J. Basic. Appl. Sci. Res., 2(10)10643-10651, 2012

© 2012, TextRoad Publication

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

Invertible and Fragile Watermarking for Medical Images Using Residue Number System and Chaos

**[1, 4, 5] Muhammad Tahir Naseem, [1, 2, 4] Ijaz Mansoor Qureshi, [1, 4] Tanvir Ahmed Cheema
[3] Muhammad Zubair**

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

ABSTRACT

—Reversible watermarking is a process in which the watermark is embedded in such a way that when the watermarked image passes through the authentication process, the original image is also recovered exactly along with watermark. Restoring the original image is important for the applications such as medical, military and law-enforcement etc. Reversible watermark being fragile using cyclic redundancy check (CRC) is embedded chaotically to some of the pixels and the rest of the pixels are changed into residues. By adding a chaotic watermark, the watermarked pixel becomes twelve bits and the residues also became twelve bits (after applying CRC) which makes the medical image secure by confusing the attacker about the location of watermark. The complexity of proposed system is very low to make it possible for real-time medical imaging. Furthermore, the proposed scheme is based on blind technique.

KEYWORDS: Cyclic Redundancy Check (CRC), Residue Number System(RNS) , Chinese Remaindet Theorem (CRT), Chaos.

INTRODUCTION

The advance multimedia and communication technology has provided new ways to store, access and distribute medical data in a digital format but these advances have also introduced new risks for inappropriate use of medical information circulating on open networks. It is well known that the integrity and confidentiality of medical images is a critical issue for ethical as well as for legal reasons. Encryption is an important tool that can be used to secure data transmitted over computer networks but it does not solve all the rightful data protection problems. At the receiver's side, decrypted information may be subject to unauthorized use or manipulation. Watermarking is an emerging technology for image authentication and copyright protection. The Copyright protection is achieved by robust watermarking while image authentication is usually achieved by fragile schemes. A fragile watermarking scheme detects any tampering in an image to guarantee the content integrity while a robust scheme prevents the watermark removal unless the quality of the image is greatly reduced. In general, fragile watermarking schemes modify the LSB planes of the original image in an irreversible way. This is not acceptable in medical images where the least significant bit modification leads to an erroneous detection. Invertible watermarking is an emerging technology which enables the exact recovery of the original image upon extraction of the embedded information.

In this paper, spatial domain reversible watermarking is proposed for medical images to achieve secrecy of patient history. It is very sensitive to any tampering in image and unauthorized attempt to recover original image. The algorithm selects some of the pixels using chaotic key from the image for embedding a chaotic watermark. The rest of the pixels are changed to residues which are recovered uniquely by Chinese remainder theorem (CRT) [1]. The chaotically selected pixels are divided by the generator polynomial and the remainder is drawn. The drawn remainder is X-ORed with watermark and appended with message. The decoder receives the appended message and divides it by the same generator polynomial and draws the remainder. The authenticity of watermark is done on the basis of remainder that is valid if it is zero and is invalid otherwise. Residues are passed through the process of CRC. The secrecy of proposed system is high. The watermarked pixel consists of 12 bits and residue also consists of 12 bits. It will be almost impossible for the intruder to find out which pixels are watermarked and which are residued only. Moreover, the proposed system also ensures high security due to four keys in chaotic maps. The original image is also not needed in extraction process which makes it blind watermarking.

The rest of the paper is organized as follows: Section 2 first gives the review about digital watermarking schemes and then about reversible watermarking schemes. In section 3, the desired functionalities of watermarking techniques are discussed in terms of medical images and the new "invertible" watermarking paradigm is presented. In section 4 we briefed about chaos. Section 5 describes the cyclic redundancy check and residue numbers system is described in section 6. In section 7 and 8, we gave

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

our proposed scheme. In section 9 some experiments are shown demonstrating the fragility of the proposed scheme and then we give finally our conclusion in section 10.

