ISSN (Print) : 2320 – 3765
ISSN (Online) : 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
*Vol. 2, Issue 4, April 2013*

# ROI Based Double Encryption Approach for Secure Transaction of Medical Images

**Vratesh Kumar Kushwaha[1], K. Anusudha[2]**

M.Tech Scholar, Dept. of Electronics Engineering, Pondicherry University, Puducherry, India[1]

Assistant Professor, Dept. of Electronics Engineering, Pondicherry University, Puducherry, India[2]

**Abstract:** The main focus is on enabling, supporting process in the health care industry for implementing a secure, robust and privacy complaint system for the safe distribution and use of medical image. In this paper, a new method that combines image encryption and watermarking technique for safe transaction of medical image is proposed. 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 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

The amount of digital medical images has increased rapidly in the Internet. The necessity of fast and secure diagnosis is vital in the medical world. Nowadays, the transmission of images is a daily routine and it is necessary to find an efficient way to transmit them over the net. In this paper we propose a new technique to cipher an image for safe transmission. Our research deals with image encryption and watermarking [3, 2, 6].

Watermarking can be an answer to make secure image transaction. For applications dealing with images, the watermarking objective is to embed secret message inside the image. The length of the transmitted message can be relatively important, in fact, longer that just for identification. Insertion can be made in different ways according to the length of the message or desired robustness. The combination in the spatial and frequency domains for the image watermarking is also possible. [5]

An encryption method which depends on the secrecy of the encryption algorithm is not considered to be a true encryption method. The existing encryption methods are based on secret keys and not on secrecy of encryption algorithms. In the traditional approach, the image is encrypted with a secret key method.

The encryption can be done by block or by stream. But the encryption block methods applied to image, have presented two inconvenient. The first one was when you have homogeneous zones; all blocks of this kind are encrypted on the same manner. The second problem was that block encryption methods are not robust to noise. The stream cypher method is robust to moderate noise like JPEG compression with high quality factor. To embed the secret key in the image we have used a spread-spectrum watermarking method. We have chosen to work in the spatial domain because of the robustness to JPEG compression of the stream cypher method [1, 4].

The paper is organised in such a way that the section II explains the Bit plane slicing, section III explain the Stream cipher, section VI explain the proposed scheme ;section VII shows the simulation results for different inputs. Finally, section VIII summarises the paper.

## 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.

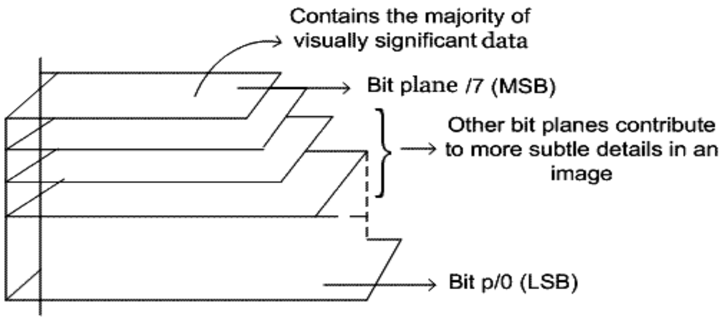

Contains the majority of visually significant data
Bit plane /7 (MSB)
Other bit planes contribute to more subtle details in an image
Bit p/0 (LSB)

**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.

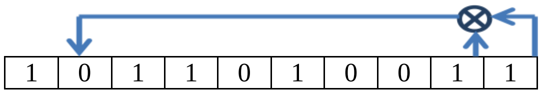
In terms of bit-plane extraction for a 8-bit image, it is seen that binary image for bit plane 7 is obtained by proceeding the input image with a thresholding gray-level transformation function that maps all levels between 0 and 127 to one level (e.g. 0)and maps all levels from 129 to 253 to another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

## III. STREAM CIPHER

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 [4].

