Securing Medical Images by Image Encryption using Key Image

Shrija Somaraj
Research Scholar
Bharathiar University
Coimbatore
Chennai, India

Mohammed Ali Hussain, PhD
Professor, Dept.of Electronics and Computer Engineering
KL University, Guntur
A.P., India

ABSTRACT
This paper presents two methods for encryption and decryption of images using XOR operation. In the first method the original image is encrypted by the key image using XOR operation and decryption process also uses the same key image with XOR operation. In the second method one of the bit planes of the key image is used for encrypting the bit planes of the original image and shuffling is done for getting the encrypted image. This method also uses XOR operation. Both the methods use a binary image of the same size as key for encrypting the original image. Experiments have shown that both algorithms are suitable for 2D as well as 3D images. These algorithms are implemented in MATLAB environment and tested on various medical images which have shown good results. These methods can be used for encrypting other images also.

General Terms
Image Encryption, Image Security.

Keywords
Image Encryption, Image Decryption, Bit Plane, XOR operation, Key image.

1. INTRODUCTION
In recent years, communications via Internet are getting more frequent with the increasingly wide reach of the Internet. Due to a large number of threats against communications security, protection of information has become an important issue. Especially because digital images contain large amount of information, security for images is a major concern. Many applications like Medical imaging, Military image databases, videoconferencing, online photograph album, etc. require a security system which is reliable and robust to store and transmit digital images. The requirements to fulfill the security needs of digital images have led to the development of good encryption techniques.

During the last decade, numerous encryption algorithms [1–12] have been proposed in the literature based on different principles. The digital images have certain characteristics such as being less sensitive as compared to the text data as a tiny change in the attribute of any pixel of the image does not drastically degrade the quality of the image and bulk capacity of data, redundancy of data, strong correlation among adjacent pixels, etc. Most conventional encryption algorithms put the emphasis on text data or binary data. Consequently, the traditional ciphers like IDEA,AES,DES, RSA etc. are not suitable for real time image encryption as these ciphers require a large computational time and high computing power. For real time image encryption only those Ciphers are preferable which does not compromise security and take lesser amount of time[13].

In this paper two methods for encryption of images are suggested, both have some common features as both use an image as key and XOR operation. First method performs encryption of original image by XORing it with the Key image, decryption has reverse process i.e. encrypted image is XORed with Key image which gives the original image.

There are three kinds of encryption techniques namely substitution, transposition or permutation and techniques that include both transposition and substitution. Substitution schemes change the pixel values while permutation schemes just shuffle the pixel values based on the algorithm. In some cases both the methods are combined to improve security.

First method uses substitution while the second uses both substitution and transposition.In the second method concept of bit plane is being applied, the key image is divided into 8 bit planes and then XORed with the original image and again bit planes shuffled in the encrypted image, reverse process is being followed for decryption.

The rest of the paper is organised as follows: Section 2 contains the related work done in this area, Section 3 contains Encryption Methods, Section 4 contains the results ,Section 5 contains Security Analysis followed by Conclusion in Section 6.

2. RELATED WORK
The security of digital images has become a major concern due to the evolution of the Internet . The security of images has attracted more attention recently, and many different image encryption methods have been proposed for enhancing the security of images. Saroj Kumar et al[1] have presented image encryption technique using the Hill cipher method. S.H. Kamali et al [2] have presented a modification of the Advanced Encryption Standard which presents a high level of security and better image encryption.

Mohammad Ali Bani Younes and Aman Jantan [3] had introduced a permutation technique based on encryption algorithm RijnDael and image permutation .M. Zeghid et al[4] have analyzed the Advanced Encryption Standard and to ensure improving the encryption performance they added a key stream generator.

Kuldeep Singh and Komalpreet Kaur[5] in their paper have compared four chaotic maps, Cross chaotic, Ikeda ,Logistic and Henon map and noise effects are seen on image. Seyed Mohammad Seyedzade et al [6] have proposed a novel

algorithm based on SHA-512 hash function for image encryption.

Rinkee Gupta and Jaipal Bhist[7] have presented a color image encryption and decryption using partition and scanning pattern which is related to Scan approach. Mohammad Ali Bani et al [8] used Blowfish algorithm and image transformation to generate a block-based transformation algorithm. Zhang Yunpeng et al [9] have worked on the combination of image encryption algorithm, chaotic encryption and DES encryption.

Sesha Pallavi Indrakanti and P.S.Avadhani[10] proposed a new image encryption algorithm based on random pixel permutation with the motivation to maintain the quality of the image. N. K Pareek et al[11] have proposed an image encryption scheme which uses an external secret key of 80 bit and two chaotic logistic maps.Inorder to make the cipher more robust the secret key is modified after encrypting each block of sixteen pixels of the image.