I. DIGITAL WATERMARKING

In digital watermarking, data is inserted into digital data on the basis of key which can be later extracted in order to authenticate the image [2]. Watermark embedding can be performed in spatial domain as well as in frequency domain. In spatial domain watermark information is embedded by directly modifying the pixels of image. In frequency domain watermark information is embedded in the transform domain. Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), Wavelet Transform or Radon Transform is generally used as a transform domain. Embedding in transform domain is considered more robust than the spatial domain as it provides more resistance [3]. Image watermarking techniques can be blind and non-blind. In blind watermarking scheme, original image is not desired at receiver while in non-blind watermarking schemes, original image is desired at receiver end and our proposed scheme also lies in the first category.

A watermarking scheme can also be classified as either robust or fragile: The robust watermarking schemes are generally used for copyright protection and ownership verification. For robust watermarking, watermark which contains the proof of ownership must survive all types of attacks so that the image remained exploitable. The fragile watermarking schemes are useful for authentication purposes. In fragile watermarking schemes, the watermark must be sensitive to all modification of the image; even slight modifications in the image can be caught. Fragile watermarking has very importance in law enforcement, defense and in medical images etc. When the fragile watermarked data is changed, the extraction of watermark can be used to detect and locate tampering.

Reversible watermarking is basically a digital watermarking scheme with an additional feature that once the watermark has been authenticated, the original image is also recovered exactly [4]. In watermarking scheme, the watermark is sensitive to intentional or un-intentional attacks and is a subject of many applications, like content authentication [5], finger printing [6] and source tracking [7].

Different techniques are developed by the researchers to solve the reversible watermarking issues. A low capacity reversible watermarking is discussed in [8] by using an invertible addition. The restriction is made on embedded side to be additive and non-adaptive. Another scheme is discussed in [7] in which the author compresses one of the least significant bit planes of the host image, appends the payload and image hash, encrypts the final result and then replaces the original bit plane with the encrypted result.

Celik *et al* [9] proposed a loss-less reversible watermarking scheme by quantizing and then compressing the coefficients and then appends payload to it. This scheme is capable of hiding 0.7 bits/pixel. A very high data-hiding capacity for color images is proposed in [10] which recover the original image exactly. The algorithm hides several bits in the difference expansion (DE) of vectors of adjacent pixels. Kalker *et al* [11] proposed capacity bounds for reversible watermarking and also proposed error correction codes to make reversible watermarking robust to ordinary processing.

Ni et al. [12] utilizes zero or minimum point of histogram. If the peak is lower than the zero or minimum point in the histogram, it increases pixel values by one from higher than the peak to lower than the zero or minimum point in the histogram. While embedding, the whole image is searched. Once a peak-pixel value is encountered, if the bit to be embedded is '1' the pixel is added by 1, else it is kept intact. Alternatively, if the peak is higher than the zero or minimum point in the histogram, the algorithm decreases pixel values by one from lower than the peak to higher than the zero or minimum point in the histogram, and to embed bit '1' the encountered peak-pixel value is subtracted by 1. The decoding process is quiet simple and opposite of the embedding process.

II. REQUIREMENTS FOR MEDICAL IMAGES

In medical images, confidentiality and protection is a key issue for proper diagnostic so it is very important to prevent unauthorized manipulation of such kind of images. Medical images should be kept intact in any circumstance and before any operation they must be checked for authentication and confidentiality. Different watermarking techniques have been proposed in the literature to address the problems of medical image confidentiality [13]. Classical watermarking schemes impose some distortions to the original data due to quantization, bit-replacement, truncation etc. For most applications some distortion in the image might be acceptable, but for medical applications, the images must be kept perfect without any loss of information, that is, the watermark after embedding should not change the image for exact diagnosis i.e., the typical shape of a ECG signal is well known to cardiologists so any slight change from that shape is usually considered as a symptom of illness [14]. If the watermark distorts the image and makes the watermarked image unseen to the naked eye also promises for security and this thing is strongly needed in this new era [15]. Image authentication has been addressed in [16] [17] involving the insertion of a watermark into the host image in a lossless manner, which enables the exact recovery of the original image after extracting the embedded watermark. Cryptographic tools as in [18] with reversible watermarking scheme also provide exact authentication and at the same time recovery of exact original image. In the verification step, removing the hash and the patient information recovers the original image. There are several advantages of encryption tools in medical images but the main disadvantage of the encryption tools is that the execution time is very low which discomforts such kind of schemes for medical use [19].