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 1, 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



| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 |

**Figure 2** Linear feedback shift resister 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 want to agree on a secret key.
- They agree on two large no. n & g such that 1<g<n.
- A choose random X computes $X=g^x$ mod n & send X to B
- B choose random Y computes $Y=g^y$ mod n & send Y to A

- A computes $K_1 = Y^x \bmod n$
- B computes $k_2 = X^y \bmod n$
- $K_1 = K_2 = g^{xy} \bmod n$.

## V. WATERMARKING

Digital watermarking is the process of embedding digital information into another for copyright protection, authentication and ownership verification. Fig 2 depicts the basic block diagram of the embedding and detection process of the watermarking technique.

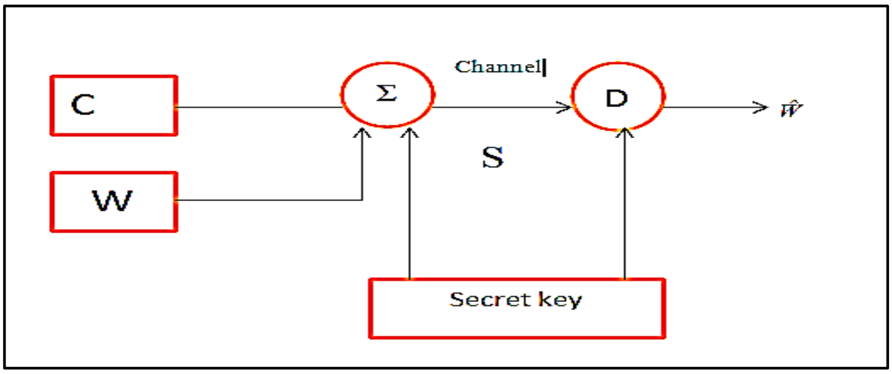


**Figure**.3 Basic block diagram of watermarking

$$S=\Sigma(c, w, k)\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots..\ldots..4.1$$

$$\hat{W} = D(S, K)\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots..\ldots4.2$$

- S=Stego image
- Σ=Embedder
- D=Detector
- C=Host Image
- W=Watermark
- K=Secret key
- $\hat{W}$ =Watermarked Image

### *A. Spread Spectrum Watermarking*

- A watermark is spread over many frequency bins so that the energy in one bin is very small and certainly undetectable.
- Because 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.

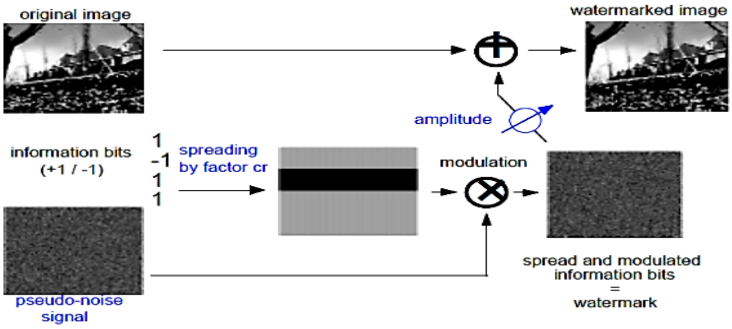


**Figure 4** Spread-spectrum watermark embedding

- 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).

- A watermark consists of a sequence of real numbers X = $x_1$ , … , $x_n$, where each value $x_i$ is chosen independently according to N(0,1) : normal distribution assumption
- When we insert X into V to obtain V ' we specify a scaling parameter α, which determines the extent to which X alters V.[7]

## VI.METHODOLOGY

### *A. Encryption Process*

Step 1: Select the MSB plane from the Medical Image using Bit plane slicing.
Step 2: Select the ROI from the MSB plane.
Step 3: A 64-bit secret key is generated by LFSR and the image is stream ciphered.
Step 4: A public key is generated by Diffie Hellman Algorithm and added to every encrypted pixel of the ROI.

$$P'(n)=p(n)+\alpha(1)p'(n-1)+\alpha(2)p'(n-2)+\ldots+\alpha(k-1)p'(n-k-1)+\alpha(k)p'(n-k)\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots5.1$$

Step 5: The encrypted ROI acts as the watermark and it is spread spectrum watermarked throughout the image.

