J. Basic. Appl. Sci. Res., 3(6)488-495, 2013

ISSN 2090-4304
Journal of Basic and Applied Scientific Research
www.textroad.com

Hash based Medical Image Authentication and Recovery using Chaos and Residue Number System

[1, 3, 4] Muhammad Tahir Naseem, [1, 2, 3] Ijaz Mansoor Qureshi, [1, 3] Tanvir Ahmed Cheema [1, 3, 4] Atta-ur-Rahman

[1] School of Engineering & Applied Sciences (SEAS), ISRA University, Islamabad Campus, Pakistan
[2] Department of Electrical Engineering, Air University, Islamabad, Pakistan
[3] Institute of Signals, Systems and Soft computing (ISSS), Islamabad, Pakistan
[4] Barani Institute of Information Technology, Rawalpindi, Pakistan

ABSTRACT

—Digital watermarking in medical images can ensure the authenticity of the image. This paper proposes a novel reversible and fragile watermarking scheme for medical images based on a chaotic key and Residue number system. Only Region of interest (ROI) of the image is residued. In making residues of ROI part some residues exceed bit size eight. So these residues are converted to eight bits by applying some trick. Hash of the whole image but with residued ROI is embedded in Region of non-interest (RONI) pixels of original image based on the chaotic key. A simple reversible method was used to minimize processing time. The embedded watermark was successfully removed and exact image was restored to its original state. In case of tampering, the hash changes and is easily detectable.

KEYWORDS: Fragile watermarking, Reversible watermarking, Residue Number System(RNS), Chinese Remainder Theorem (CRT), Chaos, Hash, Region of interest (ROI), Region of non-Interest (RONI).

1. INTRODUCTION

Advancement in medical information systems has changed the way patient records are stored, accessed and distributed. In England, 75% of the hospitals computer system failed to have adequate password scheme, 65% of the hospitals that have link to external computer systems do not have adequate security measures and 80% of the hospitals do not have policies on access control to the patient medical records [1]. The integrity of the records such as medical images needs to be protected from unauthorized tampering. Current security measures used to protect the integrity of the patient records are VPN (Virtual Private Network), data encryption and data embedding [2].

Data encryption is being used on the Internet to protect sensitive data during transmission. It is also being used to protect medical images in the form of digital signature. The problem with digital signature is that it needs to be transmitted together with the image in a separate file or in the image header. There is also a risk of losing the signature during transmission. The signature will also be lost if the image file is converted to another format that does not allow headers. Currently, there is no standard for implementation of digital watermarking. Watermark provides mainly three objectives in medical images [3]:

- data hiding; to embed information to make the image useful or easier to use;
- integrity control; to verify that the image has not been modified without authorization;
- authenticity; to verify that the image is really what the user supposes it to be.

In practice, diagnoses have been performed on medical images before being directed to the long-term storage. Thus the significant part of the image is already being determined by doctors involved in the diagnosing process [4]. The significant part is called ROI. Since information in medical images is not to be modified in any way, the watermark is usually being embedded in the RONI as this region does not contribute to the process of diagnosis. Another option is to allow the watermark to be reversible. The usage of ROI in watermarking in medical images had been used where ROI and RONI were defined before the process of watermark embedding. Reversible watermarking is where embedded watermark is removed and the original pixel value is restored.

In [5], a watermarking scheme is introduced where information describing the image is embedded into medical images and can be reversed later on. The ability to localize tampering of a watermarked image is crucial for authentication. Once tampering is localized, tampered section can be recovered. In [6], the author divides the medical image into blocks and each block is embedded with the authentication message and recovery information of other blocks. Tampered blocks can then be restored using this information.

In this paper, we are proposing Residue Number System along with chaotic key for reversible and fragile watermarking in medical images. ROI part of image is residued only. Moreover, when the ROI part of image is residued, there are some pixel pairs which exceed size eight. So some mapping is done by applying some trick on those pairs to bring them back to size eight. On the

*Corresponding Author: Muhammad Tahir Naseem, School of Engineering & Applied Sciences (SEAS), ISRA University, Islamabad Campus, Pakistantahir.naseem@biit.edu.pk

basis of chaotic key, LSB's of 256 pixels in RONI are made zero then this RONI is rearranged with residued ROI and hash is generated for the whole image which acts as a basis of watermark. This will give us 256 bit hash. Again on the basis of same chaotic key, 256 bits of hash are embedded at same 256 pixels in RONI by replacing the LSB's. On the receiver side, on the basis of chaotic key, watermark is extracted and is compared with hash of un-watermarked image to check whether image has been tampered or not. Moreover, original image is not needed on the receiver side, which makes the proposed scheme blind.