Amitava Nag et al[12] proposed a two phase encryption and decryption algorithm which is based on shuffling of the image pixels using affine transform and then performing encryption on the resulting image using XOR operation.

3. ENCRYPTION METHODS

The methods are suggested for medical images, as when patients want to share medical images on internet with only people of their interest, they need to secure them from different kinds of attacks. Medical images have different properties as compared to other digital images that are the reason; the kind of encryption required is also different.

3.1 First Method

3.1.1 Algorithm 1: For Encryption using Key image and XOR operation

Step 1: Read Original Image.

Step 2: Take the key image of same size as original image.

Step 3: Convert key image and original image to gray image.

Step 4: Perform XOR operation of original image with key image pixel by pixel.

Step 5: Resultant image is encrypted image.

3.1.2 Algorithm 2: For Decryption using Key image and XOR operation

Step 1: Read Encrypted Image.

Step 2: Take the key image which was used for encryption.

Step 3: Convert key image and encrypted image to gray image.

Step 4: Perform XOR operation of encrypted image with key image pixel by pixel.

Step 5: Resultant image is the original image.

3.2 Second Method

3.2.1Algorithm 3: For Encryption using Bitplane method

Step 1: Read Original Image(Color Image).

Step 2: Take the key image of same size as original image.

Step 3: Select at random any one bit plane of key image.

Step 4: Perform XOR operation of every bit plane of original image with the selected bit plane of key image.

Step 5: Next shuffling of bitplanes in a particular sequence is done to get the resultant image.

Step 6: Resultant image is encrypted image.

3.2.2 Algorithm 4: For Decryption using Bitplane method

Step 1: Read Encrypted Image.

Step 2: Take the key image which was used for encryption.

Step 3: Select the bit plane of key image which was used for encryption.

Step 4: Perform XOR operation of every bit plane of encrypted image with the selected bit plane of key image.

Step 5: Store result in reshuffled sequence.

Step 6: Resultant image is the original image.

4. EXPERIMENTAL RESULTS

Above algorithms are implemented in MATLAB7.0 and applied on brain image, the result is as given below. For both methods a key image is used given in Fig 1. The result of first method is given in Fig 2.which shows original image, encrypted image and the decrypted image using XOR operation. The result of the second method is shown in Fig 3 to Fig 6 . Encryption process is shown in Fig 4. and Decryption process is shown in Fig 6. A histogram analysis of the second method is shown in Fig 7. where there is much difference in the histogram of the original and encrypted image while the histogram of original and decrypted image is same showing that the image after decrption is obtained same as original image without any loss.

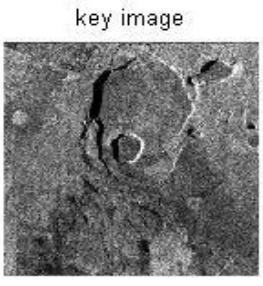

Fig 1: Key image used in both the methods

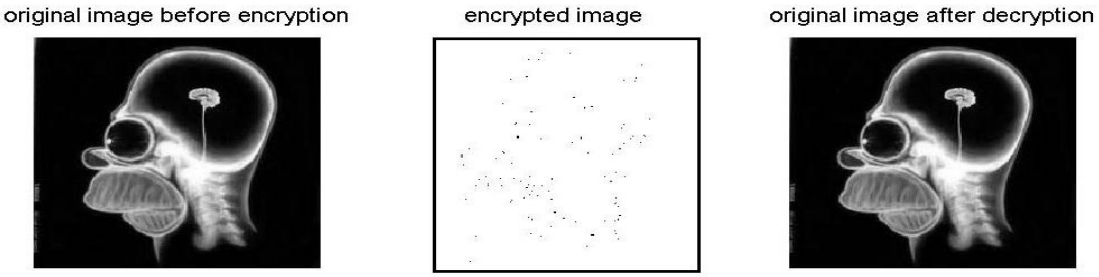

Fig 2: Showing Encryption – Decryption by XOR Method(First Method)

