ROI based Selective Plane Medical Image Encryption

Anusudha.K
Department of Electronics Engineering
School of Engineering and Technology
Pondicherry University,
Pondicherry- 605014

Abstract – **Modern healthcare systems are based on managing diagnostic information of patients through E-health. E-health refers to the Internet enabled healthcare applications involving transacting personal health records or information and other internet based services including e-Pharmacy etc. In this paper, a combination of watermarking and encryption are done for secure transaction of medical images. This method is based on selecting the ROI in the image as the watermark. This portion is encrypted by linear feedback shift register based stream ciphering which is again encrypted by the key generated by Diffie Hellman Algorithm. The encrypted ROI is embedded into the medical image by Spread spectrum technique. From the simulation results,the proposed approach proves to be highly secure as two keys are used for encryption and the secret message is spreaded throughout the Medical image.**

Keywords - **Bit Plane Slicing, Region of Interest, Stream Cipher, Diffie-Hellman Algorithm, Spread-Spectrum Watermarking, Peak Signal to Noise Ratio (PSNR)**

I. INTRODUCTION

Processing and handling medical information by computers and sharing them over high speed network infrastructure have become a common practice since wide deployment of low cost computing and networking hardware [3, 8]. In the last decade, uses of advanced electronic and digital equipment in healthcare services has been found to increase many fold. Physicians diagnose based on the electronic and digital data [4]. Exchange of medical images between hospitals located in different geographical locations is also on the rise. But unfortunately, this exchange of medical images through insecure open networks -Internet adds top potential risk of espionage provides of changes to occur in medical images and consequently creates a threat of undesirable outcome because little important information contained in the image gets lost or corrupted.

Large image databases have been handled in hospitals both for clinical and research purposes. These image databases need to be protected against malicious attacks and made more beneficial by annotating early-diagnosis related information. For this purpose, authentication of the medical images such as X-ray, MRI, Ultrasound, etc can be performed through watermarking, whereby an invisible watermark (secret message) related to the host image is inserted in the host image itself [18-19]. The secret message can not only make authentication of the host image, but could also be helpful in embedding extra/auxiliary information related to the host image. Secret embedding of the watermark signal, no matter how much invisible it may be, can cause degradation to the resultant image quality. Therefore, reversible watermarking is applied to overcome this drawback by applying a mechanism that can provide the exact original image after the watermark has been successfully extracted [12,17]. Traditional approaches such as cryptography can also perform this reversibility operation but the basic shortcoming is the loss of semantic information of the host image, i.e., after encryption the image may not be visible/understandable, which is not the case in watermarking.

Some of the existing methods are Zhou et al [11] presents a watermarking method for verifying the authenticity and integrity of a digital mammography image. The authors have used a digital envelope as watermark and the least significant bits (LSB) of one random pixel of the mammogram are replaced by one bit of the digital envelope (DE) bit stream. Instead of the whole image data, only partial image data is used. Wang et al [13,14] proposed to embed secret messages in moderately significant bit of the cover image. A genetic algorithm is developed to find the optimal substitution matrix for embedding of the secret messages. The authors have also proposed to use a local pixel adjustment process (LPAP) to improve the image quality of the stego-image. Unfortunately, since the local pixel adjustment process only considers the last three least significant bits and the fourth bit but not all bits, the local pixel adjustment process is obviously not optimal. As the local pixel adjustment process modifies the LSBs, the technique cannot be applied to data hiding schemes based on simple LSB substitution.

The remaining section of this paper is outlined as follows. Section II and III briefly introduces Bit Plane Slicing and Stream Ciphering. Section IV explains the Diffie Hellman Key exchange. Spread spectrum Watermarking is discussed in section V. Section VI explains the proposed scheme. The experimental results are listed in section VII. Section VIII is devoted for conclusion.