The rest of the paper is organized as follows: Section 2 describes the watermarking domains. Review on medical image watermarking is described in section 3. In section 4, residue numbers system is described. Section 5 describes about chaos in watermarking. Section 6 describes the proposed watermarking scheme. In section 7 some experiments are shown demonstrating the fragility of the proposed scheme and then we give finally our conclusion in section 8.

2. WATERMARKING DOMAINS

A general watermarking scheme consists of an encoder that embeds the information and a decoder for the detection of the information. The encoder embeds the watermark W inside original image I by using embedding function E as in Eq.(1).

$$E(I, W) = I_W \qquad (1)$$

Watermark can be any information such as a logo, user information or image dependant information.

The decoder D will extract the watermark W from the original image as shown in Eq.(2). Some methods allow the detection or extraction of watermark without the original image, such type of watermarking schemes are called blind detection schemes and the proposed watermarking scheme is also blind.

$$D(I, I_W) = W \qquad (2)$$

Watermarking can be done in two domains; spatial domain or in transform domain. In spatial domain, watermark is embedded into the LSBs (Least Significant Bits) of the image. Since a change in LSB corresponds a change in one unit of image gray value, its modification is not perceivable by human eyes. This technique is not as robust as transform domain techniques are. The transform domain techniques embed watermark information into the transform coefficients of the cover image by taking DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform) or DFT (Discrete Fourier Transform) of image. These methods are complex but are more robust than spatial techniques.

3. PREVIOUS WORK ON MEDICAL IMAGE WATERMARKING

Main requirement of an effective watermarking based authentication system is the ability to identify the tampered area where the authentication watermark should be able to detect the location of manipulated areas, and verify other areas as authentic [7]. Tan et al. in [8] proposed a tamper localization watermarking scheme that uses pixel value modification in order to allow the watermark to be reversible by dividing the image into 16x16 pixel blocks and computing Cyclic Redundancy Code (CRC) for each block. Each CRC is embedded into its own block and in the event that the CRC cannot be embedded into its own block, the remaining bits will be carried over to the next block. The watermarked image can be verified by extracting the watermark and the CRC of each block is being compared.

Chiang et al. in [9] proposed a reversible tamper localization scheme with tampered region recovery capability. This scheme is based on a difference expansion scheme. It was modified to allow the watermark to be embedded into the transform domain by using integer Haar wavelet transform by dividing the image into blocks. The recovery information is generated by taking the average pixel value of each block and is embedded as watermark. The watermark is encrypted before the embedding process to make it more secure. The whole image can be verified by comparing the retrieved average pixel value from the watermark with the current average pixel value of the image. The tampered block will be recovered using the average pixel value retrieved from the watermark. The advantage of this scheme is that it can be modified to allow a ROI to be defined rather than the whole image for the watermarking process.

In [10], author proposed a scheme that consists of two types of watermark. The first watermark which is patient data and hash value of ROI is embedded into ROI itself in spatial domain and the second watermark is embedded into RONI part in transform domain by dividing the image into 16x16 pixels block. An embedding map of the ROI will be produced to form a second watermark together with compressed recovery information of ROI and average value of each block in the ROI. Tamper localization is done by comparing the average value of each block in the ROI with the retrieved average value from the watermark. It was claimed that this scheme is robust against salt and pepper attack and cropping.

Earlier research in [11] had also produced tamper localization and recovery watermarking by using block based method where each blocks consists of 8 x 8 pixels. Each block will then be divided into sub-blocks of 4X4 pixels. A three-tuple watermark embedded consists of two bits authentication watermark and seven bits recovery watermark for other sub-block. Average intensity of a sub-block will be embedded as the seven bits recovery watermark in another block which was predetermined in a mapping sequence. A parity bit is generated based on the seven bits recovery watermark. Tamper localization is done by comparing the

average intensity and parity bit. Blocks that were mark invalid will be recovered using the embedded average intensity of the sub-block.

Fragility and reversibility for watermarking of medical images using chaotic key has already been done by Naseem et al. in [12] by randomly selecting some of the pixels using chaotic key for embedding chaotic watermark. The rest of the pixels were changed into residues and then checksum was computed for the whole image using cyclic redundancy check (CRC) which makes an overhead of 4 bits hence, representing each pixel with 12 bits. This overhead is removed in the proposed scheme by the author by applying some trick on the residues and by choosing different scheme for watermark embedding.

