International Journal of Advanced Technology in Engineering and Science
Vol. No.5, Issue No. 06, June 2017
www.ijates.com
ijates
ISSN 2348 - 7550

ENCRYPTED SUPPORT SYSTEM FOR MEDICAL CARE BASED ON MEDICAL IMAGE USING RDH ALGORITHM

P.Kishore Kumar[1], S.Parameshwari[2], S.Kannadhasan[3]

[1]P.G Scholar, [2]Assistant Professor, Department of Electronics and Communication Engineering, Medical Electronics, P.T.R College of Engineering and Technology, Madurai, Tamilnadu (India)

[3]Lecturer,Department of Electrical and Electronics Engineering, Medical Electronics, Tamilnadu Polytechnic College, Madurai, Tamilnadu (India)

ABSTRACT

Image processing is highly challenging field in medical image processing. To recognize the image or object is the main aim of the image processing technique. Medical imaging methods are used to image the internal part of the human body for medical diagnosis. Brain tumor is one of the critical and life changing disease condition. Then morphological filtering is used to avoids the misclustered regions that can be formed after segmentation of the brain MRI image for detection of tumor location. In image processing input image is processed to get output also as an image under consideration easier visually. Modern three-dimensional (3-D) medical imaging offers the potential and promise for major advances in science and medicine as higher fidelity images are produced. It has developed into one of the most important fields within scientific imaging due to the rapid and continuing progress in computerized medical image visualization and advances in analysis methods and computer-aided diagnosis, and is now, for example, a vital part of the early detection, diagnosis, and treatment of cancer. The challenge is to effectively process and analyze the images in order to effectively extract, quantify, and interpret this information to gain understanding and insight into the structure and function of the organs being imaged. Recognition can be performed interactively by clinicians or automatically using robust techniques, while the objective of segmentation is to precisely delineate contours and surfaces. Recently more and more attention is paid to reversible data hiding (RDH) in encrypted image. It maintains the excellent property that the original cover image can be losslessly recovered after embedded data is extracted while providing the image content confidentiality. All previous methods embed data by reversible vacating room from the encrypted images, which may be some errors on data extraction and/ or image restoration. A different scheme is proposed with a traditional RDH algorithm and the encrypting the data and embedding the data in encrypted images which is encrypted using a blow fish algorithm. In this data extraction and image recovery are free of any errors. The PSNR,MSE and RPE is significantly improved in this project.

I. INTRODUCTION

Medical image processing is one of the most challenging topics in research field. The main objective of image segmentation is to extract various features of the image that are used for analysing, interpretation and understanding of images. Medical resonance image plays a major role in medical diagnostics. Image processing in MRI of brain is highly essential due to accurate detection of the type of brain abnormality which can reduce the chance of fatal result. This paper outlines an efficient image segmentation technique that can distinguish the pathological tissues such as edema and tumor from the normal tissues such as white matter (wm), grey matter (gm), and cerebrospinal fluid (csf). Thresholding is simpler and most commonly used techniques in image segmentation. This technique can be used to detect the contour of the tumor in brain

Image segmentation plays a vital role in many medical-imaging applications, for the study of anatomical structures and to identify the region of interest. In this paper explaining the three existing segmentation approaches in medical image segmentation and Performance evaluated for these methods for the brain MRI on the basis of pixel value, volume of roi (region of interest), mean and Variance. Then reviewed with an emphasis on the advantages and disadvantages of these methods and showing the implemented outcomes of the thresholding, clustering, region growing segmentation algorithm for the brain MRI.

II. RELATED WORK

The paper presents securing the transmission of medical images. The presented algorithms will be applied to images. This work presents a new method that combines image cryptography, data hiding and Steganography technique for denoised and safe image transmission purpose. In This method we encrypt the original image with two shares mechanism encryption algorithm then embed the encrypted image with patient information by using lossless data embedding technique with data hiding method after that for more security. We apply steganography by encrypted image of any other medical image as cover image and embedded images as secrete image with the private key. In receiver side when the message is arrived then we apply the inverse methods in reverse order to get the original image and patient information and to remove noise we extract the image before the decryption of message. We have applied and showed the results of our method. Security is an important issue in digital data transmission and storage. The security can be provided by image encryption. Encryption is one of the ways to provide high security when images are transmitted over the network. Image encryption techniques scrambled the pixels of the image and decrease the correlation among the pixels, so that we will get lower correlation among the pixel and get the encrypted image which is hard to understand. There are so many different image encryption techniques available to protect confidential image data from unauthorized access. Image encryption techniques which provide transmission of digital images in more secure way. Encryptions algorithms that are good for textual data may not be suitable for multimedia data because images contain large data. This paper present survey of various encryption methods with its advantages and disadvantages.

