JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

WATER MARK BASED ENCRYPTION AND DECRYPTION OF MEDICAL IMAGES

[1]Nallabelli Manoj, [2]Medak Srinivas

[1] Assistant Professor, Department of ECE, JNTUHCEJ, JAGTIAL, Telangana, India

[2]Assistant Professor, Department of ECE, JNTUHCEJ, JAGTIAL, Telangana, India

Email id: manoj.nallabelli@gmail.com

Abstract

An encryption frame of medical image with watermark based on hyperchaotic system is proposed in this paper. Medical information, such as the patients' private information, data needed for diagnosis, and information for authentication or protection of medical files, is embedded into the regions of interest (ROI) in medical images with a high capacity difference-histogram based reversible data-hiding scheme. After that, the watermarked medical images are encrypted with hyperchaotic systems. In the receiving end, the receiver with encryption key can decrypt the image to get similar images for diagnosis. If the receiver has the key for data hiding at the same time, he/she can extract the embedded private information and reversibly recover the original medical image. Experiments and analyses demonstrate that high embedding capacity and low distortion have been achieved in the process of data hiding, and, at the same time, high security has been acquired in the encryption phase. The experimental results shows that the proposed algorithm can achieve high security with good performance. The results are evaluated using matlab tool.

Keywords:

Medical images, Encryption, decryption, Region of interest, hyperchaotic system

1. Introduction

The rapid development of the Internet makes life more convenient than ever before. However, just as the old saying: every leaf has two sides, the Internet brings us not only convenience but also many problems. Leakage of privacy is one of the most important things. For example, medical information, such as EHRs (Electronic Health Records) [1], is often closely related to patients' privacies which should be kept secret. Medical images for diagnosis need to be protected in order to prevent malicious tampering. There are two ways for solving these problems: one is encryption, and the other one is information hiding. As a traditional solution of secure communication on insecure channels, encryption has been widely explored [2], and many of the encryption schemes have introduced chaotic systems to enhance the security of encryption.

Information hiding (or data hiding) is a newly proposed way for secure communication although the ideology occurred quite a long time ago. With the development of data hiding and digital watermarking, many schemes have been proposed to embed information into medical images [3] for the protection of private information and the authentication of medical images. These schemes utilized in medical images made full use of the intrinsic features of medical images and achieved nice results too. Obviously, both encryption and data hiding have their advantages in secure communication; what if we combine them together for better protection of medical image and private information?

Recently, some novel schemes combining the data hiding and encryption have been proposed [4]. Among them, schemes can be divided into three categories: the first one is encryption before data hiding [5]; the second one is encryption after data hiding; the third one is fusion of encryption and data hiding. From the information hider's point of view, information can be hidden in the spatial domain, the encrypted domain [6], or both of the two domains. In [3], additional information is firstly coded with a quantization index modulation (QIM) method; then -this coded information is encrypted with traditional encryption methods (such as RC4 algorithm); finally, the encrypted coded information is embedded into medical image with the simple least significant bit (LSB) substitution method.

The scheme is not reversible due to the LSB substitution. Reversible data hiding schemes in encrypted images are proposed in [7]. The image is encrypted with a stream cipher, and then information is embedded into the encrypted images by modifying a small proportion of those encrypted data. In the receiving end, the encrypted image containing additional data is firstly decrypted to get similar versions of the original images; then, the embedded data can be extracted and the original image can be reversibly recovered with the data hiding key and the spatial correlation features in natural images. It is reversible; however, the hiding capacity is rather low. In [8], an improvement is proposed to increase the hiding capacity. However, the hiding capacity is still not large enough after the improvement. The separation of data extraction and recovery of original images is achieved in [9].

In this paper we are going to discuss about the process of identifying the region of interest, encryption and decryption of medical images using the proposed methodology and finally results will be evaluated.

