ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Medical Image Cryptanalysis Using Histogram Matching Bitplane and Adjoin Mapping Algorithms

Kolakaluri Anuradha
M.Tech Student,
Department of CSE,
Dr.Samuel George Institute of Engineering & Technology, Darimadugu, Markapuram, Andrapradesh, India.

P. Pedda Sadhu Naik
HOD,
Department of CSE,
Dr.Samuel George Institute of Engineering & Technology, Darimadugu, Markapuram, Andrapradesh, India.

Abstract:

Secure transmission of patient information such as magnetic resonance (MR), computed tomography (CT) imagesis a highly challenging taskand storing the data will also be an important. Hence, instead of transmitting and storing the original images, someone can encrypt the original images with the other images which can be considered as key images. Then after at receiver end, one can decrypt the original image as it is without losing the original information, this process is known as cryptanalysis. Here, a novel medical image cryptanalysis has been proposed by using histogram matching based bitplane algorithm (HMB) and adjoin mapping (AM) algorithm.Histogram matching is used to find out that the proposed algorithms are lossless or lossy cryptographic algorithms for secure transmission. Experimental results have been tested on MATLAB environment and simulation results shows that the HMB algorithm is more secured than the AM algorithm interms of perceptual vision quality.

I.INTRODUCTION:

Most of the media services and wireless network technologies were providing omnipresent conveniences for sharing, collecting or distributing images or videos over cellular mobile networks, social networks such as wechat, whatsapp, facebook etc., wireless public channels and multimedia networks for many organizations and individuals. Recent years there is a rapid growth in digital information sharing such as digital images or digital videos. Digital information sharing will be done in various applications, each of them need to transmit the information securely without knowing to the unauthorized person or party. For the applications like storage and transmission securing an image is a challenging task. For example, many strategic places like commercial centers, financial centers and public transportations will be monitored by digital video surveillance systems for the purpose of homeland security.

Every day there is a large amount of images and videos with secure information, which does not known by unauthorized persons have been generated, transmitted or restored. In addition to this, patient's records in medical images such as Magnetic Resonance (MR) or Computed Tomography (CT) and medical signal reports such as electro cardiogram (ECG) or electro encephalogram (EEG) will be shared among the most of the doctors from different branches of health service organizations (HSO) over wireless networks for diagnosis purpose. All these medical images, signals and digital videos may contain some private information, which is more confidential. Hence, it is an important task to provide security for thissort of images and videos. Many applications such as medical, military, construction industries, fashion design industries and automobile industries require scanned information, blue prints and designs to be protected against espionage.

Developing and employing schemes to enhance the lifetime of digital images or videos is an important, imperative and challenging task, which protects the content of original data for many years [1]. To protect an image or video encryption is an effective approach [1], which transforms the image or video into different format. In recent years there are so many algorithm have been developed to provide more security, enhanced quality with easy implementation and faster calculations. Among them all of the techniques have their own drawbacks like computational complexity, time consumption, not suitable for 3D images etc., To overcome all the drawbacks here in the proposed system we introduced a new technique called an improved color image cryptanalysis using two secret key image and logical operation, which will provide more security by generating two secret keys.

II.RELATED WORK:

From the past decades there are so many image cryptographic algorithms have been developed

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

to protect the images from unauthorized parties, which were looking to destroy the information sent by transmitter. In 1995 the first image and video encryption: from digital rights management to secured personal communication published by pommer andreasand uhl andreas. In [1] the authors said that an incorporated overview of schemes for encryption of images and videos will be provided by image and video encryption. This ranges from few commercial applications like digital video broadcasting (DVB) or digital audio broadcasting (DAB)to more research oriented topics and published content.The concept in [2] was published by B. Schineir, in which the theorital and practical knowledge of a cryptosystem has been provided to secure the multimedia.It was introduced in 1995 and very soon it became the standard text book for cryptography courses in all over the world.The author in [3] proposed a new invertible 2D map, called Line map, for encryption and decryption of image, which maps an image into an array of pixels and then maps it back to the original image. This approach shows the better performance than the previously existed 2D maps, in which only permutation was used.