III. CHAOS

Chaotic systems are well-suited to model real world systems because of sensitive to initial conditions/system parameters, their randomness property and non-periodicity. 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,

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

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

In our scheme, we use logistic map twice with different initial conditions to encrypt the embedded position of a watermark.

IV. CYLIC REDUNDANCY CHECK

The cyclic redundancy check (CRC) is based upon treating bit strings as representation of polynomials with coefficients of 0 and 1 only. A $k-bit$ string is regarded as the coefficient list for a polynomial with k terms, ranging from X^0 to X^{K-1}.Such a polynomial is said to be of degree $k-1$. The higher-order bit is the coefficient of X^{k-1}; the next bit is the coefficient of X^{k-2}, and so on. For example, a bit string 110001 has six bits and thus represents a six-term polynomial $X^5 + X^4 + 1$ with coefficients 1, 1, 0,0,0,1.

The polynomial arithmetic is performed in modulo 2, according to rules of algebraic field theory. When CRC method is employed, the encoder/sender and decoder/receiver just agree upon a generator polynomial $G(X)$, in advance. Both the highest- and lowest-order bits of generator polynomial must be 1. To compute the checksum for some message with m bits, corresponding to the polynomial $M(X)$, the message must be larger than the generator polynomial. The idea is to append the checksum to the end of message in such a way that the polynomial represented by the message with the checksum is divisible by $G(X)$. When the decoder gets the message with CRC checksum, it divides it by $G(X)$. If there is a non-zero remainder, it is an indication of error.

V. RESIDUE NUMBER SYETEM

The residue number system (RNS) is defined by the set of numbers $(m_1, m_2, ..., m_k)$ called moduli which are relatively prime such that $\gcd(m_i, m_j) = 1 \quad \forall i, j = 1,2,...,n$. The integer X can be represented by the set of unique $k-tuple$ residues $(x_1, x_2, ...x_k)$.

$$\text{where} \qquad x_i = X \bmod m_i \qquad (2)$$

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

$$\text{where} \qquad M = \prod_{i=1}^{k} m_i \qquad (3)$$

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

$$X \overset{FT}{\underset{RT}{\rightleftarrows}} (x_1, x_2, ..., x_k)$$

The conversion of integer X to residues is called forward transform (FT) and from residues to integer X is called reverse transform (RT) and it relies on Chinese remainder theorem (CRT) to calculate integer X back as.

$$X = [\sum_{i=1}^{k} M_i \mid x_i L_i \mid_{m_i}] \bmod M \qquad (4)$$

where M is defined in (3) and

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

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

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

VI. PROPOSED WATERMARK EMBEDDING SCHEME

The proposed watermarking scheme consists of following steps.

A. To generate Chaos-based sequence to determine the location of pixels to be watermarked.
B. Watermark embedding in these pixels.
C. Finding residues of the rest of the pixels and appending CRC bits.

The detail of these steps is as under.

A. To generate Chaos-based sequence to determine the location of pixels to be watermarked.

1. Generate two different binary chaotic sequences from same Logistic map given in (1) but with different initial conditions.

2. Multiply the sequences by 8 and take it's *ceil(.)* so that the real chaotic sequences map into chaotic integers with each integer range from 1 to 8 as,

$$X_{n+1} = ceil(X'_{n+1}) \qquad (5)$$

For the sake of simplicity, the chaotic integers from two logistic maps are,

$$I_1 = X_1, X_2, X_3, ... \qquad (6)$$

$$I_2 = Y_1, Y_2, Y_3, ... \qquad (7)$$

3. Add chaotic integers and change them into sum sequences,

$$S_1 = X_1, X_1 + X_2, X_1 + X_2 + X_3, ... \qquad (8)$$

$$S_2 = Y_1, Y_1 + Y_2, Y_1 + Y_2 + Y_3, ... \qquad (9)$$

4. The chaotic pairs are made for watermark embedding as,

$[(X_1, Y_1), (X_1, Y_1 + Y_2), (X_1, Y_1 + Y_2 + Y_3)...........]$ pairs are embedded with X_1 as a watermark.