2. Proposed Methodology

The process flow of the whole scheme is presented in Figure 1. Firstly, a block-energy-based algorithm is proposed to determine the ROI of the original medical image. Secondly, the preprocessed additional data is embedded into the ROI of the medical image with a histogram modification-based datahiding scheme. Finally, the watermarked image is encrypted utilizing a hyperchaotic system. The decryption and data extraction process are presented in Figure 2. After receiving the encrypted medical image, the receiver

decrypts it to get medical image with watermarks. Then, ROI of the watermarked image is detected. Finally, additional data is extracted and the original image is recovered reversibly.

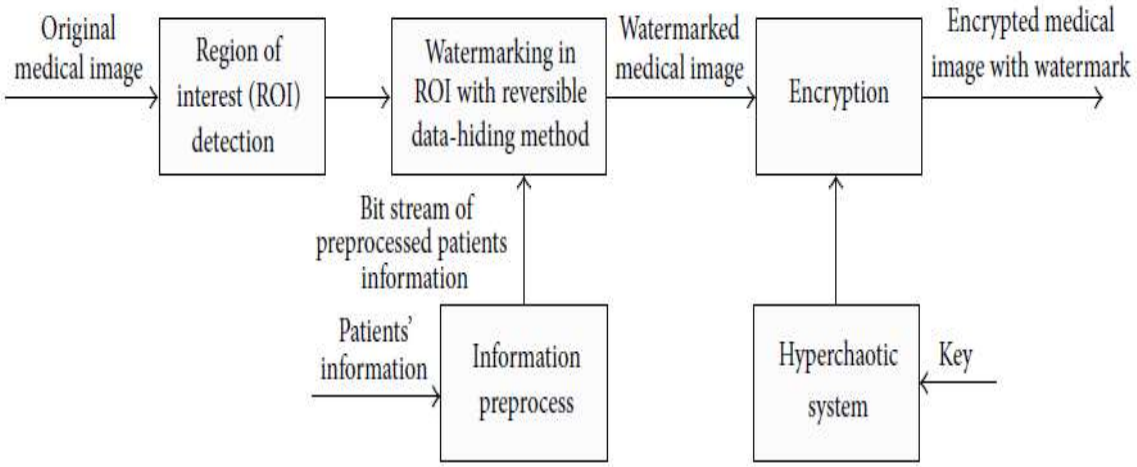


Figure1. Block diagram of proposed embedding and encrypting

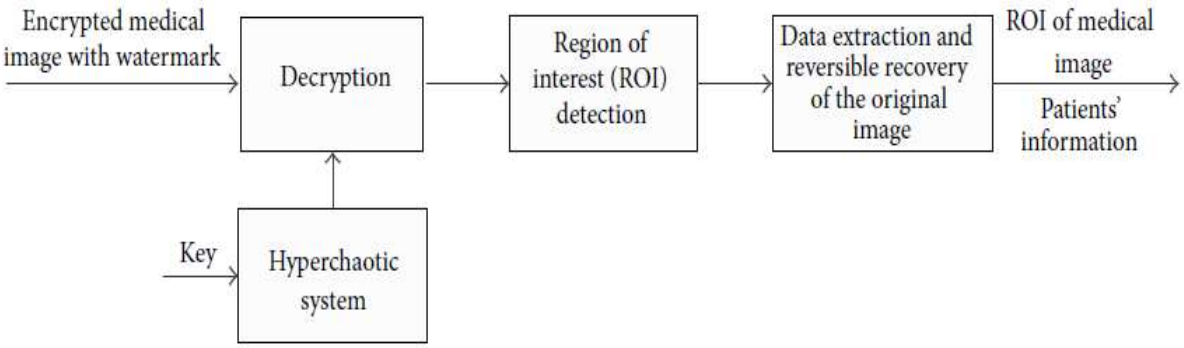


Figure2. Block diagram of decryption and extraction of information

A. ROI Detection

The medical image with size $N1 \times N2$ is firstly divided into blocks with size $n1 \times n2$. Obviously, the amount of blocks is $(N1 \times N2)/(n1 \times n2)$. Then, the average energy of every block is calculated by the following:

$$ave_{energy}(m,n) = \frac{\left(\sum_{i=1}^{n1}\sum_{j=1}^{n2} I(i,j)^2\right)}{(n1 \times n2)} \quad (1)$$

where ave energy (m, n) represents the average energy of the current block, (m, n) represents the position of image blocks, and $I(i, j)$ is pixel value. Finally, compare the average energy value of every block with an adaptive threshold T to determine whether a block belongs to ROI or not: if

ave energy $(m, n) > T$, then it belongs to the ROI; else, the block belongs to the RONI.