Information security plays one of the very important roles in the field of emergent information and communication technology. The applications such as medical images and satellite images needs the security only in the required portion, which contains the useful information .To improve the perception of surroundings and to monitor the earth’s surface, remote sensing is used and it led the way for progress in information technologies. This paper explains the concept of enhancing the resolution of an image to improve the number of pixels, which is used to represent the details of an image and then segmenting the input image by using canny edge detector and encrypting the segmented image by using RC4 stream cipher algorithm. This encryption algorithm provides the security by XOR the plaintext and key. Moreover, RC4 algorithm (stream cipher) is considered to be providing a best result in terms of security, accuracy, noise, distortion less images by the varying features like variable key size and packet size.

III. PROPOSED METHOD

In proposed method can achieve real reversibility, that is, data extraction and image recovery are free of any error. If we reverse the order of encryption and vacating room, i.e., reserving room prior to image encryption at content owner side, the RDH tasks in encrypted images would be more natural and much easier which leads us to the novel framework, Difference expansion. We propose a separable reversible data hiding method for encrypted images using Blow fish encoding.

With two different keys, the proposed method is separable. The hidden data can be completely extracted using the embedding key, and the original image can be approximately reconstructed with high quality using the encryption key. With both keys available, the hidden data can be completely extracted, and the original image perfectly recovered with the aid of some estimated side information. The proposed method achieves a high embedding payload and good image reconstruction quality, and avoids the operations of room-reserving by the sender.

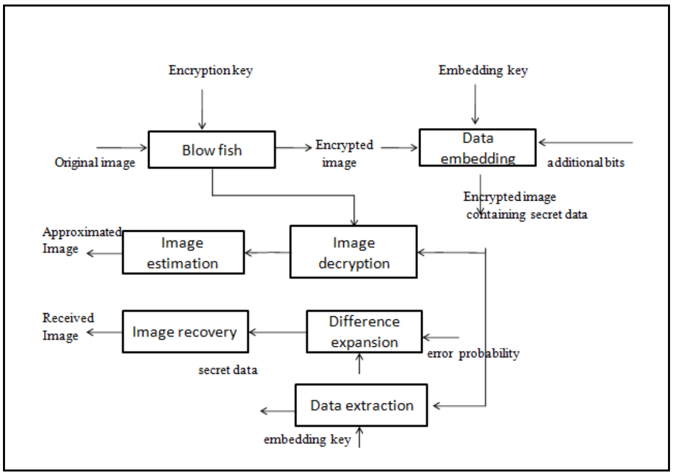


Fig: 3.1. Block Diagram of Proposed System

3.2 System Description

The proposed system is sketched in Fig. 1, which consists of three phases: image encryption, data embedding, and data extraction/image recovery. In phase I, the sender encrypts the original image into an encrypted image using a blow fish and an encryption key. In phase II, the data-hider selects and compresses some MSB of the secret image using LDPC codes to generate a spare space, and embeds additional bits into the encrypted image using an embedding key. In phase III, the receiver extracts the secret bits using the embedding key. If he/she has the encryption key, the original image can be approximately reconstructed via image decryption and estimation. When both the encryption and embedding keys are available, the receiver can extract the compressed bits, and implement the difference expansion decoding using the estimated image as side information to perfectly recover the original image.

3.3 Modules

- Encrypted Image Generation
- IMAGE PARTITION
- SELF REVERSIBLE EMBEDDING

- Data Hiding In Encrypted Image
- Data Extraction and Image Recovery
- Data Extraction and Image Restoration

3.4 Lossless Data Hiding Scheme:

A lossless data hiding scheme for public-key encrypted images is proposed. There are three parties in the scheme: an image provider, a data-hider, and a receiver. With a cryptosystem possessing probabilistic property, the image provider encrypts each pixel of the original plaintext image using the public key of the receiver, and a data-hider who does not know the original image can modify the cipher text pixel-values to embed some additional data into the encrypted image by multi-layer wet paper coding under a condition that the decrypted values of new and original cipher-text pixel values must be same. When having the encrypted image containing the additional data, a receiver knowing the data hiding key may extract the embedded data, while a receiver with the private key of the cryptosystem may perform decryption to retrieve the original plaintext image. The embedded data can be extracted in the encrypted domain, and cannot be extracted after decryption since the decrypted image would be same as the original plaintext image due to the probabilistic property.

