ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 8, August 2014

A SECURE DATA EMBEDDING TECHNIQUE IN IMAGE STEGANOGRAPHY FOR MEDICAL IMAGES

Usha B A[1], Srinath N K[2], Narayan K[3], Sangeetha K N[4]

Assistant Professor, Department of CSE, RVCE, Bangalore, India [2]
Professor and Dean PG Studies, Department of CSE, RVCE, Bangalore, India [1]
M.Tech Student, Department of CSE, RVCE, Bangalore, India [3]
Assistant Professor, Department of ECE, JSSATE, Bangalore, India [4]

Abstract: Steganography is an art and science of secure information communication where the secret data or confidential data is hidden in host file. It is used in different useful applications like secure data communication, healthcare and military. Confidential information's are commonly stored in digital media and transmitted via internet due to the rapid growth of internet. If the information's in images are altered then this may lead to wrong assumptions. Certain medical applications require information exchange over an insecure network where a small piece of medical information is modified intentionally for certain illegal purpose which may lead to wrong diagnosis. Therefore protection of integrity, reliability and confidentiality of the secret medical data in images are the important issues. To protect the secret medical information cryptography technique can be used where the secret medical data is altered, even if the attackers get to know the data it won't be of any use without knowing the algorithm. According to the survey not all issues are satisfied by the single method. In this paper a brief introduction is presented later related works followed by proposed algorithm, results and conclusion.

Keywords Medical Image, Steganography, cryptography, data hiding, soft computing, fuzzy logic**.**

I. INTRODUCTION

Handling and processing of secret data are done on high speed internet because of the common use of internet. Complete secret information's are exchanged over internet where the information security plays a major role. To achieve the security there are two approaches one is cryptography and another is Steganography. Cryptography means "secret writing". Steganography is a technique of concealing secret data that needs to be transmitted in digital cover images such that presence of data is hidden from third party other than sender and receiver.

The important factors that need to be considered while designing a Steganographic system are embedding capacity (i.e. number of secret bits that can be embedded per pixel), visual quality of stego o image (i.e. image distortion),security (encryption) and amount of data(compression) shared. It is necessary to achieve high embedding capacity and good visual quality. However, embedding capacity and visual quality are inversely proportional to each other. Thus a compromise made between visual quality and embedding capacity according to the application for which this System is used. Further security in data sending is achieved by encryption method and sending more data can be attained using the compression technique.

Many Steganography schemes for images are proposed. One of the most commonly used techniques is Least Significant Bit (LSB) Steganography in which only the LSB bit planes are replaced with the secret data [1]. Due to the simplicity of the LSB Steganography scheme it is very easy to detect the data by attackers. It is because of the payload embedding which is common for all pixels. To overcome the problem many different technique have been proposed where the payload is different for each pixels.

Some methods are based on MSB bit planes [6] where payload for each pixel is based on its own MSB bits. On top of applying LSB substitution technique, hybrid edge detector methods [4] are used to compute the actual edge pixels where pixels conceal more data in it.

Nowadays, many intelligent algorithms based on soft computing, such as Fuzzy Logic (FL), Adaptive Neural Networks (ANN), Genetic Algorithms (GA) are being used in Steganography to achieve robust and optimal solutions.[18] proposed a secure Steganography method which is based on fuzzy inference system which improves the payload for each pixels.[19] proposed a scheme for compressing and de-compressing the image using fuzzy coder and decoder. The major contribution of this paper focuses on providing a survey on different algorithms that are used so far to hide secret data in images like grey scale, colour or medical images.