B. Reversible Data Hiding Based on Histogram Modification

Additional information is preprocessed and encoded into binary stream before it is embedded into ROI blocks of medical images. A reversible data-hiding algorithm based on histogram of difference image blocks is proposed for the information embedding. This algorithm can be preceded together with ROI detection process. Once one ROI block is detected, it can be used for information embedding immediately.

The threshold T for the detection of ROI of medical images and the sizes of ROI blocks and additional information are encoded as the key for data extraction. The data extraction key can be sent to the receiving end alone or along with the watermarked medical image. It can be encrypted by symmetric encryption algorithm or by the public-key encryption algorithm. In the symmetric encryption scheme, the key for data extraction is encrypted with the same key that is shared between the sending end and the receiving end. In public-key encryption, the data extraction key is encrypted by the public key in the sending end, whereas it can be decrypted

by the private key of the receiver. It is more secure to use the public-key encryption for the delivery of key for data extraction.

C. Encryption Scheme Based on Hyperchaotic System.

The medical image with watermark is encrypted with a series of random numbers. A hyperchaotic system by Gao et al. [28] is used to generate the discrete random numbers for encryption:

$\dot{y}_1 = a(-y_1 + y_2)$,

$\dot{y}_2 = dy_1 + cy_2 - y_1y_3 - y_4)$,

$\dot{y}_3 = y_1y_2 - by_3)$,

$\dot{y}_4 = y_1 + k)$,

where a, b, c, d, and k are parameters, and when a = 36, b = 3, c = 28, d = −16, and $-0.7 \leq k \leq 0.7$, the system is hyperchaotic.

D. Decryption Scheme and Data Extraction

The encrypted medical image with hidden information is received by the remote receiver for diagnosis. The original medical image is reversibly recovered and the information embedded is

extracted with the following steps.

Step1. Generate the encryption sequence E with key $k1$ as the encryption process.

Step2. Do XOR between the encrypted image C and the encryption sequence E

Step3. Divide image P into blocks with the same sizes as that of embedding process, and then calculate the average energy of each block to determine the ROI of the image with threshold T, which is the same as the threshold T of the ROI detection procedure.

Step4. Calculate the differences of pixels in every ROI block to get difference pixel sequence sede (m, n).

Step5. Reversibly recover the original sequence se (m, n) of every ROI block through an iteration of sede (m, n), seem(m, n), and se(m, n) itself: sede (m, n, i) =seem(m, n, i) − se (m, n, i −1) and se (m, n, i) = se (m, n, i − 1) + sed (m, n, i), where sed(m, n, i) is the elements of the sequence sede (m, n).

The reason why the thresholds in the receiving end are the same as the original one is that the embedding process-based histogram of difference image blocks causes little distortion to the original image, which can be ignored in the calculation of average energy of ROI blocks.

3. Results and Discussion

A group of test medical images with different sizes can be considered for performing experimental evaluation. In Figure 3, the sizes of images for test are 512 × 512 respectively.