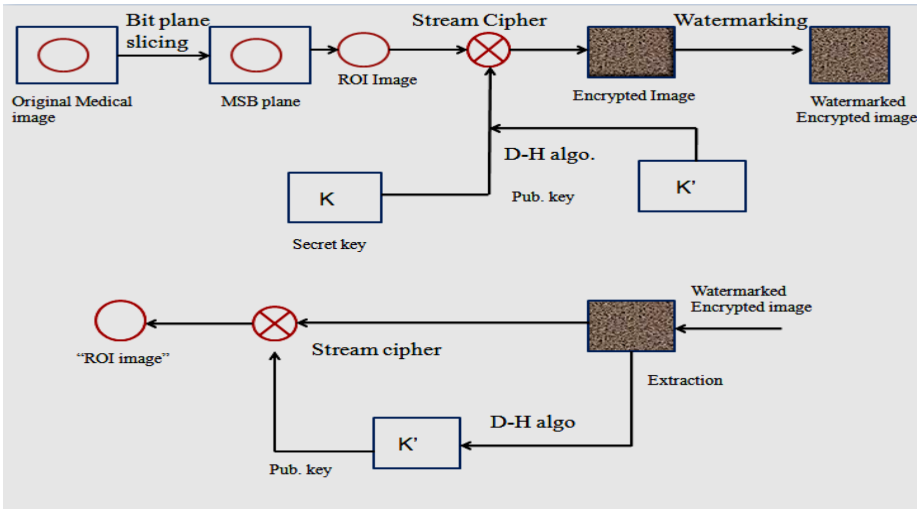


**Figure 5** Crypto-Watermarking processes

### *B. Decryption Process*

Step1: Select the encrypted watermark image for extraction.
Step2: The extracted image is deciphered by stream cipher by using a64-bit secret key.
Step3: A public key is generated by Diffie – Hellman algorithm and add to every extracted pixel of the encrypted image.
Step4: The ROI image is finally received at the receiving end.

## VII. SIMULATION RESULTS

The scheme was tested for different medical images i.e. MRI, CT-scan and X-ray images. A MRI image of size 256x256 was taken as cover image and the ROI of the image is taken as the watermark. A 64 bit secret key is used for stream ciphering. A public key is generated by Diffie Hellman algorithm by increasing the level of security.

### *Peak Signal-To-Noise Ratio*

PSNR is most commonly used to measure of quality of reconstruction of lossy compression codecs (e.g., for image compression). PSNR is most easily defined via the mean squared error (*MSE*).

$$\text{PSNR}= 10\log_{10} (255)^2/\text{MSE} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots7.1$$

### *Mean Squared Error*

MSE of an estimator is one of many ways to quantify the difference between values implied by an estimator and the true values of the quantity being estimated. MSE measures the average of the squares of the "errors."

$$MSE=\frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j)-K(i,j)]^2\ldots\ldots\ldots\ldots\ldots7.2$$

The proposed algorithm is checked for fidelity and the PSNR value of **48.49dB** was obtained

