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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 6, June 2014

Analysis of Data Embedding Technique in Image Steganography – A Survey

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

Professor and Dean PG Studies, Department of CSE, RVCE, Bangalore, India [1]
Assistant Professor, Department of CSE, RVCE, Bangalore, India [2]
M.Tech Student, Department of CSE, RVCE, Bangalore, India [3]
M.Tech Student, Department of CSE, RVCE, 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 data in images are the important issues. To protect the secret information cryptography technique can be used where the secret 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 survey is made on the data hiding and Steganography methods.

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

Dah Jung CHUNG et.al [2] proposed a reversible data hiding algorithm which prevents the distortion of the stego image after the extraction process. In this algorithm the cover image is divided into 3*3 blocks and by using the statistics of the pixel a key parameter is chosen for each block. A global key parameter is chosen from the minimum value of key parameter from each block. The adaptive modulation algorithm is used in the embedding process and pixel values are modified based on the distance between the centre value of the dynamic range and the actual pixel value. After embedding the pixel value is checked based on the average and the standard deviation value of the neighbour pixel, then the embedding goes on until the pixel values are not in the overflow or the underflow range. To prevent the distortion a small weight

is added to the pixel which has low probability to occur overflow or underflow. In the extraction process the same process is followed where the data is extracted based on the weight and key parameter. This algorithm increases the Quality and reduces the distortion.

Edlira Martiri et.al [3] proposed a medical image authentication method using the Steganography algorithm. The algorithm injects the image metadata, a unique ID generated by the algorithm, patients name, type of image source, name of healthcare organization and date into the image itself. All the text is encoded using AES technique and they are embedded in the region of interest in the image. LSB algorithm is used to embed the data into the image. This paper proposes a scheme for the generation of ID number for the patients. This scheme is the digital signature and the adaption of the Rabin digital signature used to identify false images. The IDs are embedded in the lower part of the image which is the region of interest and this is based on the secret keys. An n-couple of key are generated and half is kept by scheme and other half is given to public. Using these keys they can access the information. Major advantage is reduces confusion between patients data.

Mahdi Hasssani Goodarzi et.al [4] proposed a Steganography algorithm with the combination of the fuzzy logic which increases the embedding capacity and the security. First the edge detection algorithm called hybrid edge detection algorithm is applied on the image. The hybrid edge detection algorithm is the combination of Canny Edge Detection (CED) and the Fuzzy Edge Detection (FED). The HED is formed by applying the logical OR on the CED and FED. The LSB algorithm is applied on the output image. The method divides the image into 3*3 blocks. Assign the first 3 pixels or the row as p1, p2 and p3.the embedding is a follows where p3 acts as a flag and the previous p1 and p2 are embedded based on whether the pervious pixels are edge or not. The messages are encrypted using DES algorithm before embedding. The same process is followed during extraction process. The scheme improves the quality and capacity.

Nagham Hamid et.al [5] 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. The SURF finds the key point in the image; this point is the centre of the region where the data has to be embedded and the Euclidian distance is used to assure that the local region are disjoint. The embedding is done using the discrete wavelet transform domain. The key points generated from SURF are verified to prevent region intersection. From the final list of key points a square region in the image if found and the one level DWT is applied to produce wavelet co-efficient. Based on the coefficient the data is embedded in the content based manner. After this one level inverse DWT is applied to get stego square image. In the extracting phase the initial steps are same as embedding after that the one level DWT is applied to get the coefficient and based on the coefficient the bits are extracted. 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 [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 base o 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 by the complexity.

Prabakaran G et.al [7] 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. In the embedding process the container image is taken and the flip left is applied, a dummy container image is obtained. The patient's medical image is taken and the Arnold transform is applied and scrambled secret image is obtained. This scrambled secret image was embedded into the dummy container image and the inverse IWT was taken to get dummy secret image. This dummy secret image is embedded into the container image and transferred to receiver. The reverse with sub band subtraction is applied to get the actual data in extraction phase. The algorithm increases the capacity and the quality.

Vn Mai et.al [8] proposed a Steganography scheme to have control over the access of the data stored in the ECG (Electrocardiogram). The scheme requires that the patient's data to be stored in a tree structure which consists of leaf node and branch and each node represents a kind of data. Each leaf node or a branch is protected from access by Steganographic keys. The normal Steganography algorithm is used to embed data into ECG. Once data is embedded the data is stored in the public cloud and the data owner can upload some access keys and the interested users can request for keys to cloud server and retrieve some information and if there are some restricted data then the key has to be obtained from owner itself. In the extraction process the user key is compared with the key file on the cloud and only if the key matches the access is allowed. Confidentiality of the patient's information is maintained.