Another approach for image encryption in [4], which is proposed by kuang tsan lin, this approach utilized the both magic matrix scrambling and binary coding method to form a hybrid encoding method to encrypt an image. This will not provide any sort of distortion in decoding process, which means that the exact original image will be recovered at the receiver end. Anil kumar et. al. in [5] introduced a new image encryption technique based on chaotic standard map which uses extended substitution-diffusion scheme. This method uses linear feedback shift register to overcome the drawbacks of existing techniques by adding non-linearity. This approach is highly secured and faster than the conventional methods. Zhi liang zhu et. al. [6] introduced a chaos based symmetric image encryption using a bit level permutation, in which the Arnold cat map for bit level permutation proposed for an image cryptosystem to provide more security and faster simulations.

An effective, secured, fast and cost effective image transmission scheme proposed in [7] employs encryption, compression and secured key exchanging along with the image transmission. Recently, an image encryption scheme based on fractional Fourier transform (FRFT), singular value decomposition and Arnold transform has been proposed in [10] to improve the security to enhance the quality of decrypted image.

Image encryption technique using bit plane decomposition and scrambling was proposed by qiudong sun [8], which aims at the pixels positions interchanging and changing the gray values of pixels at the same time. This approach has better efficiency and properties than the random scrambling methods and it has more stability degree than the classical methods such as Arnold transform.

III.PROPOSED TECHNIQUE :

Here in this thesis we proposed two lossless image crypto systems to provide higher security and lossless recovery of encrypted image at the receiver end. Those two algorithms are as follows:

1.Histogram matching based bitplane (HMB) algorithm.

2.Adjoinmapping (AM) algorithm.

The proposed algorithm included with inverting and scrambling of data after doing the XOR operation for the combined key and input image bitplanes. Scrambling is done by converting the decimal or binary numbers into the strings and then converting them into binary to decimal values afterwards the values will be reshaped into the number of rows and number of columns of input image.

A.HMB Algorithm:

Here are the steps involved in medical image encryption using HMB algorithm:

* Select and read a MRT image i.e., 2D or 3D
* Find out the histogram of input MRT image
* Convert the input image into the number of bit planes. There are 8 bit planes for grayscale image and 24 bit planes for 3D or true color image
* Now, select and read the two key images of any type with the same size of input image
* Convert the both key matrices into number of bit planes and then do the logical XOR, OR, AND or XNOR operation to get the combined key from the two key matrices
* Do the XOR for the 8th bit plane of input image with the combined key matrix bit planes
* Now, inverting and scrambling algorithm to get the encrypted MRT image

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

B.Histogram Matching:

Histogram is known as the graphical representation of an image. Here, we utilized the histogram for measuring the performance of proposed algorithms i.e., lossy or lossless. We supposed to find the histogram of original MRT image in the encryption algorithm, then after we will find the histogram of decrypted MRT image after applying the proposed decryption algorithm to the encrypted MRT image. Then we will match the both histograms with the gray levels, if both of same it is known as lossless cryptography otherwise lossy cryptography algorithms.

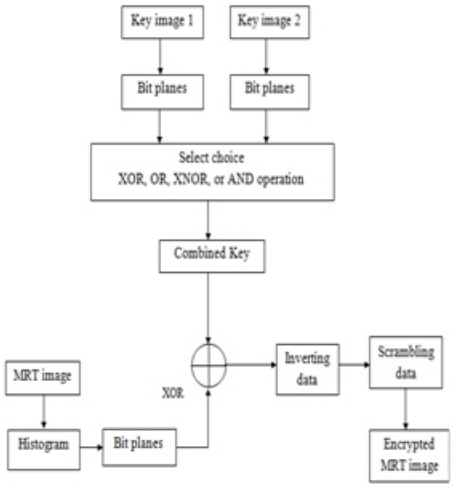


Fig1. Proposed HMB Block diagram of encryption algorithm.