$[(X_1 + X_2, Y_1), (X_1 + X_2, Y_1 + Y_2), (X_1 + X_2, Y_1 + Y_2 + Y_3)...........]$ pairs are embedded with X_2 as a watermark. Similarly, for other pairs until all the X_i's are embedded.

B. Watermark Embedding in these pixels

When the pixels to be watermarked are chosen using the chaotic key, the watermark embedding consists of following steps.

1. Choose the primitive polynomial $G(X)$ of degree 4 as

$$G(X) = X^4 + X^3 + 1$$

2. Make the polynomial of message $M(X)$ which is pixel value in our case. Multiply $M(X)$ by X^4 and divide it by $G(X)$ to generate the remainder $R(X)$ as,

$$\mathrm{Re}\,m\left(\frac{X^4 M(X)}{G(X)}\right) = R(X)$$

where $\deg ree(R(X)) < \deg ree(G(X))$

3. Since, the watermark for each pixel pair consists of 4 bits each and $R(X)$ also consists of 4 bits so, $R(X)$ is X-ORed with corresponding watermark (X) as,

$$C(X) = R(X) \oplus X$$

4. Append $C(X)$ with $M(X)$ as,

$$T(X) = [C(X), M(X)]$$

where $T(X)$ is the watermarked pixel.

C. Finding residues of the rest of the pixels and appending CRC bits

As we have seen, there is a set of pixels chosen in the image by a chaotic key in which the watermark is embedded. The complementary set of pixels undergoes the process of residue with CRC given below after pre-processing.

The value 255 is factorized to 15 and 17 which become the corresponding moduli (m_1, m_2) of image respectively. Since, the dynamic range of RNS is 0 to 254 so; every 255 intensity value is treated as 254. Pre-processing of the residued pixels is a key to get residued pixels back. Moreover, the residued pixels which are pre-processed are appended with some character so at decoder side we are able to know that which cut pixels were pre-processed.

As given in section 5 and section 6A, our dynamic range is 0 to 254 and $m_1 = 15, m_2 = 17$. We get for any pixel residues (x_1, x_2) where $x_i = X \bmod m_i$. Since $x_1 \le 14$ and $x_2 \le 16$, x_1 can be represented by four bits and x_2 by five bits which makes a total nine bits. Let us treat these nine bits as Residue polynomial $\mathrm{Re}\,s(X)$. Its highest degree can be eight.

1. For each residue, make its polynomial $\mathrm{Re}\,s(X)$ and choose primitive polynomial $H(X)$ as,

$$H(X) = X^3 + X^2 + 1$$

2. Multiply $\mathrm{Re}\,s(X)$ by X^3 and divide it by $H(X)$ to get remainder $\mathrm{Re}\,m(X)$ as,

$$\mathrm{Re}\,m\left(\frac{X^3\,\mathrm{Re}\,s(X)}{H(X)}\right) = \mathrm{Re}\,m(X)$$

3. Append $\mathrm{Re}\,m(X)$ with $\mathrm{Re}\,s(X)$ as,

$$\mathrm{R}(X) = X^3\,\mathrm{Re}\,s(X) + \mathrm{Re}\,m(X)$$

$\mathrm{R}(X)$ is at most 11 degree polynomial and represent 12 bits.

VII. PROPOSED WATERMARK EXTRACTION SCHEME

Watermark and original image extraction consists of following steps.

A. Indicate the watermarked pixels using the chaotic key.
B. Watermark extraction and comparing.
C. Residues and CRC.

Their detailed explanation is as under.

A. Indicating the watermarked pixels using the chaotic key.

Having known the chaotic key which is same as on encoding side, the watermarked pixels are indicated as,

$$[(X_1, Y_1), (X_1, Y_1 + Y_2), (X_1, Y_1 + Y_2 + Y_3)\ldots\ldots\ldots\ldots]$$
$$[(X_1 + X_2, Y_1), (X_1 + X_2, Y_1 + Y_2), (X_1 + X_2, Y_1 + Y_2 + Y_3)\ldots\ldots\ldots\ldots]$$

Other chaotic pairs are also generated as in embedding side.