II. BIT PLANE SLICING

Instead of highlighting gray level images, highlighting the contribution made to total image appearance by specific bits might be desired. Suppose that each pixel in an image is represented by 8 bits. Imagine the image is composed of 8, 1-bit planes ranging from bit plane1-0 (LSB)to bit plane 7 (MSB).In terms of 8-bits bytes, plane 0 contains all lowest order bits in the bytes comprising the pixels in the image and plane 7 contains all high order bits.

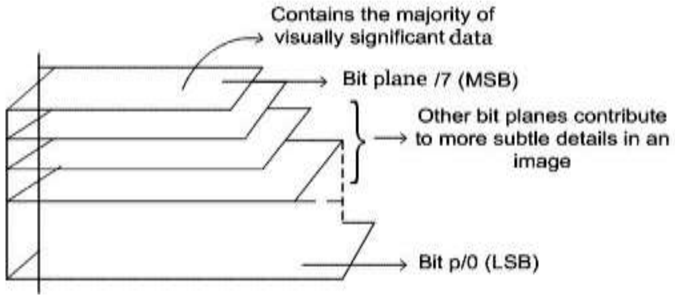

Contains the majority of visually significant data
Bit plane /7 (MSB)
Other bit planes contribute to more subtle details in an image
Bit p/0 (LSB)

Figure 1: Bit Plane Slicing

Separating a digital image into its bit planes is useful for analyzing the relative importance played by each bit of the image, implying, it determines the adequacy of numbers of bits used to quantize each pixel, useful for image compression[10].

In terms of bit-plane extraction for a 8-bit image, it is seen that binary image for bit plane 7 is obtained by proceeding the input image with a thresholding gray-level transformation function that maps all levels between 0 and 127 to one level (e.g. 0)and maps all levels from 129 to 253 to another (e.g. 255).

III. Stream Ciphering

Algorithms of flux ciphering (stream ciphers) can be defined as being algorithms of ciphering by blocks, where the block has a unitary dimension (1 bit, 1 byte, etc.) or relatively small. Their main advantages are their extreme speeds and their capacity to change every symbol of the plaintext. Besides, they are less numerous than those of ciphering by blocks, they are useful in an environment where mistakes are frequents, because they have the advantage of non-propagation [7].

Current interest in stream cipher is most commonly attributed to properties of the one-time pad, called the Vernam cipher. It uses a string of bits that is completely random generated. The key stream has the same length as the plaintext message. The random string is combined using *exclusive OR* operations with the plaintext to produce the cipher text.

The Linear Feedback Shift Register (LFSR), illustrated Figure.2, is a mechanism very often applied in applications that require very fast generation of a pseudo-random sequence. The symmetrical ciphering uses LFSR to generate some pseudo-random bit sequences called register's vector. This vector is generally the key of the ciphering process and it is defined in relation to a meter. For every iteration, the content of the register is baffled toward the right of a position, and the XOR operation is applied on one under whole of bits whose result is placed to the left extreme of the register

Figure 2: Linear Feedback Shift Register Method

IV. Diffie hellman key exchange

Diffie–Hellman key exchange (D-H) is a specific method of exchanging cryptographic keys. It is one of the earliest practical examples of key exchange implemented within the field of cryptography. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher [9].

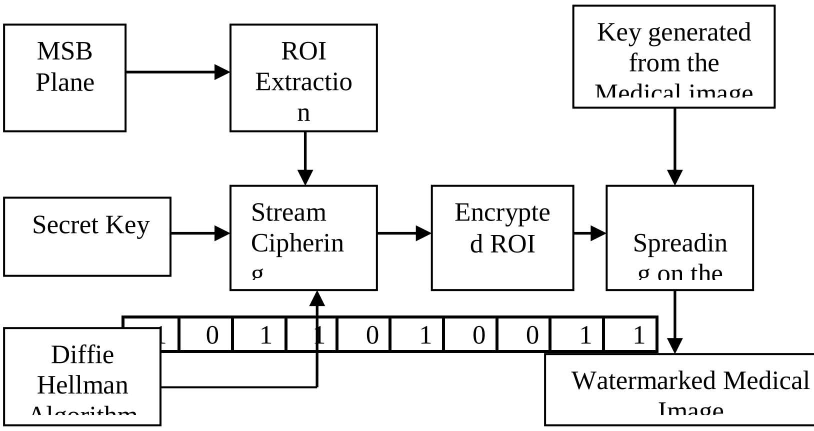
Suppose A& B are two parties:

- A &B wants to agree on a secret key.
- They agree on two large no. n & g such that $1<g<n$.
- A chooses randomly X and computes $X=g^x$ mod n & send X to B
- B chooses randomly Y and computes $Y=g^y$ mod n & send Y to A
- A computes $K_1 = Y^x$ mod n
- B computes $k_2= X^y$ mod n
- $K_1=K_2 =g^{xy}$ mod n.

V. Spread Spectrum Watermarking

The watermark to be embedded is spreaded throughout the cover object, thereby causing very less visible distortions to the watermarked cover Image. The key used as the reference for the embedding process is generated from the cover object there by increasing the level of security. Spreading technique is said to be an efficient method for watermarking as the security level is high and the size of the watermark is comparatively small with the cover object. Some of the salient features are:

- The watermark verification process knows the location and content of the watermark, it is possible to concentrate these weak signals into a single output with high SNR.
- In order to place a length n watermark into an N×N image, the N×N DCT of the image is computed and watermark is placed into the n highest magnitude coefficients (which are data dependent) of the transformed image, excluding the DC component (not necessary).



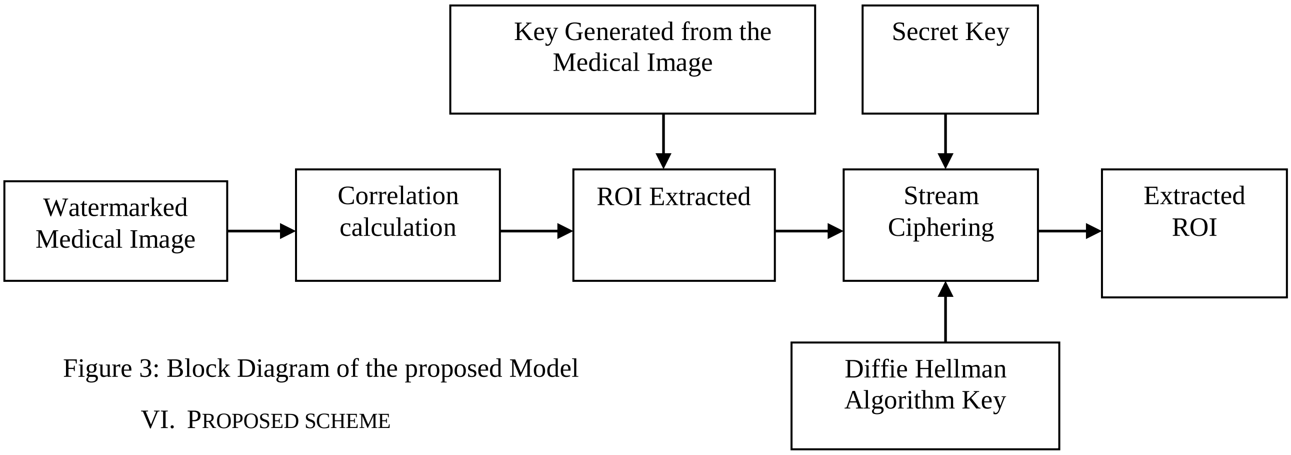

Key Generated from the Medical Image
Secret Key
Watermarked Medical Image
Correlation calculation
ROI Extracted
Stream Ciphering
Extracted ROI
Diffie Hellman Algorithm Key

Figure 3: Block Diagram of the proposed Model

VI. Proposed scheme

The proposed scheme aims at providing a combined watermarking and encryption scheme which uses spread spectrum watermarking and Diffie Hellman Key exchange encryption. Figure 3.Depicts the block diagram of the proposed scheme.