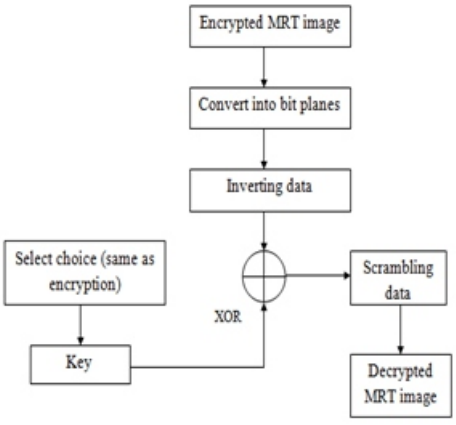


Fig2. Block diagram for Decryption algorithm of HMB.

C.AM Algorithm:

The following steps are used for the image crypto system which is based on AM algorithm.

* Select and read MRT image i.e., 2D or 3D image
* Convert the input image into the number of bit planes.
* Now, select and read the two key images of any type with the same size of input
* Apply adjoin mapping to the key matrices, then do the logical XOR, OR, AND or XNOR operation to get the combined key from the two key matrices
* Do the XOR for the each bit plane of input image with the combined key matrix
* Now, apply inverting and scrambling to get the encrypted MRT image.

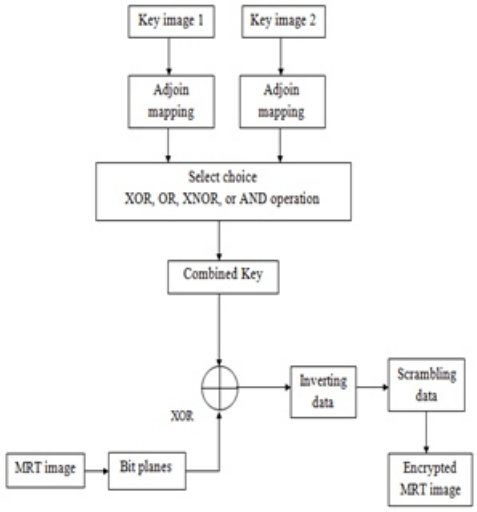


Fig3. Block diagram of AM algorithm

IV.EXPERIMENTAL ANALYSIS:

In this section, the performance analysis of proposed algorithms has been discussed. All the experiments have been done in MATLAB 2014a with 4.0 GB RAM and i3 processor, with multiple images taken from the medical databases, various sitesand from text books.We tested few sets of MR and CT images with general images as key images. Fig.4 and 6 shows that the original MR image, two key images i.e., images lena.jpg, which is a true color image and graylena.jpg, which is a gray scale image, encrypted MR image and decrypted MR images. We can see that the encrypted image will not be decrypted if any one of the key matrix is not available. The decrypted image is almost equal to the original image which has been encrypted by using HMB algorithm. Histogram of the original and decrypted MR images has been shown in fig.5. By observing the fig.4, 5, 6 and 7, we can conclude that the proposed HMB algorithm is a lossless cryptanalysis system.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

In fig.8, AM results has been displayed, which uses adjoin mapping for the encrypting the key matrix with the original image.By observing the fig8, one can conclude that the AM algorithm has given poor results over HMB algorithm. And also there is no measurement for matching the original and decrypted images.