B. Watermark extraction and comparing

1. Extract $C(X)$ from $T(X)$ and the remaining part is $M(X)$ which are the original pixels.

2. $M(X)$ is multiplied with X^4 and is divided by the known primitive polynomial $G(X)$ used in encoding side as,

$$\mathrm{Re}\,m\left(\frac{X^4 M(X)}{G(X)}\right) = R(X)$$

3. $R(X)$ is X-ORed with $C(X)$ to get watermark as,

$$W = C(X) \oplus R(X)$$

If W is the same watermark, then no pixel in $M(X)$ has been corrupted.

C. Residues and CRC

The residued pixels are extracted from the watermarked image by ignoring the pixels which are watermarked. Each residue is divided by the known primitive polynomial $H(X)$ and the remainder is drawn as,

$$\mathrm{Re}\,m\left(\frac{R(X)}{H(X)}\right)$$
$$= \mathrm{Re}\,m\left(\frac{X^3\,\mathrm{Re}\,s(X) + \mathrm{Re}\,m(X)}{H(X)}\right) = 0$$

If the remainder is zero, it is an indicator that no bit is corrupted and (4) is used to recover back the original coefficients of an image then the character embedded coefficients are searched and are made 255 which is now the coefficients of original image. On the other hand if the remainder is not zero, it means that image is tampered.

VIII. 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 MRI image of size 348*314. 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. Both the maps are Logistic map2 with initial conditions x(0) = 0.25, r = 3.58 and x(0) = 0.56, r = 3.57 respectively at embedding side and chaotic watermark pattern of size 55×55 is used. Fig.1 shows the original MRI image. Fig.2 shows the watermarked MRI image. The total time for watermark embedding and extracting was 46 sec which is quite less.

We have tested fragility of the proposed technique against various attacks. The experiment and results are explained as follows.

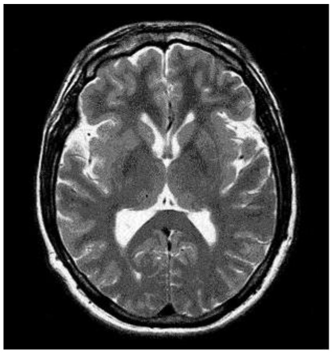

Figure 1: Original MRI image

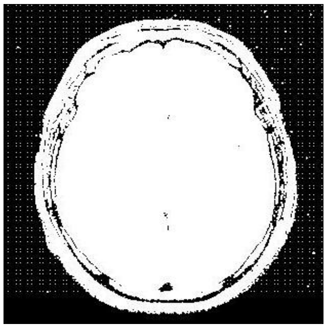

Figure 2: Watermarked MRI image

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.

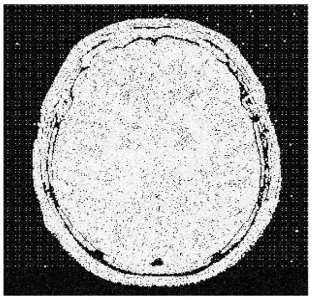

Figure 3: Watermarked image added with salt and pepper noise with variance 0.02

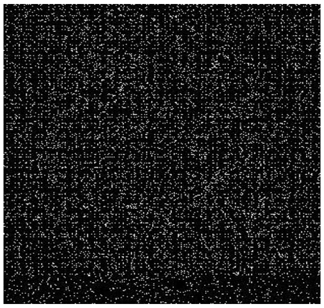

Figure 4: Recovered image from salt and pepper noise

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.