A. Embedding Process

Step 1: The region of interest (ROI) portion is extracted from the MSB Plane of the Image.

Step 2: PRNG is performed on 64 bit random binary number and the final bit stream is divided into groups of eight bits to form eight 8 bit key sequences.

Step 3: The pixel values of the ROI portion is encrypted by stream ciphering technique .The entire portion is divided into 8x8 blocks and each pixel is multiplied with the 8 bit key sequences.

Step 4: The same 64 bit random binary sequence is used for generating the Diffie Hellman Key generation.

Step 5: The key generated by the Diffie Hellman algorithm is added to every encrypted stream ciphered pixel Values thereby the Encrypted portion of ROI is obtained which acts as the Watermark.

Step 6: A pseudo random key generated from the medical image is used for spreading the encrypted watermark on to the medical image to generate the watermarked medical image.

B. Extraction process

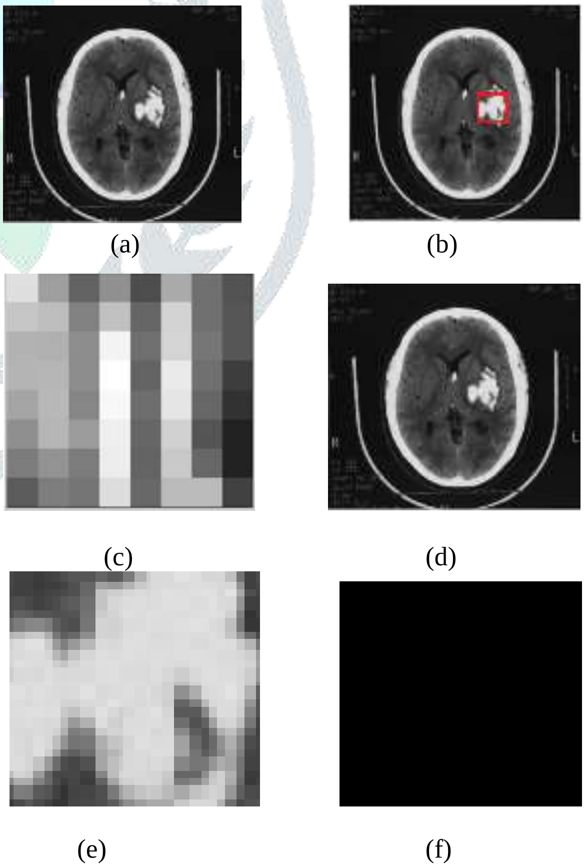
Step 1: The correlation between the received watermarked image and the Pseudo random sequence is calculated.

Step 2: The correlation value is used as the threshold for despreading the watermark

Step 3: The obtained watermark is decrypted by the Diffie Hellman algorithm key and the 64 bit sequence.

VII. Experimental results and discussion

In this section, experimental results are demonstrated to show the effectiveness of the proposed Digital watermarking and encryption scheme. The proposed scheme is simulated using MATLAB R2014 on a PC with Intel core i5-650, 3.2 GHz, 2GB memory, 250 GB hard disk with window 7 professional operating system. A number of standard 256 x256 images obtained from DICOM open source are used for the simulation purpose. The performance of the proposed algorithm is used on an MRI image as shown in Figure.4



(a) (b)

(c) (d)

(e) (f)

Figure.4 (a) MRI Image (512x512) (b) ROI portion of the Cover image (c) encrypted ROI (d) Watermarked MRI image (e) Zoomed retrieved ROI from the watermarked Image (f) Difference between the MRI image and the watermarked image