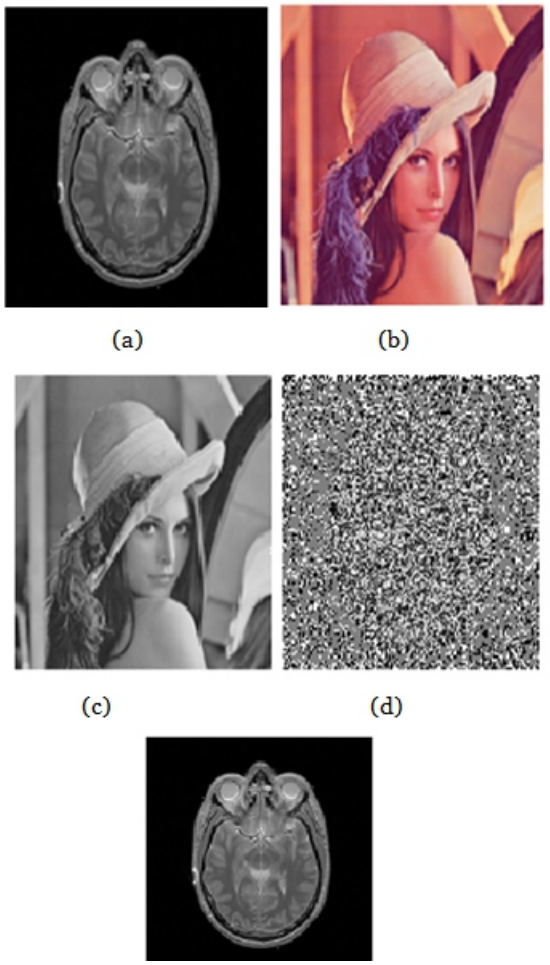


Fig4. (a) Original MR image (b) Key image-1 (c) Key image-2 (d) Encrypted MR image and decrypted image.

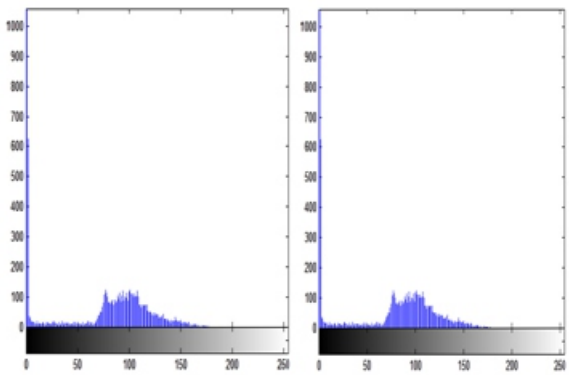


Fig5. Histograms of Original and Decrypted image

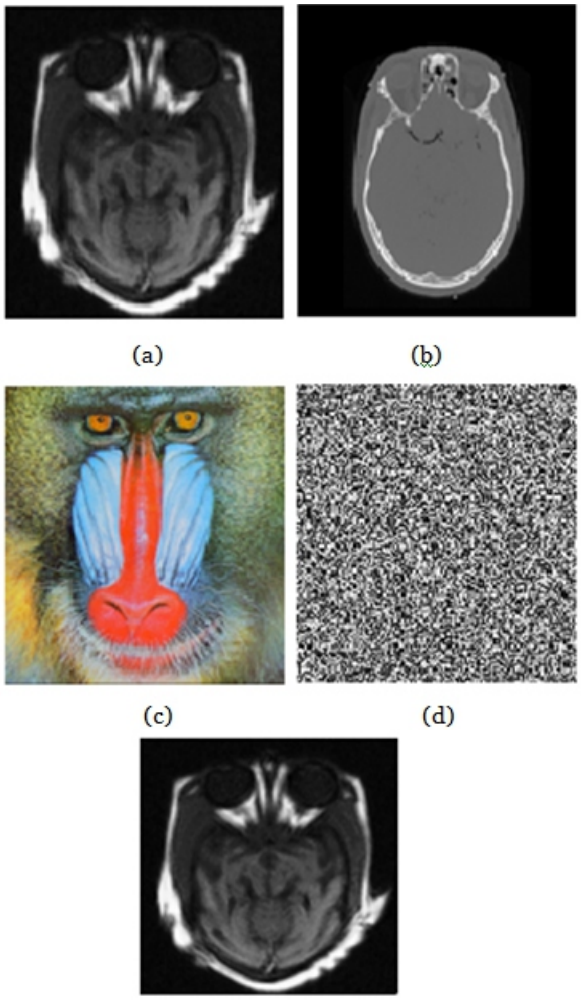


Fig6. (a) Original MR image (b) key image-1 (c) Key image-2 (d) Encrypted image and decrypted image.