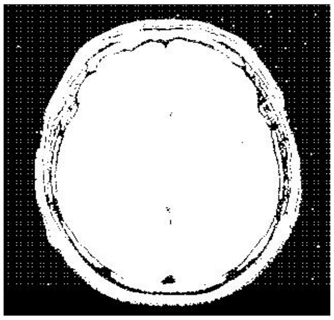

Figure 5: Compressed with a quality factor = 10

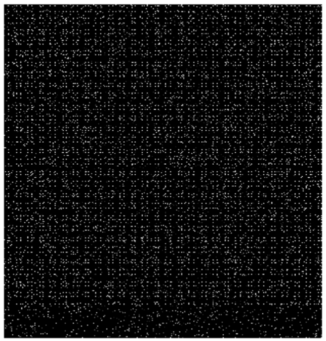

Figure 6: Recovered image after compression

Experiment 3: Security Analysis

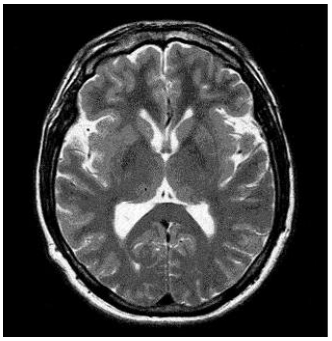

Figure 7: Recovered image with x(0) = 0.25, r = 3.58 and
x(0) = 0.56, r = 3.57.

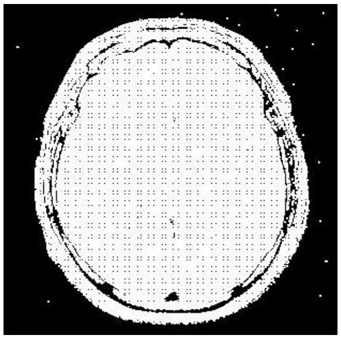

Figure 8: Recovered image with x(0) = 0.25000001, r = 3.58 and x(0) = 0.56, r = 3.57.

Fig.7. shows the recovered image with initial conditions x(0) = 0.25, r = 3.58 and x(0) = 0.56, r = 3.57 which are exactly same in embedding side. Fig.8. shows the recovered image with slightly modified initial conditions with x(0) = 0.25000001, r = 3.58 and x(0) = 0.56, r = 3.57. Fig.7. shows the original image exactly because initial conditions are exactly same as in embedding side. As we can see in Fig.8, when initial conditions are slightly modified, the original MRI image is not recovered back which demonstrates the high secrecy of our proposed system.

Experiment 4: Fragility against rotation
The watermarked image is rotated counterclockwise with a degree of 3. We conclude from this experiment that watermark is fragile against rotation attack and exactly different image is obtained.

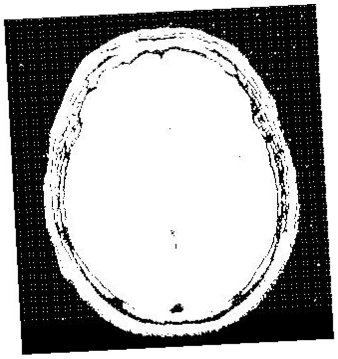

Figure 9: Watermarked image rotated with 3 degree counterclockwise.

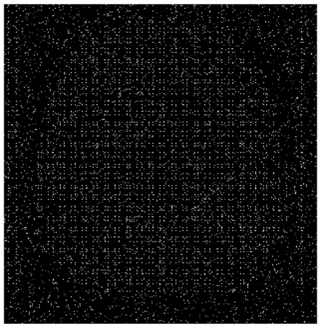

Figure 10: Recovered image after rotation of 3 degree.

IX. CONCLUSION

In this paper, reversible watermarking technique is proposed to embed chaotic watermark into digital images in such a way that when the watermarked image passes through the authentication process, the exact image is recovered back. Unlike traditional watermarking techniques, during watermark embedding, original host is not altered at all. As we have seen, the original host image is watermarked chaotically to provide maximum secrecy and even the watermark information is not sent on the transmission channel. The only thing we need for exact recovery is the knowledge of exact initial conditions as we have seen in our simulation results that a slightly modification in initial conditions does not recovers original image which demonstrates the high security of our proposed system. MRI image is simulated under different attacks and the time needed to embed and extract the watermark and original was 46 sec which is quite less.

The experimental results provide an indication of the potential of the approach and there are several advantages that make it suitable for practical use:

Watermarked locations are not sent separately but it is a part of image only (chaotic) key is required for extraction which enhances security. Corresponding modulli's of RNS which are 15 and 17 also enhances security being used as a key. Patient information is hidden and image is altered which also make our image secure such like encryption. Fragility of watermark and image is achieved. Exact Image can be recovered for a reliable diagnosis. Complexity of proposed model is very low.