II. RELATED WORKS

There are few characters which describe the pros and cons of the steganography system which are capacity and robustness. Both these characters depend on each other and they are inversely proportional to each other. Any steganography system pros and cons are decided based on this. Very first LSB substitution algorithm was proposed by C C Chang et.al [1] which replaces the LSB bit planes of the image. Later many algorithms are proposed which are still based on LSB bit planes. Keeping these parameters as base many authors have developed different algorithm were the embedding is in the LSB bit plane. Dah Jung CHUNG et.al [2] proposed a reversible data hiding algorithm which prevents the distortion of the stego image after the extraction process. This algorithm increases the Quality and reduces the distortion. Edlira Martiri et.al [3] proposed a medical image authentication method using the Steganography algorithm. Major advantage is reduces confusion between patients data. Nagham Hamid et.al [4] proposed a region based Steganography technique where the data is embedded in the robust region of the image. First SURF (Speed-Up Robust Feature) technique is used to find the characteristic robust region.. After this one level inverse DWT is applied to get stego square image. The advantages are visual quality and the accurate retrieval is achieved even in the presence of lossy compression and noise. Siva Jana Kiraman et.al [5] proposed a gray block embedding method, in this method the LSB bits are modified based on the MSB bit plane. The proposed scheme increases the embedding capacity and security by the complexity. Prabakaran G et.al [6] aims to develop a Steganography scheme to secure the medical digital images. The proposed method is based on the integer wavelet transform and the Arnold transform the algorithm increases the capacity and the quality. Kavitha et.al [7] presented a steganographic scheme using LSB algorithm to protect the secret message by using password for the authentication process. The scheme is used to enable secret communication and used in military applications. Roszcati Ibrahim et.al [8] proposed a Steganography imaging system for hiding data inside an image. The system provides two layer of security to provide data protection. The method improves the security and the image quality. Vijay Kumar Sharma et.al [9] describes an improved LSB substitution method for hiding image inside an image with minimizing the detection. The proposed method makes use of First Component Alteration technique for Steganography where only the Blue component bits are modified. This method can be used for both grey scale and colour images. The advantage is that the same size secret image can be embedded inside the cover image.

Nowadays many authors have proposed steganography system based on emerging soft computing technique like Fuzzy Logic, Genetic Algorithm and Neural Networks. Mahdi Hasssani Goodarzi et.al [10] proposed a Steganography algorithm with the combination of the fuzzy logic which increases the embedding capacity and the security. The messages are encrypted using DES algorithm before embedding. The same process is followed during extraction process. The scheme improves the quality and capacity. Shuenn-Shyang Wang et.al [11] proposed a method using fuzzy predictors for reversible data hiding. The fuzzy predictors use the correlation among the neighbouring pixels of the image. The proposed scheme reduces the distortion. Mazhar Tayel et.al [12] aims to produce a full capacity stego image system with the help of hybrid fuzzy decomposition algorithm. Some of the concepts used are Steganography, fuzzy logic and discrete wavelet transform (DWT) and modified weight function. The advantage of the system is the full capacity usage of the cover image high robustness. Sara Sajasi et.al [13] proposed a fuzzy inference system based image Steganography scheme which makes use of local features of the image to improve the payload that can be embedded on the cover image. This new scheme produces the high quality stego image. Zahra Toony et.al [14] proposed image hiding method based on fuzzy coding and decoding. In this method the fuzzy coder and decoder are used to compress and decompress the secret image. Jun Kong et.al [15] proposed a novel content-based information hiding scheme to protect the transmission of secret data with improved security and secrecy. Firstly in the scheme the secret data is encrypted by using the chaotic maps, later the cover image is segmented using watershed algorithm and classified using fuzzy c-means clustering algorithm. After clustering, each regions feature is extracted by calculating the entropy. A threshold is maintained during embedding, if the entropy is lower than the threshold then 2 bits are embedded if it is more than 4 bits are embedded. In the extraction process is same as embedding. The scheme overcomes the dis-advantages of block based Steganography technique. Qingzhong Li et.al [16] presents a Steganography method based on sign embedding and fuzzy classification to minimize the distortion of secret image. The proposed scheme produces good quality stego image and increases the payload.

III.PROPOSED METHOD

I. METHOD 1

Siva Janakiraman et.al [6] proposed a gray block embedding method, in this method the LSB bits are modified based on the MSB bit plane. In the embedding process the gray image is divided into the 4*4 blocks further this is divided into 2*2 blocks. The embedding process is done in 2 phase outer embedding and the inner embedding. In the outer a reference point is found in each of the 2*2 blocks and based on the MSB bit plane of then reference point in the 2*2 block the secret data is embedded into the other pixels. In the inner embedding the values of the reference point has been changed to increase the security. In the extracting process the reference point value are bought back and based on the reference point value the actual value are extracted from the stego image. The proposed scheme increases the embedding capacity and security but we think that the complexity in embedding uses most of the CPU cycles during embedding and extracting and some of the pixel are not used for embedding like reference pixels.

So we propose an algorithm by modifying the algorithm in [6].

DATA EMBEDDING PHASE:

In the embedding process the medical image and the secret data is selected. Later each pixel value of the medical image is used for embedding data. We embed the data directly based on the MSB bit planes of each pixel. If the MSB bit plane is 0 we embed 2 bits if it is 1 then we embed 3 bits. The security is provided by encrypting the message before embedding it into cover image.