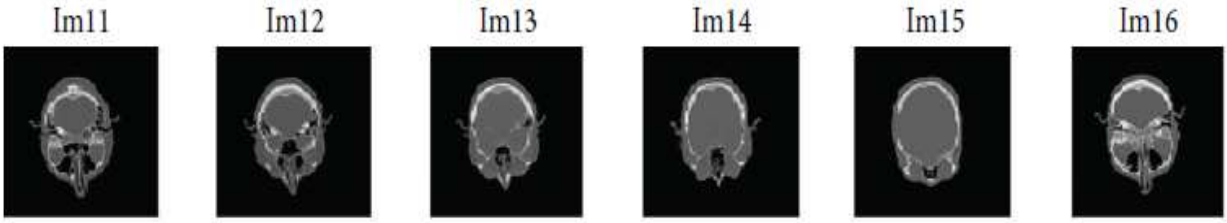


Figure 3. Medical images

ROI Detection

For the tested images with different sizes, such as 512 × 512, 256 × 256, and 128 × 128, different sizes of blocks and different thresholds are utilized. The block size is equal to 32 × 32 for images with size 512 × 512, and the threshold is T = 9; the block size is equal to 16 × 16 for images with size 256 × 256, and the threshold is T =1000; the block size is equal to 8 × 8 for images with size
128 × 128, and the threshold is T = 2000. The test results are presented, respectively, in Figure 4.

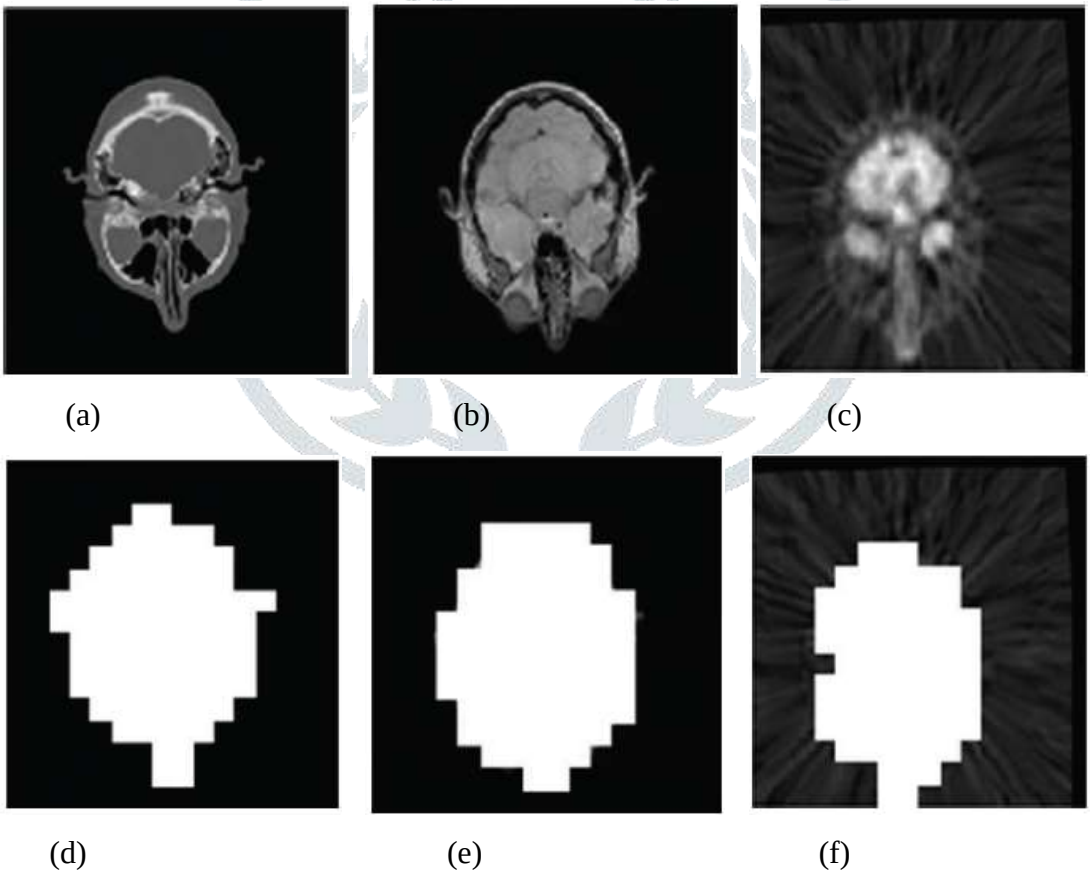


Figure4. ROI detection of different images with different sizes

The original medical images and images after reversible data hiding are presented in Figure 5.