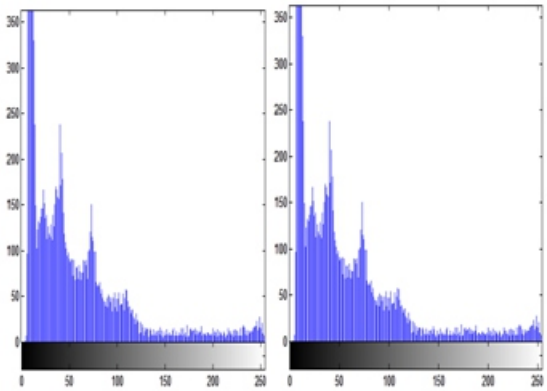


Fig.7 Histograms of original and decrypted image

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

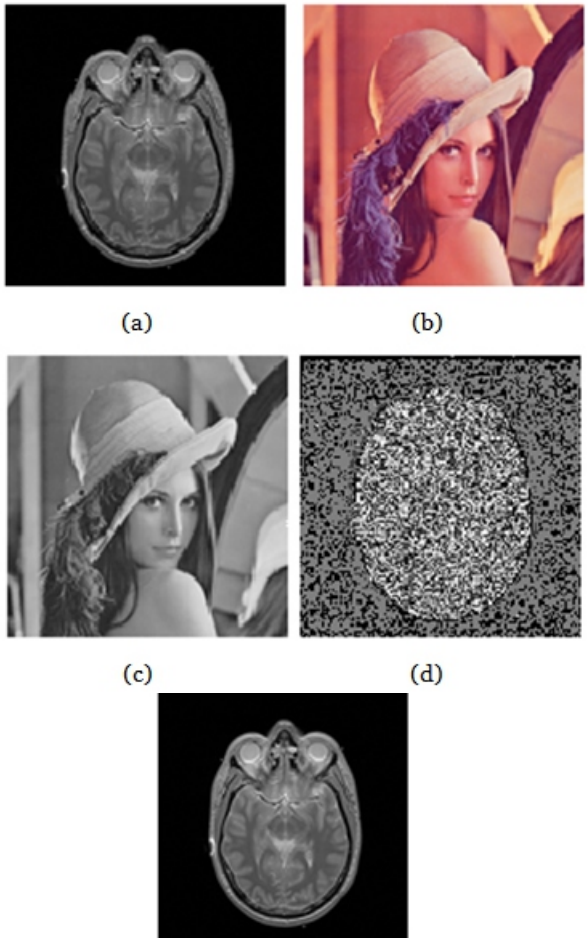
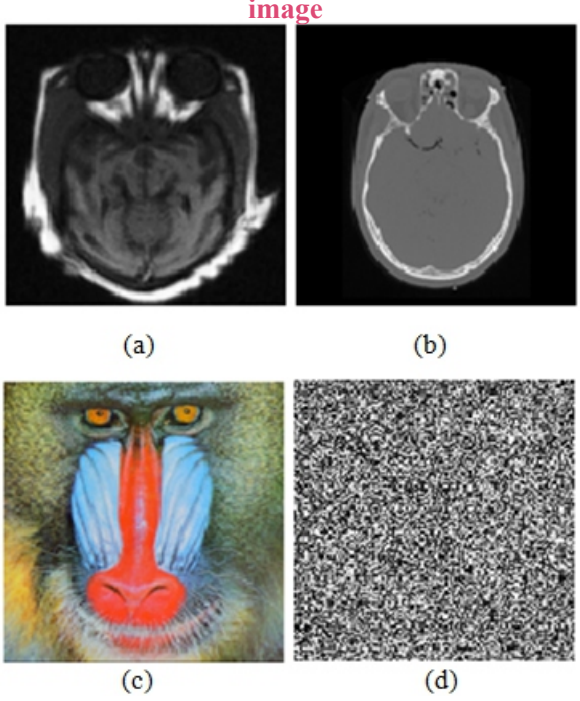
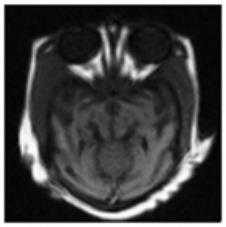


Fig.8 (a) Original image (b) key image-1 (c) key image-2 (d) encrypted image using AM and (e) decrypted image





(e)

Fig.9 (a) Original image (b) key image-1 (c) key image-2 (d) encrypted image using AM and (e) decrypted image.

