal modifications in image histogram. To covert the LSBs and secret message to set of blocks, segmentation is done in this genetic algorithm. After this algorithm finds the appropriate locations for embedding, the secret blocks are embedded and it generates the key file which is used during message extraction process.

[10]Bingwen Feng, Wei Lu, and Wei Sun in their paper "Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture"purposed a state-of-the-art approach of binary image steganography. This technique is proposed to minimize the distortion on the texture. In this method of steganography firstly the rotation, complement and mirroring invariant texture patterns are extracted from the binary image. They also proposed a measurement and based on this proposed measurement this approach is practically implemented. Practical results show that proposed steganographic approach has high statistical security with high stego image quality and high embedding capacity.

III.Experiment Results



Experiment result shows that the Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture scheme achieves the best security. As a result, the proposed scheme can provide additional steganographic security without degrading the stego image quality.

IV.Conclusion

In this survey exploits the texture property of binary images and propose a secure binary image steganographic scheme by minimizing the distortion on the texture. The proposed complement, rotation, and mirroring-invariant local texture pattern -crmiLTP is suitable of binary image processing and thus can stably describe the local structure of binary image texture. Further, the changes in the crmiLTP distribution show a strong relationship with the detectability of the embedding distortion. Therefore, the proposed flipping distortion scheme is set with the weighted sum of crmiLTP changes, where the weight is consequently assigned on the basis of discrimination power of the crmiLTP histogram. By comparing with traditional Human Virtual System-based approaches, it can be seen that the proposed measurement performs well on both image quality and security.

It is worth noting that, employing statistical model to design distortion measurements may raise the risk of embedding in the "clean" edges, which dramatically reduces the steganographic security in grayscale images. This characteristic provides a reasonable tradeoff between the

image quality and the statistical security in binary images, since distortions not on the boundary are easily to be noticed. At last, a practical steganographic scheme is constructed by combining the proposed flipping distortion measurement with the syndrome trellis code (STC). Experiments on the constructed image dataset have shown that the proposed steganographic scheme can yield more secure stego images with better, at least similar ,image qualities when the same length of message bits are embedded. The crmiLTP and the proposed distortion measurement are extendable for other binary image applications, such as the binary image classification and the assessment of error diffusion methods.

References

[1] Yu-Chee Tseng,Yu-Yuan Chen, and Hsiang-Kuang Pan, "A secure data hiding scheme for binary images" in IEEE transactions on communications, vol. 50, no. 8, august 2002.

[2] S.-C. Pei and J.-M. Guo, "Hybrid pixel-based data hiding and Blockbased Watermarking for error-diffused halftone images",in IEEE transactions on circuits and systems for video technology, vol. 13, no. 8, august 2003.

[3] T.-Y. Liu and W.-H. Tsai, "A New Steganographic method for data hiding in Microsoft Word document by change tracking technique," in IEEE transactions on information forensics and security, vol. 2, no. 1, march 2007.

[4] H. Yang and A. C. Kot, "Pattern-based data hiding for binary image authentication by connectivity-preserving," in IEEE trans. multimedia, vol. 9, no. 3, pp. 475–486, apr. 2007.

[5] E. Dagar and S. Dagar, "LSB based Image Steganography using X-Box Mapping", IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI), **(2014)**, September 24-27, New Delhi, India.

[6] G. Prashanti, and K. Sandhyarani, "A New Approach for Data Hiding with LSB Steganography", Emerging ICT for Bridging the Future - Proceedings of the 49th Annual Convention of the Computer Society of India CSI, vol. 2, Springer (2015).

[7] S. Goel, S. Gupta, and N. Kaushik, "Image Steganography – Least Significant Bit with Multiple Progressions", Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA), vol. 2, Springer (2014).

[8] D. Baby, J. Thomas, G. Augustine, E. George, and N.R. Michael, " A Novel DWT based Image Securing method using Steganography", International Conference on Information and Communication Technologies (ICICT), Procedia Computer Science, vol. 46, (2015).

[9] M. Nusrati, A. Hanani and R. Karimi, "Steganography in Image Segments Using Genetic Algorithm", 5th IEEE International Conference on Advanced Computing & Communication Technologies (ACCT), (2015) February 21-22, Haryana, India.

[10] B. Feng, W. Lu, and W. Sun, "Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture", IEEE transactions on Information Forensics and Security, vol. 10, no. 2, (2015).