DATA EXTRACTION PHASE:

The secret message from the stego image can be retrieved only by using the extracting algorithm. In the extracting process the pixel value of stego image is used and MSB bit plane of each stego pixel is verified to extract the bits from the LSB. If the MSB is 0 then 2 bits are extracted or if it is 1 then 3 bits are extracted.

By the proposed complexity of embedding and extracting is reduced and enhanced security is maintained with the help of cryptography.

II. METHOD 2

Shuenn-Shyang Wang et.al [11] proposed a method using fuzzy predictors for reversible data hiding. He defines predicted functions based on the neighbouring pixels and also defines the Fuzzy Membership Functions.

DATA EMBEDDING PHASE:

In the embedding process the medical image and the secret data is selected. Secret data is converted to binary form. We make use of predicted function and Fuzzy membership function and calculate the predicted errors. For this predicted errors the histogram is calculated and the peak value is found. In the histogram the value greater than the peak is incremented by 1. Based on the peak value the binary message is embedded into cover image. If the message bit is 1, the peak value is incremented by 1 and if the message bit is 0, the peak value is kept as it is. Later stego image is constructed and sent to receiver.

DATA EXTRACTION PHASE:

The secret message from the stego image can be retrieved only by using the extracting algorithm. Using the same predictor and membership function the predicted errors are calculated. For the predictor errors a histogram is constructed. The sender has to send the peak value for extracting. The receiver after receiving the peak value can extract the data. If the predictor error value is equal to sender's peak value then 0 is extracted and if it is peak+1 then 1 is extracted from the error.

The algorithm is secure because extracting of data is completely depends on the peak value sent by sender. So until no one gets this peak value the secret data is safe.

IV. PERFORMANCE ANALYSIS AND RESULTS

The factors to be considered while designing a steganography system are:

1. Number of bits to be embedded.
2. Visual quality of the image.
3. Less distortion in the embedded cover image compared to original image.

The performance is evaluated based on PSNR (Peak Signal to Noise Ratio) which defines the quality of the image. The PSNR is defined as follows.

$$PSNR= 10 \log_{10}(255^2/MSE) \ dB,$$

Where MSE is Mean Square Error between the original image and the stego image. The MSE is defined as follows.

$$MSE = (1/ (MxN)) \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (Rij-Kij)^2.$$

Where Rij and Kij are pixel values of original image and the stego image. MxN represents all the pixel values of the image. Larger the PSNR value better the quality which means stego image will be almost similar to original image. The PSNR value for the percentage of image used is shown in the form of table and graph.

TABLE 1
THE PERCENTAGE OF IMAGE USED AND THE RESPECT IVE PSNR RATIOS.

% OF IMAGE USED	PSNR for Image 1024*768 by MSB System in dB	PSNR for Image 1024*768 by FUZZY System in dB
10	54.665	87.213
20	52.664	80.735
30	49.892	69.374
40	48.644	63.329
50	47.765	53.289
60	46.881	51.452
70	46.213	50.574
80	45.639	50.115
90	45.128	49.581
100	44.672	48.669

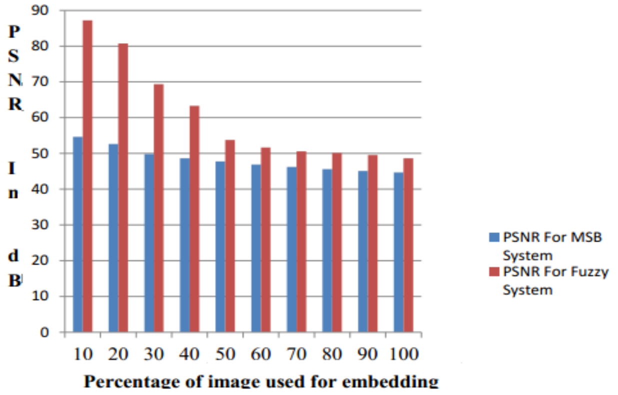

Fig. 1. Graph showing relation between PSNR along y-axis and percentage of image used for embedding along x-axis.

V. CONCLUSION

In this paper an analysis is presented for different image Steganography techniques which can be employed to protect the secret information. Many existing techniques have been employed in recent years for the protection of secret information. In this paper an overview of different algorithm for protecting, improving the embedding capacity and quality of stego image is presented and also the proposed algorithm, comparative study and encoding and decoding techniques.

ACKNOWLEDGMENT

It is our privilege to acknowledge thanking all the department personals and sponsors who gave us an opportunity to present a paper at this level. We wish to place our deep sense of gratitude to all reference papers authors for their beneficial papers, books and websites etc.