REFERENCES

[1] K. W. Watson, “Self-checking computations using residue arithmetic, ” Proc. IEEE, vol. 54, pp. 1920–1931, Dec. 1966.

[2] F. Hartung and M. Kutter, “Multimedia watermarking techniques,” Proceedings of the IEEE, vol. 87, no. 7, pp. 1079–1107, July 1999.

[3] Juan RHMA, Perez-Gonzalez F: DCT-Domain Watermarking Techniques for still images: Detector Performance Analysis and a New Structure. IEEE Transactions on Image Processing 2000, 9:55-68.

[4] J. Tian , “Reversible data embedding using difference expansion”, IEEE Trans. On Circuits and Systems for Video Technology, 13(8): pp. 890-896, August 2003.

[5] J. Cox, L. Miller and A. Blossom, “Digital watermarking(ist edition)”, USA: Morgan Kaufmann Publishers, 2002.

[6] M. Fridrich and A. Baldoza, “New Fragile Authentication watermark for Images”, in Proc of IEEE Integrated conference om Image Processing, pp. 10-13, Sep 2000.

[7] J. Fridrich, M. Golijan and R. Du, “Invertible Authentication”, in Proc of SPIE Photonics West Security and Watermarking of Multimedia Contents, vol. 3971, san Jose, CA, pp. 197-208, Jan 2001.

[8] C.W. Hansiger. P.W. James, M. rabbani and J.C. Stoffel, “Lossless Recovery of an Orignal Image containing Embedded Data”, U.S Patent 6, 278, 791, 2001.

[9] M. Celik, G. Sharma, “reversible Data Hiding”, in Proc IEEE Int. Conf Image Processing, vol 2, pp. 137-160, sep. 2002.

[10] Alattar, “Reversible Watermark using the Difference Expansion of a Generalized Integer Transform”, IEEE Transaction On Image Processing, vol. 13, No. 8, August 2004.

[11] T. Kalker and F.M. Willems, “Capacity bounds and Code construction for reversible data-hiding”, in Proc. Of Electronic Imaging 2003, Security and Watermarking of Multimedia contents, santa Clera, california, Jan 2003.

[12] Z. Ni, Y.Q. Shi, N. Ansari, and W. Su, “Reversible Data Hiding, In Proc. of International Symposium on Circuits and Systems, Bangkok, Thailand, Vol. 2, pp. 912-915, 25-28 May 2003.

[13] G. Coatrieux, H. Maitre, B. Sankur, Y. Rolland, R. Collorec, “Relevance of Watermarking in Medical Imaging”, in Proceedings of the IEEE EMBS Conf. on Information Technology Applications in Biomedicine, Arlington, USA, p. 250-255, Nov. 2000.

[14] J. Fridrich et al, Lossless Data Embedding for All Image Formats, Proc. SPIE Photonics West, Security and Watermarking of Multimedia Contents, pp. 572–583, 2002.

[15] W. Puech and J.M. Rodrigues, ‘’A NEW CRYPTO- WATERMARKING METHOD FOR MEDICAL IMAGES SAFE TRANSFER’’, in Image Prorcessing Theory, Tools and Applications,pp. 1-2, 2008.

[16] P. Campisi, D. Kundur, D. Hatzinakos and A.Neri, “Compressive Data Hiding: An Unconventional Approach for Improved Colour Image Coding,”EURASIP Journal on Applied Signal Processing, special issue on Emerging Applications of Multimedia Data Hiding, vol. no. 2, pp. 152-163, February 2002.

[17] J. Fridrich, M. Golijan and R. Du, “Lossless data embedding – new paradigm in digital watermarking”, EURASIP Journal on applied Signal Processing, vol 2, No. 2, pp. 185-196, Feb 2002.

[18] J. Menezes, P. C. Van Oorschot, S. A. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1997.

[19] M. Yang, L. Song, M. Trifas, D. Buenos_Aires, L. Chen and J. Elston, “Secure Patient Information and Privacy in Medical Imaging”, Journal of Systemics, Cybernetics and Informatics, vol. 8, No. 3, pp. 63-66, 2010.