3.5 Reversible Data Hiding Scheme:

This section proposes a reversible data hiding scheme for public-key-encrypted images. In the reversible scheme, a preprocessing is employed to shrink the image histogram, and then each pixel is encrypted with additive homomorphic cryptosystem by the image provider. When having the encrypted image, the data-hider modifies the cipher text pixel values to embed a bit-sequence generated from the additional data and error correction codes. Due to the homomorphic property, the modification in encrypted domain will result in slight increase/decrease on plaintext pixel values, implying that a decryption can be implemented to obtain an image similar to the original plaintext image on receiver side. Because of the histogram shrink before encryption, the data embedding operation does not cause any overflow/underflow in the directly decrypted image. Then, the original plaintext image can be recovered and the embedded additional data can be extracted from the directly decrypted image.

3.6 Encrypted Image Generation

In this module, to construct the encrypted image, the first stage can be divided into three steps:

- IMAGE PARTITION
- SELF REVERSIBLE EMBEDDING
- IMAGE ENCRYPTION

At the beginning, image partition step divides original image into two parts and then, the LSBs of are reversibly embedded into with a standard RDH algorithm so that LSBs of can be used for accommodating messages; at last, encrypt the rearranged image to generate its final version.

3.7 Image Partition

The operator here for reserving room before encryption is a standard RDH technique, the goal of image partition.

3.8 Self Reversible Embedding

The goal of self-reversible embedding is to embed the LSB-planes of into by employing traditional RDH algorithms. We simplify the method in to demonstrate the process of self-embedding.

3.9 Data Hiding In Encrypted Image

In this module, a content owner encrypts the original image using a standard cipher with an encryption key. After producing the encrypted image, the content owner hands over it to a data hider (e.g., a database manager) and the data hider can embed some auxiliary data into the encrypted image by lossless vacating some room according to a data hiding key. Then a receiver, maybe the content owner himself or an authorized third party can extract the embedded data with the data hiding key and further recover the original image from the encrypted version according to the encryption key.

3.10 Data Extraction And Image Recovery

In this module, Extracting Data from Encrypted Images to manage and update personal information of images which are encrypted for protecting clients' privacy, an inferior database manager may only get access to the data hiding key and have to manipulate data in encrypted domain. When the database manager gets the data hiding key, he can decrypt and extract the additional data by directly reading the decrypted version. When requesting for updating information of encrypted images, the database manager, then, updates information through LSB replacement and encrypts up dated information according to the data hiding key all over again. As the whole process is entirely operated on encrypted domain, it avoids the leakage of original content.

3.11 Data Extraction And Image Restoration

In this module, after generating the marked decrypted image, the content owner can further extract the data and recover original image. On the receiver end, with the marked encrypted image, the hidden data can be extracted using the embedding key, and the original image can be approximately reconstructed using the encryption key, or losslessly recovered using both of the keys. Three cases are analyzed below in Subsections A, B and C respectively, in which the receiver has the embedding key only, the encryption key only, and both. We denote the received encrypted image containing secret data as V.

3.12 Advantages

- Reutilization Technique
- Reduces Hardware Complexity
- High Speed Computing Dwt

IV. SIMULATION RESULTS AND DISCUSSION

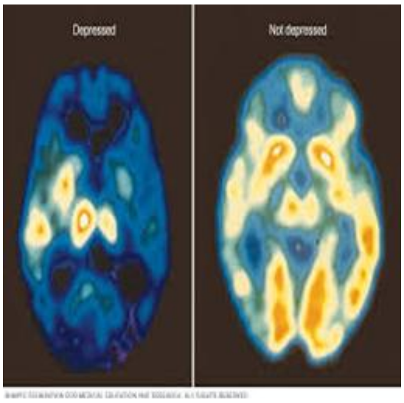
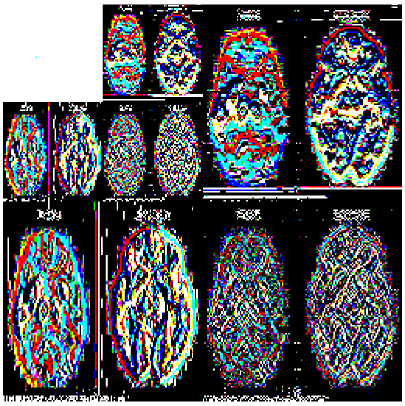