Bremnavas et.al [9] presented a scheme for encryption and decryption of medical data and image using chaotic signals. The data is encrypted twice before transferring it through insecure channel. Firstly LSB algorithm for encryption which is as follows: the medical data is converted to UTF-8 format later the medical images are divided into blocks then the binary data is embedded into the medical images randomly. The reverse is applied in the decryption process. Secondly chaotic algorithm for encryption: the output of the first algorithm is used and the chaotic sequence is generated using logistic map then

converts the image into pixel array and encrypts the image with the logistic sequence signal in the chaotic region to generate encrypted signal. In the decryption process the reverse approach is used and the subtraction of the received encrypted signal with the raw logistic signal is done. Using this scheme the place of data embedded is made unknown to steg-analyst.

Pouria Mortazavian et.al [10] proposed a method for protecting the textual labels on the medical images from unauthorized users. Firstly a template matching algorithm is applied and the text is extracted later the image is reconstructed. To the new image the embedding and the extracting the textual data are done. In the embedding process the textual data is encoded using Error Coding Code(Hamming Code), then the cover image is shuffled in terms of n*n blocks by using a pseudo random sequence which uses a key called password between sender and the receiver. The mean value of the block is modified in the embedding process and the modified value is defined by decision table which generates a mean spectrum for binary symbols. The embedding process is done in two modes based on the threshold values, in the normal mode pixel values are subtracted by one unit and if the modification increases the threshold then the switch mode is applied where the pixel value is increased. The same process is applied in the extraction process with the shared password. As the pixel alteration can't increase more than 2k the quality is maintained.

Kavitha et.al [11] presented a steganographic scheme using LSB algorithm to protect the secret message by using password for the authentication process. There are two phase, firstly cover image and secret data (image , audio or video) are processed by encryption phase where the secret data is embedded to carrier file and this is protected by password, then this is sent to the receiver by web or mail. Secondly at the receiver side the received file is passed to decryption phase where by appropriate use of password the secret data can be revealed. The scheme is used to enable secret communication and used in military applications.

Vinay Pandey et.al [12] presented a method which combines cryptography, data hiding and Steganography for the protection of medical images. Firstly, the original image is encrypted with the stream cipher algorithm to this encrypted image the patient's information is embedded using lossless data embedding technique with the key for security purpose, and then the Steganography is applied. At the receiver end once the message is arrived, extraction process is done in the reverse process in order to obtain original image and the information with the help of the key. The presented method prevents the distortion of the images after the retrieval process.

Shuenn-Shyang Wang et.al [13] proposed a method using fuzzy predictors for reversible data hiding. The fuzzy predictors use the correlation among the neighbouring pixels of the image. In embedding process five fuzzy membership functions (MFs) are defined, based on these MFs the predicted value of each pixel is calculated. The predicted errors are calculated by obtaining the difference between the actual value and the predicted value of pixel. A histogram is generated for the prediction error and based on this histogram the prediction error values are modified slightly to embed data. To obtain the actual embedded data add the predicted values with errors. The reverse is applied at the extraction process. The proposed scheme reduces the distortion.

Mazhar Tayel et.al [14] 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. In this system DWT is applied for both cover image and secret message with the help of fuzzy membership functions. The secret message are compressed and then embedded into the cover image based on weighted function. In the extraction process Inverse-DWT is applied with de-fuzzification to obtain the secret message. The advantage of the system is the full capacity usage of the cover image high robustness.

Vijay Kumar Sharma et.al [15] 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. In the embedding or extracting process a key is used to improve the security. The key is embedded on the initial pixel of the image and the same key is compared at the receiver. To improve the quality of the image the Steganography process is carried out with the help of logic gates. 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.

Vinay Pandey et.al [16] provides a method for secure transmission of medical images with the use of techniques like Steganography, encryption, decryption, de-noising and data hiding. Firstly, the image is embedded with the patient's information using LSB lossless data embedding technique. After embedding the image is encrypted with two share mechanism for security and then Steganography is applied where image is hidden into other cover image. In the receiver side the reverse is applied to get the original image and patient's information.

Roszcati Ibrahim et.al [17] proposed a Steganography imaging system for hiding data inside an image. The system provides two layer of security to provide data protection. The first layer of security is the username and the password for login purpose. The second layer of security is the secret key for data hiding and retrieving which locks and un-locks the secret message. Later the data is embedded inside the image before embedding the secret message it is transferred to text file and compressed into zip file. The zip text file is converted to binary codes, then using the novel steganographic algorithm two bits in of the binary codes are embedded in each of the pixel until the end of the binary co9des. The method improves the security and the image quality.