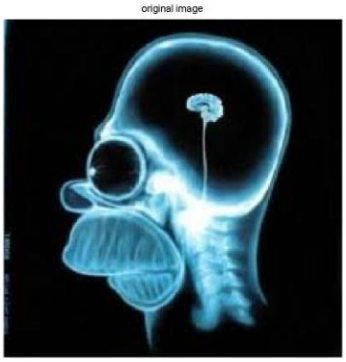

Fig 3: Original image before encryption

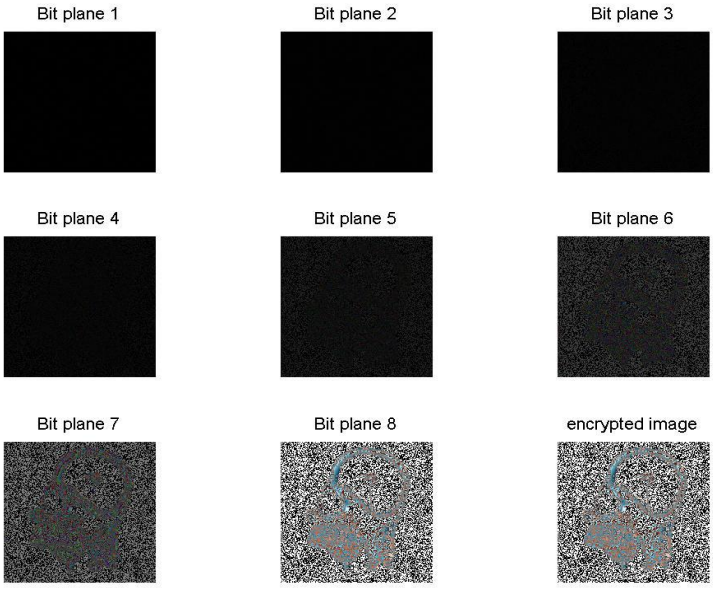

Fig 4: Encryption process using bitplane method

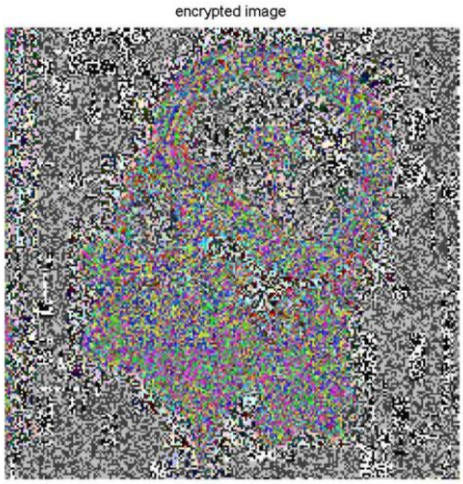

Fig 5: Shows encrypted image using bitplane method

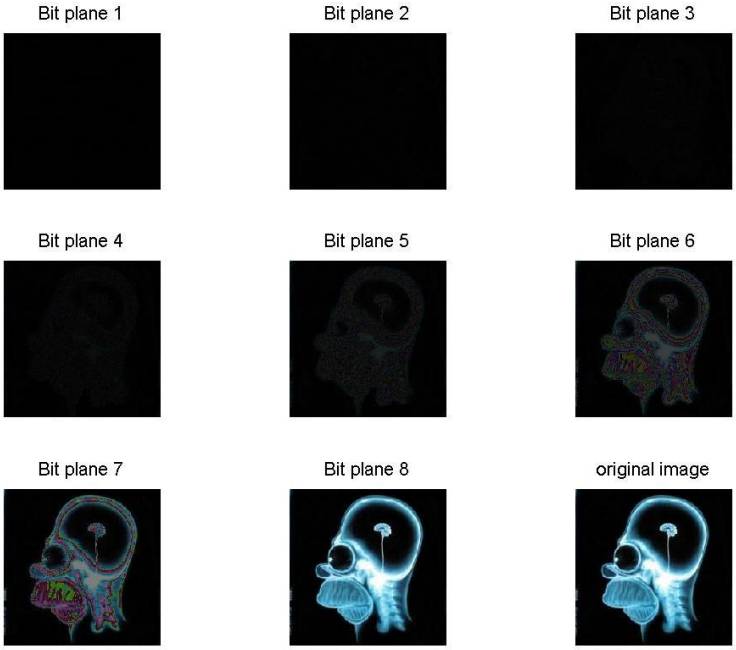

Fig 6: Decryption process using bitplane method

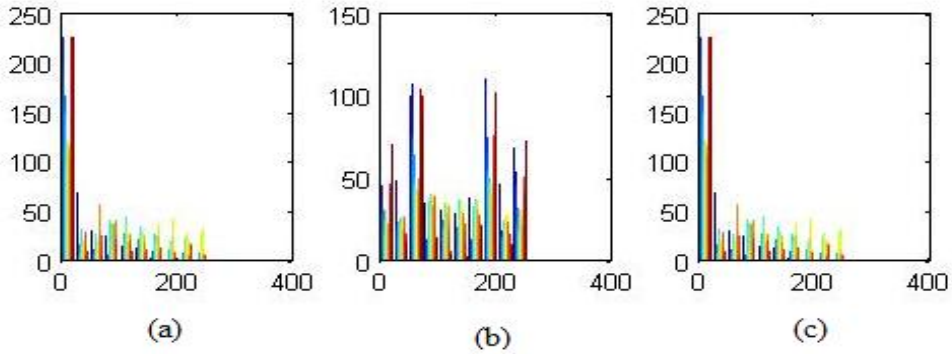

Fig 7: Showing histogram of bit plane method (a) histogtram of original image (b)histogram of encrypted image and (c) histogram of decrypted image