4. RESIDUE NUMBER SYSTEM

A residue number system (RNS) represents a large integer using a set of smaller integers, so that computation may be performed more efficiently and it relies on the Chinese remainder theorem of modular arithmetic for its operation. It is defined by the set of k integer constants $(m_1, m_2, ..., m_k)$ referred at as moduli. Maximum representational efficiency it is imperative that all the moduli are coprime; that is, no modulus may have a common factor with any other. The integer X can be represented by the set of unique $k-tuple$ residues $(x_1, x_2, ...x_k)$.

$$\text{where} \qquad x_i = X \bmod m_i \qquad (1)$$

The dynamic range of RNS is 0 to $M-1$

$$\text{where} \qquad M = \prod_{i=1}^{k} m_i \qquad (2)$$

Any positive integer X in the range $0 \le X < M$ can be represented by the unique $k-tuple$ residue sequence as

$$X \xleftarrow[RT]{FT} (x_1, x_2, x_3, ...x_k)$$

For converting integer X to residues, forward transform (FT) is used and from residues to get back integer X reverse transform (RT) is used and it uses Chinese remainder theorem (CRT) as reverse transform to get integer X back as.

$$X = [\sum_{i=1}^{k} M_i \mid x_i L_i \mid_{m_i}] \bmod M \qquad (3)$$

where M is defined in (2) and

$$M_i = \frac{M}{m_i} \quad \text{and}$$

$$\left| L_i M_i \right|_{m_i} = 1$$

where L_i is the multiplicative inverse of M_i w.r.t m_i.

5. CHAOS IN WATERMARKING

Chaotic systems are well-suited to model real world systems because of their sensitive to initial conditions. All these characteristics make chaos a good candidate for security. Chaotic behavior is too difficult to predict by analytical methods without the knowledge of exact secret key. Even if the initial conditions that the opponent tries are very close to the ones used to encrypt the data, the opponent will still get gibberish as output.

Logistic map is general form of chaotic map. It is a non-linear polynomial of second degree and can be expressed by using the following equations,

$$X_{n+1} = rX_n(1 - X_n) \qquad (4)$$

where $x_0 \in (0,1)$ and r is a bifurcation parameter and for chaotic behavior $3.57 < r \le 4$. There are also other chaotic maps in the literature as well.

In our scheme, we use logistic map to encrypt the embedded position of a watermark.

6. PROPOSED WATERMARKING SCHEME

The watermarking scheme consists of two stages: watermark embedding and watermark and original image extracting.

6.1. Watermark embedding

1. Extract the possible ROI from original image by bounding the smallest rectangle around the desired area, since only the ROI part of the image is residued as explained in step 2.
2. The value 255 is factorized to 17 and 15 which become the corresponding moduli (m_1, m_2) of the RNS to be used for this image. Since, the dynamic range of RNS is 0 to 254 so every pixel with 255 intensity is treated separately as explained

below. Pre-processing of the residued pixels is a key to get pixels back. For every pixel of ROI we get residue pairs (x_1, x_2) where $x_i = X \bmod m_i$ such that $x_1 \le 16$ and $x_2 \le 14$. With the exception of the case when $x_1 = 16$, we observe that x_1 and x_2 can be represented by 4 bits each thus making the pair (x_1, x_2) representation by 8. Our main problem is with those pairs in which first residue is 16 as it has to be represented by five bits. We shall apply some trick so that it becomes 4 bits each for both residues. The pairs having first residue as 16 are mapped to corresponding unique pairs which do not otherwise occur in this RNS scheme. The mapping scheme is given below.

$$(16,0) \rightarrow (0,15)$$
$$(16,1) \rightarrow (1,15)$$
$$(16,2) \rightarrow (2,15)$$
$$(16,3) \rightarrow (3,15)$$
$$(16,4) \rightarrow (4,15)$$
$$(16,5) \rightarrow (5,15)$$
$$(16,6) \rightarrow (6,15)$$
$$(16,7) \rightarrow (7,15)$$
$$(16,8) \rightarrow (8,15)$$
$$(16,9) \rightarrow (9,15)$$
$$(16,10) \rightarrow (10,15)$$
$$(16,11) \rightarrow (11,15)$$
$$(16,12) \rightarrow (12,15)$$
$$(16,13) \rightarrow (13,15)$$
$$(16,14) \rightarrow (14,15)$$

All of the above pairs which were to be represented by 9 bits each, are mapped to the unique pairs which can be represented by 8 bits each as seen above. Since 15 cannot occur in the normal pairs as a second residue so it acts as an indicator that these pairs are exceptional pairs. Forward process and Inverse process for these exceptional pairs are given below.