A. Performance Metrics

The performance evolution of the watermarking approach is analyzed against various attacks. The Peak-Signal-to-Noise Ratio is defined as:

$$PSNR = \frac{10log_{10}(255)^2}{MSE}$$

Where 'MSE' is the mean squared error between the original and distorted image and is defined as follows:

$$MSE = \frac{1}{mn}\sum_{i,j=0}^{m-1,n-1}[I(i,j) - K(i,j)]$$

Where m, n gives the size of the image and $I(i,j), K(i,j)$ are the pixel values at location (i,j) of the original and distorted image respectively .However, robustness is measured by the normalized correlation (NC) and calculated using:

$$NC = \frac{\sum_{i,j} W(i,j) * W'(i,j)}{\sqrt{\sum_{i,j} W(i,j)^2}\sqrt{\sum_{i,j} W'(i,j)^2}}$$

Where $W(i,j)$ is the reference image and $W'(i,j)$ is the watermarked image. Table 1 shows the PSNR, NC for the sample images subjected to various attacks.

The Number of pixel change per rate gives the changes happening to the pixels of the watermarked image to that of the host image.

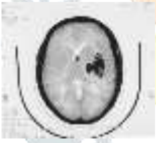
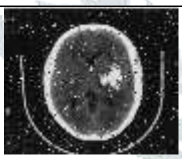
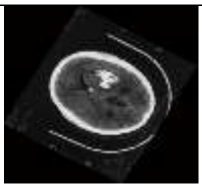
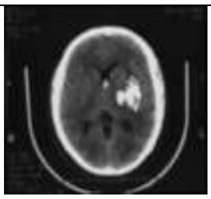
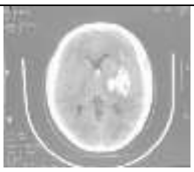
$$NPCR = \frac{\sum D(i,j)}{W \times H} \times 100\,\%$$

The unified average change in intensity is calculated using:

$$UACI = \frac{1}{W\times H}[\sum_{i,j}\frac{W(i,j)-w'(i,j)}{2^L-1}]$$

Table .2 shows the entropy, NPCR and UACI values for the watermarked images. The standard NPCR value for an encrypted image is 1 and the UACI value is 0.5.

Table.1 Watermarked Image subjected to Various Attacks

ATTACKS	IMAGES	MSE	PSNR (dB)	NC
Negative Transform		0.2567	54.2315	0.98
Noise Attack (Salt & Pepper) 0.2 0.4 0.6 1		0.3001 0.3210 0.3210 0.5915	54.2540 53.1151 52.5640 50.0976	0.98 0.97 0.99 0.96
Rotation 45^o 60^o 90^0		0.2965 0.3174 0.4978	54.9824 53.6561 51.7862	0.99 0.98 0.99
Smoothening		0.3224	53.1432	0.99
Gamma correction 0.6 0.4 0.2		0.3120 0.3967 0.4328	55.1245 53.4645 50.3131	0.99 0.96 0.97

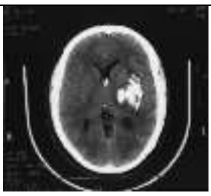
Contrast Stretching		0.4367	50.2145	0.96

Table.2 Parametric values for the Watermarked Medical Image

Watermarked Medical Image	Entropy	NPCR	UACI	Correlation Co-efficient		
				Horizontal	Vertical	Diagonal
MRI	7.90	0.97	0.33	0.0012	0.0014	- 0.0031

VIII. Conclusion

This paper presents a method that provides secure medical image transaction based on a hybrid algorithm Bit plane Slicing, Stream Ciphering, Spread Spectrum watermarking and Diffie Hellman Key exchange. The advantages of both encryption algorithms, with secret key and with public-key are used. This method is based on selecting the ROI in the image

as the watermark. This portion is encrypted by linear feedback shift register based stream ciphering which is again encrypted by the key generated by Diffie Hellman Algorithm. The encrypted ROI is embedded into the medical image by Spread spectrum technique. The effectiveness of the proposed algorithm is verified against various attacks. The proposed system uses the power of Spread spectrum and Diffie Hellman Key Exchange. The comprehensive simulation study of the proposed algorithm also demonstrates the improved security

References

[1] J. Bernarding, A. Thiel, and A. Grzesik, "A JAVA-based DICOM server with integration of clinical findings and DICOM-conform data encryption," International Journal of Medical Informatics, vol. 64, pp.429–438, 2001.