5. SECURITY ANALYSIS

Security is one of the major aspects to be taken care of for both the encrypted objects and the encryption algorithms. Some of the security aspects of the two methods are discussed here. In both the methods as an image itself is used as key it is very difficult for the attackers to find which image will be used as key. The original image is completely reconstructed without any loss or distortion only when the correct key image is used. Some of the possible attacks are:

Brute Force Attack : In Brute force attack the attacker performs an exhaustive search of all the possible combinations of security keys for guessing the keys. This kind of attack is possible only if the key space of the algorithm is limited and the attacker also knows the encryption algorithm. But in the proposed methods as image itself is used as key and any other images can be used by the users if required as key, limits this kind of attack.

Ciphertext Related Attacks: The ciphertext is the encrypted plaintext. In this kind of attack , attacker tries to deduce the security keys by using the ciphertext . But these kind of attacks are also not possible in these methods as the encrypted images are unrecognizable ,and have no information about the original image , attacker cannot use them for judging anything.

6. CONCLUSION

In this paper two simple methods of encrypting an image is introduced which is less complex than RSA and DES algorithms and has given good results on being implemented in MATLAB. In both the methods encryption is done using a key image. The first method uses XOR operation for encryption while in the second method bit plane concept and shuffling of bit planes is done along with XOR operation. Both the methods were applied on different images and the results obtained were commendable. These methods can be used for security of images in a variety of environments.

In this paper these methods are applied on medical images but these methods can very well be used for other digital images also, but the level of encryption achieved will depend upon the selection of key image.

7. ACKNOWLEDGMENTS

Our thanks to the experts who have contributed towards development of the template especially Ms.K.H.Vijaya Kumari for her assistance in Matlab programming.

8. REFERENCES

[1] Panigrahy, S.K., Acharya, B. and Jen, D., 2008. Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm. In 1st International Conference on Advances in Computing, Chikhli, India.

[2] Kamali, S.H., Shakerian, R., Hedayati, M.,Rahmani, M., 2010. A new modified version of Advance Encryption Standard based algorithm for image encryption.In International Conference on Electronics and Information Engineering (ICEIE),

[3] Younes,M.A.B and Jantan,A., 2008. An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption. In International Journal of Computer Science and Network Security(IJCSNS), VOL.8.

[4] Zeghid,M., Machhout,M., Khriji,L., Baganne,A., Tourki, R.,2007.Modified AES Based Algorithm for Image Encryption. In World Academy of Science, Engineering and Technology.

[5] Singh,K., Kaur,K., 2011. Image Encryption using Chaotic Maps and DNA Addition Operation and Noise Effects on it. In International Journal of Computer Applications, Volume 23– No.6.

[6] Seyedzade,S.M., Atani,R.E. and Mirzakuchaki,S. 2010. A Novel Image Encryption Algorithm Based on Hash Function. In 6th Iranian Conference on Machine Vision and Image Processing.

[7] Gupta,R.,Bisht,J. 2013.Colour Image Encryption and Decryption by using Scan Approach. In International Journal of software & Hardware Research in Engineering, Volume 1 Issue 2.

[8] Younes,M.A.B and Jantan,A. , 2008. Image Encryption Using Block-Based Transformation Algorithm. In International Journal of Computer Science(IAENG),.

[9] Yun-peng,Z., Wei,L., Shui-ping,C., Zheng-jun,Z., Xuan ,N.,Wei-di,D., 2009. Digital image encryption algorithm based on chaos and improved DES.In IEEE International Conference on Systems, Man and Cybernetics.

[10] Seyedzade,S.M., Atani,R.E. and Mirzakuchaki,S., 2010. A Novel Image Encryption Algorithm Based on Hash Function. In 6th Iranian Conference on Machine Vision and Image Processing.

[11] Pareek ,N. K., Patidar , V., Sud, .K .K. 2006. Image encryption using chaotic logistic map. In Image and Vision Computing 24(2006)926–934, Elsevier.

[12] Nag, A., Srabani Khan, Saswati Ghosh, Singh, J.P., Biswas, S., Sarkar,D., Sarkar,P.P. 2011. Image Encryption Using Affine Transform and XOR Operation. In International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN).

[13] Reddy Jyoteeswara Prasad, S. and Sathyanarayana, R.V.S. 2013. Image encryption using color key images. In International Journal of Elec. & Electr. Eng. & Telecom.