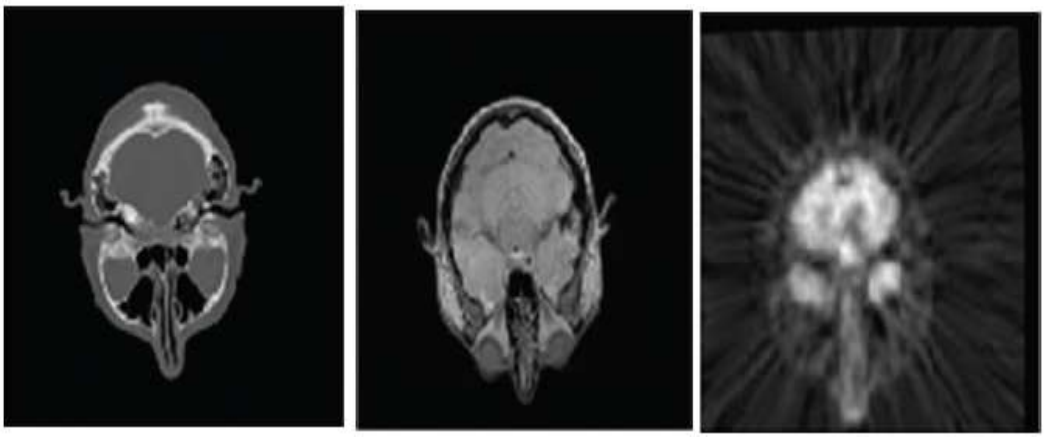


Figure5. Medical images and their corresponding watermarked images

Embedding Capacity and PSNR of Medical Images with Different Sizes

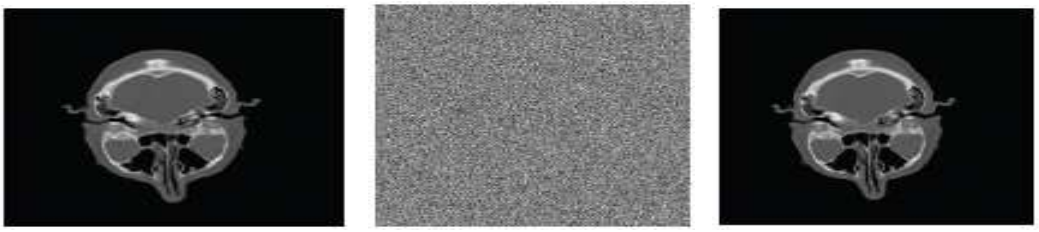
The embedding capacity and the corresponding PSNR of different medical images of different sizes are presented in Tables 1. Medical images of different sizes are divided into different blocks; therefore, the numbers of ROI blocks are different due to the block energy-based ROI detection method. Besides, the thresholds for ROI detection of different medical images are different too.

Table1. Capacity and PSNR of medical images with size of 512 × 512 with block size of 32 × 32

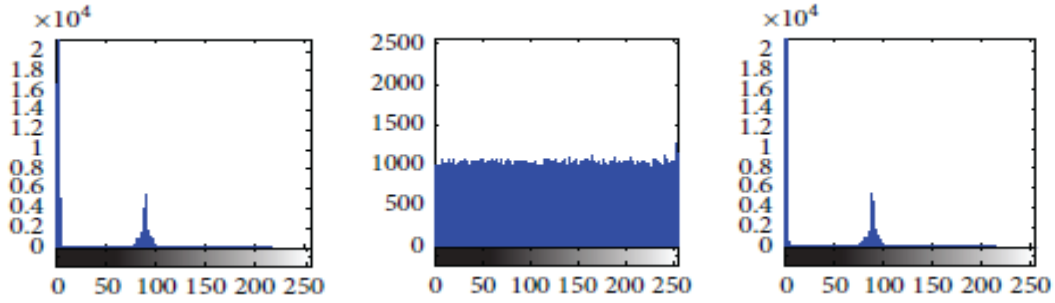
Image	Im1	Im2	Im3	Im4
Capacity (bits)	42617	42593	48997	52359
PSNR (dB)	56.24	56.04	55.70	56.01
ROI blocks number	86	83	85	85
Threshold	9	9	9	9