[2] C.C. Chang, M.S. Hwang, and T-S Chen. "A new encryption algorithm for image cryptosystems". The Journal of Systems and Software, vol. 58, pp.83–91, 2001.

[3] K.L. Chung and L.C. Chang., "Large encrypting binary images with higher security" Pattern Recognition Letters, vol, 19, pp.461–468, 1998.

[4] R. Norcen, M. Podesser, A. Pommer, H.P. Schmidt, and A. Uhl. "Confidential storage and transmission of medical image data". Computers in Biology and Medicine, vol, 33pp, 277–292, 2003.

[5] F. Y. Shih and S. Y.T.Wu. "Combinational image watermarking in the spatial and frequency domains" Pattern Recognition, vol.36, pp.969–975, 2003.

[6] A. Sinha and K. Singh. "A technique for image encryption using digital signature" Optics Communications, vol.218, pp.229–234, 2003.

[7] J. Cox, J. Kilian, F. T. Leighton, and T.Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Trans. Image Processing, vol. 6, pp. 1673-1687, Dec-1997.

[8] Diffie W., Hellman M. "New directions in cryptography", IEEE Transactions on Information Theory, vol. 22, pp. 644-654 1976.

[9] Francois J., Raymond A.," Security Issues in the Diffie-Hellman Key Agreement Protocol" IEEE Trans. on Information Theory, pp.1–17,1998.

[10] Wang Yan and Ling-di Ping, "A New Steganography Algorithm Based on Spatial Domain", Journal on Information Science and Engineering, vol. 6, pp.45-51, 2009.

[11] Zkou, X.Q., Huang, H.K. and Lou, S.L., "Authenticity and integrity of digital mammography images". IEEE Transactions on Medical Imaging, **20**(8), pp. 784-791, 2001.

[12] C.-S Woo, "Digital Image Watermarking Methods for Copyright Protection and Authentication", PhD Thesis, Queensland University of Technology, Australia, March2007.

[13] C. Wu, R. Cathey, "Digital Watermarking: A Comparative Overview of Several Digital Watermarking Schemes", available at: http://www.csam.iit.edu/cs549/cs549/project / presentation report.pdf.

[14] Wang Yan and Ling-di Ping, "A New Steganography Algorithm Based on Spatial Domain",Journal on Information Science and Engineering ,vol 6,45-51,2009.

[15] Ran Zan Wang, Chi-Fang Lin, Ja Chen Lin, "Hiding data in images by optimal moderately significant bit replacement" Pattern Recognition, Vol 3, pp 671-683, 2001.

[16] Cao, F., Huang, H.K. and Zhou, X.Q., "Medical image security in a HIPAA mandated PACS environment. Computerized Medical Imaging and Graphics", IEEE transaction on Image Processing 27(2-3), pp. 185- 196, 2003.

[17] Chao, H.M., Hsu, C.M. and Miaou, S.G.,"A data-hiding technique with authentication, integration, and confidentiality for electronic patients records", IEEE Transactions Information Technology in Biomedicine, 6, pp. 46-53, 2002.

[18] K. Youngberry, "Telemedicine Research", Journal of Telemedicine and Telecare, Vol. 10, No. 2, pp. 121-123, 2004.

[19] R. Wootton, J. Blignault, J. Cignoli, "A National Survey of Telehealth Activity in Australian Hospitals", Journal of Telemedicine and Telecare, Vol. 9(supplement 2),pp. 73-75, 2003.