Figure 4.1 Original Image



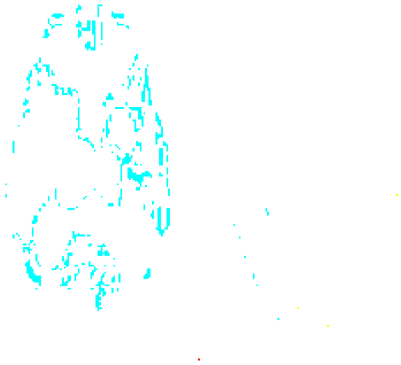
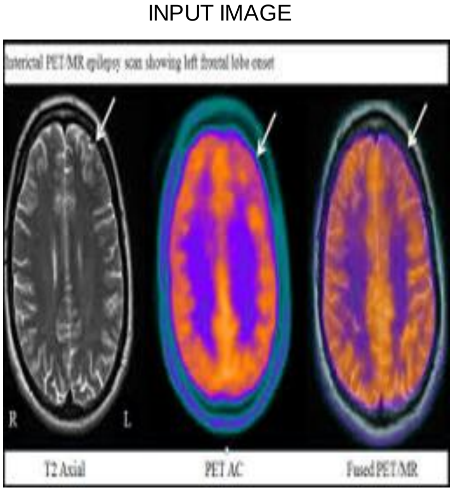


Figure 4.2 Embedded Image **Figure 4.3 Encrypted Image**


INPUT IMAGE
Interictal PET/MR epilepsy scan showing left frontal lobe onset
R
L
T2 Axial
PET AC
Fused PET/MR

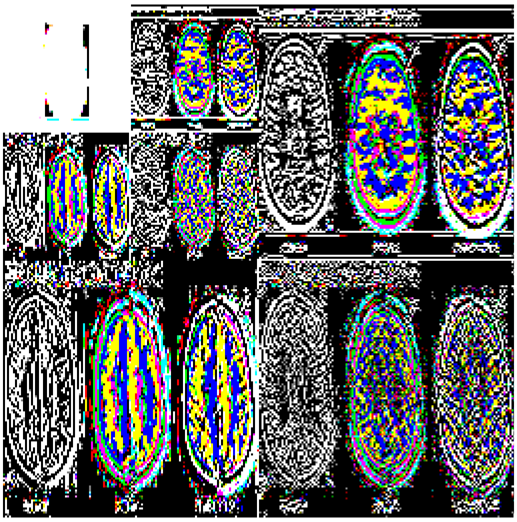


Figure 4.4 Another Original Image **Figure 4.5 Embedded Image**

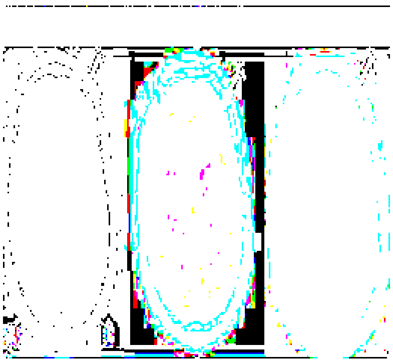


Figure 4.6 Encrypted Image

Here we compare a PSNR, MSE, RPE values for the proposed work and existing work

Table: 4.1 Performance Comparisons

	PSNR	MSE	RPE
BRAIN IMAGE 1			
EXISTINGWORK	**72.4395**	**0.0037**	**243.0000**
PROPOSEDWORK	**91.5792**	**4.502e-27**	**2.9634e-22**
BRAIN IMAGE 2			
EXISTINGWORK	**74.8343**	**0.0021**	**140.0000**
PROPOSEDWORK	**90.2552**	**6.1314e-27**	**4.0183e-22**