Encryption and Decryption

The experimental results of encryption and decryption are shown in Figures 6. The watermarked medical images, their encrypted versions, their right decrypted versions, their wrong decrypted versions, and their corresponding histograms with sizes 512 × 512, 256 × 256, and 128 × 128 are presented in the three groups of figures, respectively.



(a) original (b) Encryption (c) Decrypted image



(d)Histogram of (a) (e) Histogram of (b) (f) Histogram of (c)

Figure6. Encryption and decryption of medical image with size 512 × 512

It can be clearly seen that without the correct key, the decrypted images are random noise like pixels. In each group of images and their corresponding histograms, subimage (d) is the decrypted images with random streams. Subimage (e) is the decrypted images with wrong initial values, and only 10−10 difference is introduced in the chaotic system. Actually, the initial values of hyperchaotic system are [12, 2, 9, 1] in the encryption while in the wrong decryption 2 the initial values are [12, 2, 9, 1.0000000001]. Therefore, high sensitivity has been achieved through the hyperchaotic system.

4. Conclusion

An encryption scheme frame for medical image with watermarking is proposed in this paper. Private medical information is embedded into ROI of medical images with a histogram-based reversible data-hiding scheme. The watermarked medical image is encrypted with a hyperchaotic system. In the receiver end, medical information can be extracted and the original medical image can be reversibly recovered. Compared with standalone encryption or watermarking scheme, the proposed scheme is a fusion of encryption and watermark, and it not only has large space of secret key, but it also has large capacity of watermark embedding. Experimental results testified the effectiveness of the scheme.

References

[1] V. Fotopoulos, M. L. Stavrinou, and A. N. Skodras, "Medical image authentication and self-correction through an adaptive reversible watermarking technique," in *Proceedings of the 8th IEEE International Conference on BioInformatics and BioEngineering (BIBE '08)*, pp. 1–5, October 2008.

[2] T. Gao and Z. Chen, "A new image encryption algorithm based on hyper-chaos," *Physics Letters A*, vol. 372, no. 4, pp. 394–400, 2008.

[3] D. Bouslimi, G. Coatrieux, M. Cozic, and C. Roux, "A joint encryption/watermarking system for verifying the reliability of medical images," *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, pp. 891–899, 2012.

[4] X. Zhang, "Separable reversible data hiding in encrypted image," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 826–832, 2012.

[5] X. Zhang, "Reversible data hiding in encrypted image," *IEEE Signal Processing Letters*, vol. 18, no. 4, pp. 255–258, 2011.

[6] X. Zhang, "Separable reversible data hiding in encrypted image," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 826–832, 2012.

[7] W. Hong, T.-S. Chen, and H.-Y. Wu, "An improved reversible data hiding in encrypted images using side match," *IEEE Signal Processing Letters*, vol. 19, no. 4, pp. 199–202, 2012.

[8] A. Lavanya and V. Natarajan, "Watermarking patient data in encrypted medical images," *Sadhana-Academy Proceedings in Engineering Sciences*, vol. 37, pp. 723–729, 2012.

[9] K. W. Wong, "A fast chaotic cryptographic scheme with dynamic look-up table," *Physics Letters A*, vol. 298, no. 4, pp. 238–242, 2002.

[10] J. Fridrich, M. Goljan, and R. Du, "Lossless data embedding for all image formats," in *Electronic Imaging*, vol. 2002, pp. 572–583, 2002.

[11] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 890–896, 2003.

[12] Z. Ni, Y.-Q. Shi, N. Ansari, andW. Su, "Reversible data hiding," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 16, no. 3, pp. 354–361, 2006.