Forward process at transmitter end: $(16,12) \rightarrow (12,16) \xrightarrow{16-1} (12,15)$

Inverse process at receiver end: $(12,15) \rightarrow (15,12) \xrightarrow{15+1} (16,12)$

Pixel 255 has residue (0, 0). We need to differentiate it from pixel 0 which also has residue (0, 0). We send 255 pixel as pair (15, 15) which can be represented by 8 bits. This unique pair cannot occur normally in this residual scheme with moduli 17 and 15.

3. Generate chaotic sequences using Eq. (4), multiply by 8 and take its *ceil(.)* so that the real chaotic sequences map into integers and change them into sum sequences as,

$$S_1 = \{X_1, X_1 + X_2, X_1 + X_2 + X_3, ...\} \qquad (5)$$
$$= \{Y_1, Y_2, Y_3, ..., Y_{256}\}$$
$$\text{where } Y_i = X_1 + X_2 + ...X_i$$

This sequence of 256 which is an outcome of chaotic key will give 256 locations for embedding the 256 bits of hash in RONI.

4. Arrange all the pixels of RONI in vector form and using the chaotic sequence obtained in step 3, make the LSB's of those corresponding pixels of RONI to zero.
5. Rearrange the RONI pixels obtained in step 4 with residued ROI obtained in step 2.
6. Compute the hash of the image obtained in step 5. This will give 256-bit one way hash value which will be the basis of watermark.
7. Again arrange the pixels of RONI in vector form as in step 4. Now we have 256 locations of RONI which are replaced by respective256 bits of hash.
8. Rearrange the RONI pixels in its original position to obtain the watermarked image. Now the watermark exists in RONI while ROI is residued.

6.2. Watermark and Orignal Image Extraction

Watermark and original image extracting steps are as under,

1. Separate RONI form ROI in the watermarked image.

2. Arrange all the pixels of RONI in some arbitrary vector. Now by knowing the chaotic key, watermarked pixels are indicated as,

$$S_1 = \{Y_1, Y_2, Y_3, ..., Y_{64}\}$$

This sequence of 64 which is an outcome of chaotic key will give 64 locations for extracting the 64 characters of hash from RONI.

3. Using the chaotic sequence obtained in step 2, extract the hash form the first 4 LSB's of RONI pixels and store it as hash_1 and place four bit value 0 at that location.
4. Rearrange this RONI with the residued ROI to form an image. Now compute the hash of this whole image and store it as hash_2.
5. Compare hash_1 with hash_2. If the hash is same then the image is authentic and go to step 6 and 7 else image is tampered.
6. In scanning residued ROI, the residue pairs having second residue as 15 go through inversion process as given in the step 2 of embedding. In this way all of the residue pairs are converted into 9 bits again. Then apply Chinese remainder theorem (CRT) to get back original pixels of ROI from residues.
7. Combine these ROI pixels with RONI pixels to get the original image.

6. SIMULATION RESULTS

To see the effectiveness of proposed system, experiments were conducted in MATLAB 7.0 with dual core processor with 2 GB RAM. The test image is ultrasound image of size 194*259. The proposed watermarking scheme discussed in this paper effectively embedded the watermark image into the original image and extracted it back from the watermarked image. Logistic map2 as in equation (4) with initial conditions x(0) = 0.25, r = 3.58 at embedding side and SHA-256 hash algorithm is used to calculate the hash of image. Fig.1. shows the original ultrasound image in which ROI is selected as a smallest rectangular region that bounds the ROI region and Fig.2. shows the hash of image. We have tested fragility of the proposed technique against various attacks. The experiment and results are explained as follows.

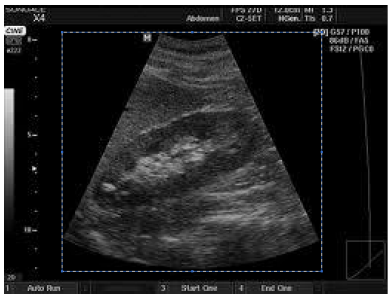

Figure 1: Original ultrasound image

a16c4d371f512de40f836428ea2541fe76b7ec06e5a82760628e4e363d83a795

Figure 2: Hash

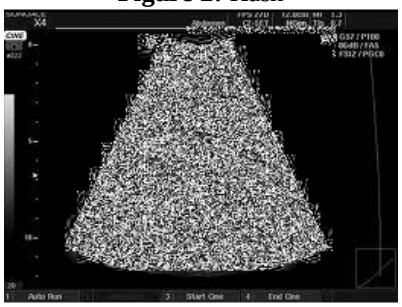

Figure 3: Watermarked image

Experiment 1: Fragility against Noise

The watermarked image is added with salt and pepper noise with noise density of 0.02. We conclude from this experiment that watermark is fragile against salt and pepper noise and exactly different image is obtained as seen in Fig.4 and in Fig.5.