Sara Sajasi et.al [18] 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. In the scheme there are two process firstly, Adaptive embedding process where certain features of the image are extracted like texture feature, edge sensitivity and brightness sensitivity. Based

on the value produced by the features a fuzzy inference system is build which defines the inference rules where block types are defined and based on the type of block the number of bits to be embedded is decided. Then extracting process is the reverse of the embedding process. Based on de-fuzzification the original data is extracted from the cover image. This new scheme produces the high quality stego image.

Zahra Toony et.al [19] 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. In the proposed method the secret image is divided into blocks and the theses blocks are compressed into smaller blocks using fuzzy coders. A suitable cover image is selected from the database. Selected image is divided into blocks and then the similar blocks from the cover image and the secret image is obtained. This similar blocks in the cover image are later replaced by the secret image blocks with the use of model based Steganography which is based on discrete cosine transform and histogram. In the extraction phase the once the image is extracted from the stego image, fuzzy decoder is used to decompress and get the original secret image.

Jun Kong et.al [20] 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.

Amanpreet Kaur et.al [21] develops a Steganography scheme based on Hybrid Edge Detection (HED) and 2^k correction method. The HED is the combination of fuzzy edge detection and canny edge detection which is used to improve the embedding capacity and 2^k correction method is use improves the quality of the stego image. Any Steganography technique can be used like LSB, Injection, Substitution and Generation. In the embedding process the HED is executed, later LSB is used to encode the bits into the image after that 2^k correction method is used to get the final images. The same is used in the extraction process. The proposed scheme improves the capacity and the quality of the edgy images.

SeungWA HAN et.al [22] proposed a lossless data hiding for image tamper detection. In the proposed scheme the image is divided into blocks and each block features are described using one way hash function (SHA-256) and stored in the same block with data using lossless data hiding technique. During the embedding process a parameter is derived which plays an important role in embedding and extracting the data. In the extraction process the features are extracted from stego image and the image is recovered, from this recovered image features are extracted and these features are compared with the extracted features form authentication purpose and to detect tampers. The proposed scheme provides the authentication and improves the stego image quality.

Hanizan Shaker Hussain et.al [23] proposed a hybrid fuzzy- SVM image Steganography based system which makes use of some of the soft computing techniques like fuzzy logic and support vector machine (SVM). The author proposed a new hybrid fuzzy c-means and F-SVM for image Steganography. In the proposed scheme the SVM learning ability is used to improve the imperceptibility and payload. In the scheme the JPEG cover image is converted to YCbCr colour space and then it is transformed from space domain to transform domain later quantization is applied to divide the DCT coefficients. After this the image is permuted later in the embedding process the secret message is embedded in the medium frequency of the coefficients based on the trained SVM. The output stego image will go through inverse permutation and Huffman encoder. The extracting process is the reverse process of the embedding. Fuzzy c means cluster used to differentiate between the smooth and the non-smooth areas in the cover image to strength embedding. The scheme improves the payload and imperceptibility.

Vinay Pandey et.al [24] develops a method for secure transmission of medical images. To overcome the problem of the previous algorithm where if data hiding key or the encryption key is leaked then the attackers can get the secret data, the author proposes Steganography by using crypto-image of any other medical image as cover image and embeds the data into it. Even if the hackers has the key he can't identified the exact secret data. In this scheme a private key is shared between sender and the receiver the key is compared to get the original data at the receiver. Due to the crypto image and the secret key the secret data is more secure.

Qingzhong Li et.al [25] presents a Steganography method based on sign embedding and fuzzy classification to minimize the distortion of secret image. There are two processes in the algorithm firstly embedding and extracting secondly fuzzy classification of DCT coefficients. The image is divided into 8*8 blocks and DCT is applied on each block to transform from spatial domain to the frequency domain, then classify the blocks using the fuzzy theory and obtain the embedding strength. Quantize and inverse quantize the DCT coefficients to get the integral coefficients after this embed the secret message into the ac coefficients of the image. As we embed into the ac coefficients very little error produces more distortion, to overcome this we use sign embedding method and apply inverse DCT to get stego-image. Fuzzy classifier is used to determine the embedding strength based on the frequency of the blocks. The proposed scheme produces good quality stego image and increases the payload.