V. CONCLUSION AND FUTURE WORK

Segmentation of brain image is imperative in medical planning and treatment planning in the field of medicine. In this work, we have proposed a computer aided system for brain MR image segmentation for detection of tumor location using fuzzy clustering algorithm followed by morphological filtering. Further study includes the implementation of the algorithm and analysis of the result. An image segmentation approach based on thresholding has been discussed. This approach for segmentation of MRI brain images can help in the proper detection of the region of interest. The main limitation of this approach is that only two classes are generated and it cannot be used for multi-channel images. Thresholding approach is sensitive to noise and intensity homogeneities. Based on application we can select any one or combination of methods to get the desired segmented output. The Reversible data hiding in encrypted image is drawing lots of attention because of security maintaining requirements. Thus proposed scheme provides a completely new framework for reversible data hiding. This paper proposes a scheme of low complexity reversible data hiding in encrypted images using Multilayer embedding scheme. After encrypting the original image with a stream cipher, some bits of MSB planes are selected and compressed to make secret data effectively. The data are decoded using BPA concept. On the receiver side, all hidden information can be extracted with the embedding key only, and the original image approximately recovered with high quality using the encryption key only. When both the embedding and encryption keys are available to the receiver, the hidden data can be extracted completely and the original image recovered perfectly. The performance parameter is evaluated and compared with the conventional system, which provides better PSNR rate.

Thus, we conclude that, the prevention of data attack is reduced and data security is provided at greater extend. Total loss data recovery is possible at the time of data extraction. This work proposes a lossless, a reversible, and a combined data hiding schemes for cipher-text images encrypted by public key cryptography. In our future work, we will embed not only the data but also the image with additional information to be encrypted using different source coding schemes.

REFERENCES

[1.] E. J. Delp and O. R. Mitchell, "Image compression using block truncation coding," IEEE Trans. Commun., vol. 27, no. 9, pp. 1335–1342, Sep. 2016.

[2.] V. Udpikar and J. Raina, “BTC image coding using vector quantization,” IEEE Trans. Commun., vol. 35, no. 3, pp. 352–356, Mar. 2016.

[3.] Y. Wu and D. C. Coll, “BTC-VQ-DCT hybrid coding of digital images,” IEEE Trans. Commun., vol. 39, no. 9, pp. 1283–1287, Sep. 2015.

[4.] C. S. Huang and Y. Lin, “Hybrid block truncation coding,” IEEE Signal Process. Lett, vol. 4, no. 12, pp. 328–330, Dec. 2015.

[5.] Y.-G. Wu and S.-C. Tai, “An efficient BTC image compression technique,” IEEE Trans. Consum. Electron, vol. 44, no. 2, pp. 317–325, May 2015.

[6.] M. Lema and O. R. Mitchell, “Absolute moment block truncation coding and its application to color images,” IEEE Trans. Commun., vol. 32, no. 10, pp. 1148–1157, Oct. 2014.

[7.] J.-M. Guo and M.-F. Wu, “Improved block truncation coding based on the void-and-cluster dithering approach,” IEEE Trans. Image Process., vol. 18, no. 1, pp. 211–213, Jan. 2013.

[8.] N. A. Saleh, H. N. Boghdad, S. I. Shaheen, A. M. Darwish, High Capacity Lossless Data Embedding Technique for Palette Images Based on Histogram Analysis, Digital Signal Processing, 20, pp. 16291636, 2013.

[9.] J. Tian, Reversible Data Embedding Using a Difference Expansion, IEEE Trans. on Circuits and Systems for Video Technology, 13(8), pp. 890896, 2013.

[10.] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, Lossless Generalized-LSB Data Embedding, IEEE Trans. on Image Processing, 14(2), pp. 253266, 2011.

[11.] M. Ghebleh and A. Kanso, A robust chaotic algorithm for digital image steganography, Commun Nonlinear Sci. Numer. Simulat. 19 (2014) 1898–1907.

[12.] Z. Qian, X. Han and X. Zhang, “Separable Reversible Data hiding in Encrypted Images by n-nary Histogram Modification,” 3rd International Conference on Multimedia Technology (ICMT 2013), pp. 869-876, Guangzhou, China, 2011.

[13.] W. Zhang, K. Ma and N. Yu, “Reversibility improved data hiding in encrypted images,” Signal Processing, vol. 94, pp. 118–127, 2014.

[14.] T. Kalker and F. M. Willems, “Capacity bounds and code constructions for reversible data-hiding,” in Proc. 14th Int. Conf. Digital Signal Processing (DSP2002), 2002, pp. 71–76.

[15.] J. Fridrich and M. Goljan, “Lossless data embedding for all image formats,” in Proc. SPIE Proc. Photonics West, Electronic Imaging, Security and Watermarking of Multimedia Contents, San Jose, CA, USA, Jan. 2002, vol. 4675, pp. 572–583.

[16.] J. Tian, “Reversible data embedding using a difference expansion,” IEEE Trans. Circuits Syst. Video Technol., vol. 13, no. 8, pp. 890–896, Aug. 2003.