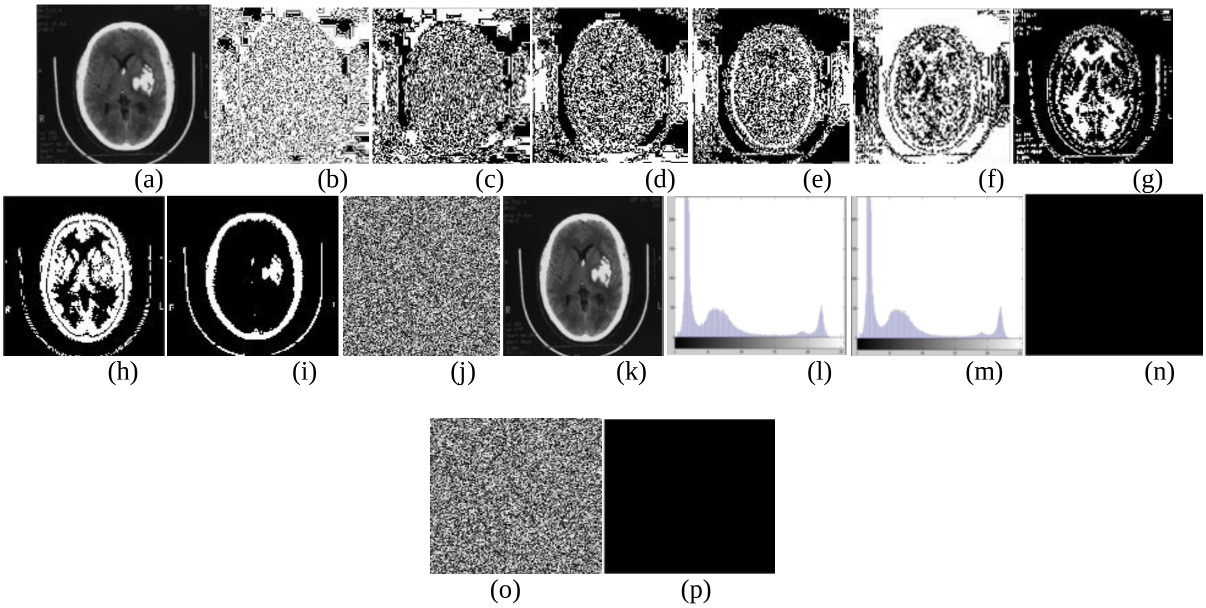


**Figure 6**: a) original image, (b),(c),(d),(e),(f),(g),(h),(i)slices of the image,(b)LSB plane and (i)MSB plane (j)Encrypted ROI (k) watermarked encrypted image with 64-bit key (l) original image histogram, (m) histogram of the image (j), (k), (n) Difference between the encrypted image and the watermarked encrypted image, (o) decryption of the watermarked encrypted image, (p) Difference between original image and decrypted watermarked one. (* Images are resized to fit in the column)

## VIII CONCLUSION

A method is presented that combines encryption and watermarking for image safe transaction purpose. The advantages of both encryption algorithms, with secret key and with public-key are used. In combination method, to encrypt the image with secret key and Diffie-Hellman algorithm with public key, stream cipher method is chosen. The stream cipher method is robust to moderate noise like JPEG compression with high quality factor. To embed the secret key in the encrypted image spread-spectrum watermarking method is used . Simulation results prove that the proposed approach meets fidelity and an appreciated PSNR value.

## 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] C.-S Woo, "Digital Image Watermarking Methods for Copyright Protection and Authentication", PhD Thesis, Queensland University of Technology, Australia, March2007.
[12] 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.
[13] 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.
[14] 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.
[15] K. Youngberry, "Telemedicine Research", Journal of Telemedicine and Telecare, Vol. 10, No. 2, pp. 121-123, 2004.
[16] 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.

## BIOGRAPHY

**Vratesh Kumar kushwaha** received the B. Tech degree in Electronics and Communication Engineering from the utter Pradesh technical university, utter Pradesh in 2010. Currently, he is studying M. Tech in the Dept. of Electronics Engineering, School of Engineering and Technology, Pondicherry University, Puducherry, India.

**K.Anusudha** received the B.E degree (2002) in Electronics &Communication from Madras University, M. Tech degree (2004) in communication system from Anna University, India. She is currently pursuing Ph.D. She is currently working as Assistant Professor in the Dept. of Electronics Engineering, School of Engineering and Technology, Pondicherry University, Puducherry, India. Her research interests include Digital data security, Digital watermarking and Forensic informatics.