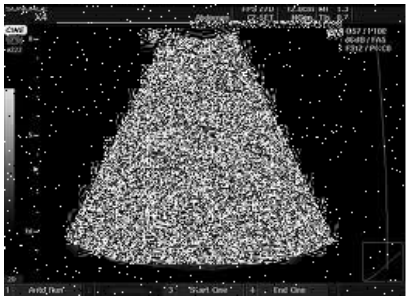

Figure 4: Watermarked image added with salt & pepper noise with variance of 0.02

1f5195742a12de40f8365ff25416e06b7ec0363483f 6e5a6c4d382768527d459

Figure 5: Recovered hash

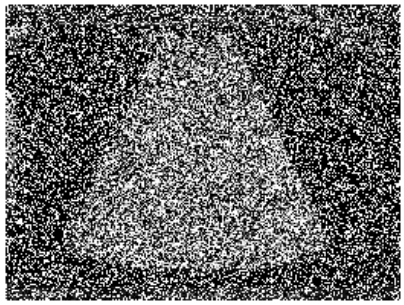

Figure 6: Recovered image from salt and pepper noise

Experiment 2: Fragility against compression

The watermarked image is compressed with a quality factor of 10. We conclude from this experiment that watermark is fragile against compression and exactly different image is obtained as seen in Fig.8 and in Fig.9.

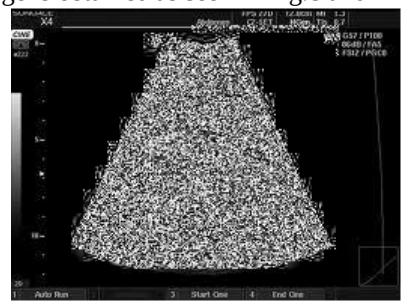

Figure 7: Watermarked image compressed with quality factor of 10

e6e363a1fe06b7ec16786a1990f36a2ad6c4d38276de5a7571f512de40f80628

Figure 8: Recovered hash

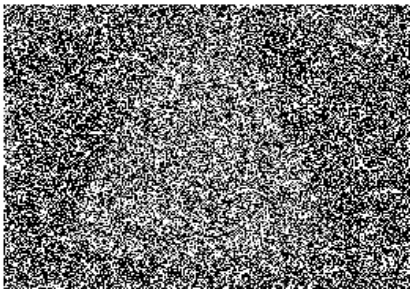

Figure 9: Recovered image after compression

Experiment 3: Fragility against rotation

The watermarked image is rotated counterclockwise with a degree of 2. We conclude from this experiment that watermark is fragile against rotation attack and exactly different image is obtained as shown in Fig.11 and in Fig.12.