Abbas Cheddad et.al [26] proposed a method to enhance the digital image Steganography where the data is embedded in the frames of the video files and the embedding pixels are selected based on the region of interest. An adaptive approach "steganoflage" is used for embedding the data in the region of image which assures the greater performance. In the process the videos are

divided into frames and the data are embedded in the specific region of the image after embedding the stego video is generated. Choosing a specific region is based on the human face or the skin tone which requires conversion of RGB image to YCbCr. The skin tone has a centre point at Cb, Cr components where data can be embedded safely and preserving these facts. Before embedding, the salient features of the region are considered. Embedding into this region produces less distortion and produces robust output. Joyshree Nath et.al [27] presents a new steganography algorithm for hiding encrypted secret message into a cover image. The author has proposed a new encrypting and data hiding algorithm. The encrypting algorithm is MSA (Meheboob, Saima and Ashoke) which is a symmetric key cryptographic method. This method uses a random key generator for generating the initial key and this key is used to encrypt the secret message. This method generates a randomized key matrix of 16*16 whose values will range from ASCII (0-255). MSA is a substitution method where 2 characters from the input file are replaced by the character from the random matrix. MSA can be used for multiple encryption of message. In the embedding process we use LSB but not sequentially. To embed the secret message we have to skip 600 bytes from the last byte of the cover image after that again we skip 8*n bytes where n is the size of message. The reverse process is followed while extracting and one has to use password while embedding and the extracting the data. Due to the multiple encryptions the security is enhanced.

III. 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. The main focus is on using image processing concepts combined with cryptography and data hiding techniques for Steganography. The summary of various data hiding techniques and cryptography techniques with their advantages has been presented. From the study it has been found that many intelligent soft computing algorithms like Fuzzy Logic, Adaptive Neural Network, Genetic Algorithm and Support Vector Machines can be used in Steganography which improves the embedding capacity, security and stego image quality.

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] J. Breckling, Ed., the Analysis of Directional Time Series: Applications to Wind Speed and Direction, ser. Lecture Notes in Statistics. Berlin, Germany: Springer, 1989, vol. 61.

[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] 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.

[5] 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.

[6] 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.

[7] 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.

[8] Vu Mai, Ibrahim Khalil, Ayman Ibaida, "Steganography-based Access Control to Medical Data Hidden in Electrocardiogram", 35th Annual International Conference of the IEEE EMBS, pp: 1302-1305, 2013.

[9] Bremnavas, B. Pooma and G.R.Kanagachidambaresan "MEDICAL IMAGE SECURITY USING LSB AND CHAOTIC LOGISTIC MAP", proc. of Int. Con! on Advances in Recent Technologies in Communication and Computing, pp: 229-231, 2011.

[10] Pouria Mortazavian, Mohammad Jaha ngiri and Emad Fatemizadeh," A LOW-DEGRADATION STEGANOGRAPHY MODEL FOR DATA HIDING IN MEDICAL IMAGES", preceedings of Fourth IASTED International conference visualization. Imaging and image processing, pp: 914-920, 2004.

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

[12] Vinay Pandey, Angad singh and manish shrivastava, "Medical Image Protection By Using Cryptograhpy Data hiding and steganography", IJETAE, vol. 2, issue 1,pp: 106-109,2012.

[13] 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

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

[15] 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.

[16] Vinay pandey, Manish Shrivastava," Secure Medical Image Transmission Using Combined Approach of Data-hiding, Encryption and Steganography", IJARCSSE, vol. 2, issue 12, pp: 54-57, 2012.

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

[18] 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.

[19] 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.

[20] 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.

[21] Amanpreet Kaur and Sumeet Kaur, "Image Steganography Based on Hybrid Edge detection and 2^k correction Method", IJEIT,vol.1, issue 2,pp: 167-170,2012.

[22] SeungWu HAN, Hong Lin JIN, Masaaki FUJIYOSHI and Hitoshi KIYA, "Lossless Data Hiding in the Spatial Domain for Image Tamper Detection", ISPACS, IEEE, pp: 760-763, 2006.

[23] Hanizan Shaker Hussain, Syed Ahmad ALunid and Saadiah Yahya, "A novel Hybrid Fuzzy-Svm Image Steganography Model", IEEE, 2010.

[24] Vinay pandey and Manish Srivastava, "Medical Image Protection Using Steganography by Crytpo-image as cover image", International Journal of Advanced Computer Research, vol.2, issue 5, pp: 45-48, 2012.

[25] 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.

[26] Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt," Enhancing Steganography In Digital Images", Canadian Conference on Computer and Robot Vision, IEEE, pp: 326-322, 2008.

[27] Joyshree Nath, Asoke Nath,"Advanced Steganography Algorithm using Encrypted Secret message", International Journal of Advanced Computer Science and Applications, vol. 2, no 3, pp: 19-24, 2011.

BIOGRAPHIES

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

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

Tushara C K. MTech Student, Department of CSE, RVCE, Bangalore, India

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

.