REFERENCES

[1] C.C. Chang, M.H. Lin, and Y.C. Hu , "A fast and secure image hiding scheme based on LSB substitution," International journal of pattern recognition and artificial intelligence, vol. 16, no. 4, pp. 399–418, June 2002

[2] Dah Jung CHUNG, Hong Lin JIN and Yoon Sik CHOE "Reversible Data Hiding Algorithm for High Quality Stego Images", IEEE, pp: 251-254, 2011.

[3] Edlir Martiri, Artur Baxhaku and Ezmolda Barolli "Steganographic Algorithm Injection in Image Information Systems used in Healthcare Organizations", IEEE, pp: 408-411, 2011.

[4] Nagham Hamid, Abid Yahya, R. Badlishah Ahmad, Osamah Al-Qershi, "Characteristic Region Based Image Steganography Using Speeded-Up Robust Features Technique", 2012 International conference on future computer networks, IEEE , pp: 141-146, 2012.

[5] Siva Janakiraman, Suriya.N, Nithiya.V, Badrinath Radhakrishnan, Janani Ramanathan and Rengarajan Amirtharajan, " Reflective Code for Gray Block Embedding," Proceedings of the International Conference on Pattern Recognition, Informatics and Medical Engineering,IEEE, pp: 215-220, 2012.

[6] Prabakaran G, Dr. Bhavani R and Rajeswari P. S, "Multi Secure and Robustness for Medical Image Based Steganography Scheme", International Conference on Circuits, Power and Computing Technologies [ICCPCT-], IEEE, and pp: 1188-1193, 2013.

[7] Mrs. Kavitha, Kavita Kadam, Ashwini Koshti and Priya Dunghav, "Steganography using Least Significant Bit Algorithm", IJERA,vol. 2, ISSUE 3, pp: 338-341, 2012.

[8] Rosziati Ibrahim and Teoh Suk Kuan," Steganography Algorithm to hide secret Message inside an Image", Computer Technology and Application, pp: 102-108, 2011.

[9] Vijay kumar Sharma, Vishal shrivastava, "A Steganography Algorithm For Hiding Image In Image By Improved LSB Substitution By Minimise Detection", Journal of Theoretical and Applied Information Technology, vol .36, pp: 1-8,2012.

[10] Mahdi Hassani Goodarzi, Arash Zaeim, and Amir Shahab Shahabi "Convergence between Fuzzy Logic and Steganography for High Payload Data Embedding and More Security", The 6th International Conference on Telecommunication Systems, Services, and Applications, IEEE, pp: 130-138, 2011.

[11] Shuenn-Shyang Wang, Sz-Jiun Fan and Chien-Sung Li, "A New Reversible Data Hiding Based on Fuzzy Predictor", Proceedings of 2012 International Conference on Fuzzy Theory and Its Applications National Chung Hsing University, Taichung, Taiwan, pp: 258-262, 2012

[12] Mazhar Tayel, Alaa Hafez, Hamed Shawky, "A New Hybrid Fuzzy-Decomposed Full Capacity Stego-System", IEEE, pp: 16-20, 2013.

[13] Sara Sajasi and Amir Masoud Eftekhari Moghadam, "A High Quality Image Steganography Scheme Based on Fuzzy Inference System", 13th Iranian conference on fuzzy systems, IEEE, 2013.

[14] Zahra Toony, Hedieh sajedi and Mansour Jamzad," A High Capacity Image Hiding Method Based on Fuzzy Image Coding/Decoding", Proceedings of the 14th International CSI computer conference, IEEE,pp:518-523,2009.

[15] Jun Kong, Hongru Jia, Xiaolu Li and Zhi Qi," A Novel Content-Based Information Hiding Scheme", International Conference on Computer Engineering and Technology, IEEE, pp:436-4401, 2009.

[16] Qingzhong Li, Chen Yu and Dongsheng Chu," A robust Image Hiding Method Based on Sign Embedding and Fuzzy clzssification", Proceedings of the 6th world congress on Intelligent comtrol and Automation, IEEE,pp: 10050-10053,2006.

BIOGRAPHIES

Usha B A. Assistant Professor, Department of CSE, RVCE, Bangalore, India.

Dr. Srinath N K. Professor and Dean PG Studies, Department of CSE, RVCE, Bangalore, India

Narayan K. Mtech Student, Department of CSE, RVCE, Bangalore, India.

Sangeetha K N. Assistant Professor, Department of ECE, JSSATE, Bangalore, India.