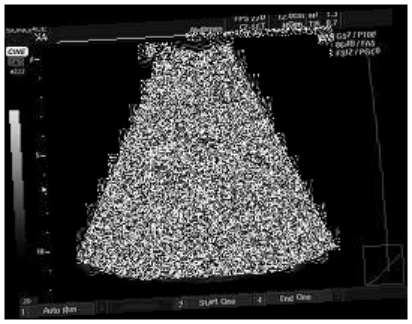

Figure 10: Watermarked image rotated with 3 degree counterclockwise

ce5ae869d89540f2db1fe7edff12de40f83642a16cedf89b7eca396ac28e43ba

Figure 11: Recovered hash

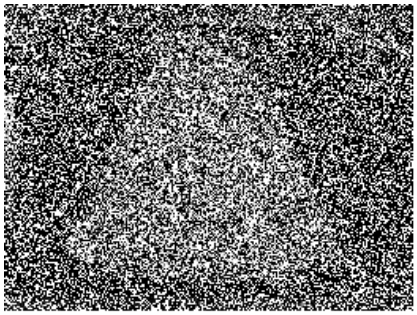

Figure 12: Recovered image after rotation attack

Experiment 4: Security Analysis

a16c4d371f512de40f836428ea2541fe76b7ec06e5a82760628e4e363d83a795

Figure 13: Recovered hash using initial conditions

x(0) = 0.25, r = 3.58 at receiver side same as embedding side

Figure 14: Recovered image using initial conditions

x(0) = 0.25, r = 3.58 at receiver side same as embedding side

f838ea642a16c4d382706e5a9254c83a7571f512de401fe76b7e 60628e4e363d

Figure 15: Recovered hash using initial conditions

x(0) = 0.25001, r = 3.58 at receiver side

Fig.13. shows the recovered hash with initial conditions x(0) = 0.25, r = 3.58 which is exactly same as in Fig.2. Similarly, Fig.14. shows the recovered image with initial conditions x(0) = 0.25, r = 3.58 which is exactly same as in Fig.1. Fig.15. and Fig.16. shows the recovered hash and recovered image respectively with initial conditions x(0) = 0.250001, r = 3.58 As we can see in Fig.15., that when initial conditions are slightly modified, exact hash is not recovered back hence, the image is tampered.

7. CONCLUSION

A novel reversible and fragile watermarking technique is proposed to embed hash based watermark in medical images on the basis of chaotic key and Residue number system. In traditional watermarking schemes, during watermark embedding, original host is not altered at all but in the proposed scheme the original host image is altered to provide maximum secrecy and even the watermark information is not sent on the transmission channel.

Our main contributions are:

- Residues are made and trick is applied to make them size eight.
- Image is altered after watermarking which also make our image secure such like encryption.
- Embedding locations are not sent separately but it is a part of image only (chaotic) key is required for extraction which enhances security.
- Modulli's of RNS which are 17 and 15 also enhances security being used as a key.

REFERENCES

1. Steele, H.L.: The prevention of non-consensual access to confidential healthcare information in cyberspace. Computer Law Review and Technology Journal, (1997)

2. Cao, F., Huang H.K., Zhou, X.Q. :Medical image security in a HIPAA mandated PACS environment, Computerized Med. Imaging and Graphics 27, pp.185-196, (2003)

3. Coatrieux G., Main H., Sankur B., Rolland, Y., Collorec, R.: Relevance of watermarking in medical imaging. In Proceedings of IEEE-EMBS Information Technology Applications in Biomedicine, Arlington, pp. 250-255, (2000)

4. Wakatani, A. Digital Watermarking for ROI Medical Images by Using Compressed Signature Image. In Proceedings of 35th Annual Hawaii International Conference on System Sciences (HICSS-35'02), Hawaii, pp. 2043-2048, (2002)

5. Coatrieux, G., Guillou, C. Le., Cauvin, J.-M., Roux, C.: Reversible watermarking for knowledge digest embedding and reliability control in medical images. IEEE Trans. Inform. Techno Biomed 13 (2), pp.158 – 165, (2009)

6. Wu, JHK., Chang, RF., Chen, CJ., Wang, CL., Kuo, TH., Moon, W K., Che , DR.: Tamper detection and recovery for medical images using near-lossless information hiding technique, J. of Digital Imaging 21(1), pp.59-76, (2008)

7. Liu, T., and Qiu, Zheng-ding.: The survey of digital watermarking-based image authentication techniques, Proceedings of the 6th International Conference on Signal Processing , pp. 1556- 1559, (2002)

8. Tan, C.K., Ng, C., Xu, X., Yong C.L. Poh L. G., Sheah K. Security protection of DICOM medical images using dual-layer reversible watermarking with tamper detection capability, J. of Digit. Imaging. Online First, (2010)

9. Chang, K. Chiang K., Chang, R., Yen, H. :Tamper detection and restoring system for medical images using wavelet-based reversible data embedding. J. of Digit. Imaging 21(1), pp.77-90, (2008)

10. Osamah, M., Khoo, B. E. : Authentication and data hiding using a hybrid ROI-based watermarking scheme for DICOM images, J. of Digit. Imaging. Online First, (2009)

11. Zain, J. M., Fauzi, Abdul R.M. Medical Image Watermarking with Tamper Detection and Recovery. In Proceedings of 28th Annual International Conference of the IEEE EMBS, pp. 3270-3273, (2006)

12. Naseem, M.T., Qureshi, I.M., Cheema, T.A., Zubair, M. :Invertible and Fragile Watermarking for Medical images Using Residue Number System and Chaos, Journal of Basic and Applied Scientific Research, Vol. 10, No 2, pp: 10643-10651,(2012)