V.CONCLUSION:

In this letter, we had implemented a new image cryptanalysis for improving the security to digital information based on the two powerful image encryption algorithms, which uses a binary key matrix for encrypting and decrypting the data. Here we had used two binary keys for improving the security and robustness. The proposed method has two methods BPC and BMC, which can be applied to any sort of image like real time, satellite, medical, bio-medical, remote sensing etc., Simulation results shows that the both algorithms have shown the excellent performance.

REFERENCES:

1.A. Pommer, A. Uhl, "Image and video encryption: from digital rights management to secured personal communication", Advances in Information Security, Vol. 15, 161p., 2005

2.B. Schneier.: Cryptography: Theory and Practice, CRC Press, Boca Raton, 1995.

3.Yong Feng, Xinghuo Yu, "A Novel symmetric image encryption approach based on an invertible two dimensional map".35th Annual Conference on Industrial Electronics,pp.1973-1978, 2009.

4.Kuang Tsan Lin, "Hybrid encoding method by assembling the magic-matrix scrambling method and the binary encoding method in image hiding", Optics Communications, Vol. 284, pp. 1778-1784, 2011.

5.Anil Kumar and M. K. Ghose, "Extended substitution-diffusion based image cipher using chaotic standard map", Communication in Nonlinear Science and Numerical Simulation, Vol.16, Issue 1, pp. 372-382, 2011.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

6.Zhi-liang Zhu, Wei Zhang, Kwok-wo Wong and Hai Yu, "A chaos-based symmetric image encryption scheme using a bit-level permutation", Information Sciences, Vol. 181, pp. 1171-1186, 2011.

7.Kamlesh Gupta and Sanjay Silakari, "Novel Approach for fast Compressed Hybrid color image Cryptosystem", Advances in Engineering Software, Vol.49, pp. 29-42, 2012.

8.Qiudong Sun, Wenying Yan, Jiangwei Huang and Wenxin Ma, "Image encryption based on bit-plane decomposition and random scrambling".2nd International Conference on Consumer Electronics, Communications and Network, pp. 2630-2633, 2012.

9.Y. Zhou, K. Panetta, S. Agaian and C. L. Philip Chen, "Image encryption using P-Fibonacci transform and decomposition", Optics Communications, Vol. 285, pp. 594-608, 2012.

10.A Linfei Chen, Daomu Zhao and Fan Ge, "Image encryption based on singular value decomposition and Arnold transform in fractional domain", Optics Communications, Vol.291, pp. 98-103, 2013.

Author's Details:

Kolakaluri Anuradha
M.Tech Student, Department of CSE, Dr.Samuel George Institute of Engineering & Technology, Darimadugu, Markapuram, Andrapradesh, India.

P.Pedda Sadhu Naik
received B.Tech (CSE) Degree from JNT University in 2003 and M. Tech (CS) Degree from JNTUCE Anatapur in 2007.He is doing Ph. D from JNTUK, Kakinada in Computer Science under the guidance of Dr. T. Venu Gopal. He has 12 years of teaching experience. He joined as Assistant Professor in Dr.Samuel George Institute of Engineering& Technology, Markapuram, India in 2003. Presently he is working as Associate Professor and Head of the Department of CSE. His Interested research areas are Image Processing and Soft Computing. He has life member of ISTE and IAENG. He organized various National Level Technical Symposiums as Convener. He attended Various National and International Workshops and Conferences on image Processing.