Spread Spectrum based Invertible Watermarking for Medical Images using RNS and Chaos

Muhammad Naseem[1], Ijaz Qureshi[2], Muhammad Muzaffar [1], and Atta ur Rahman[3]
[1]School of Engineering and Applied Sciences, ISRA University, Pakistan
[2]Department of Electrical Engineering, Air University, Pakistan
[3]Barani Institute of Information Technology, University Rawalpindi, Pakistan

Abstract: *In the current paper, we have presented a novel watermarking scheme with making watermark as robust while keeping the image fragile using Residue Number System (RNS) and Chaos. Residues of the image are made to keep it secure since, their sensitive to change is high. Only Region Of Interest (ROI) part of the image is residued. In making residues of ROI, some residues exceed bit size eight so, these residues are converted to eight bits by applying some trick. Two watermarks are embedded in two stages; one to achieve robustness using Spread Spectrum (SS) technique and other to achieve fragility of image by calculating the digest of image. In the first stage, spreaded watermark is embedded in Region Of Non-Interest (RONI) pixels using the chaotic key and in the second stage, hash calculated from the first stage is again embedded in RONI pixels based on the chaotic key. Moreover, the original image is not needed at receiver end, which makes the proposed scheme blind.*

Keywords: *RNS, chinese remainder theorem, ROI, SS, RON, chaos.*

Received October 5, 2013; accepted April 24, 2014; *published online April 1, 2015*

1. Introduction

Nowadays, the new developments in the digital technology have resulted in explosion in the use of digital media products such as image, audio and video. However, this raises security concerns due to digital multimedia products and high vulnerability to the illegal copying, distribution, manipulation and other attacks. Thus, the watermark must be secure and easy to recover from the particular document [19]. Two types of watermarks can be embedded in the data, one is visible and the other is invisible. In visible watermarking, the content changes completely and the watermarked content differs from the original one, but in invisible watermarking, the content is not changed to a large extent and only the minor variations exist in the watermarked content which is not even perceivable by the naked eye. Watermarking can be classified into three categories, namely, robust, fragile and semi-fragile [22]. In robust watermarking, the watermark is embedded into the content and by removing it, the quality of original content is badly damaged. Robust watermarks are mostly used for copyright protection. Fragile watermarks are very sensitive and are destroyed when a person tries to tamper the document. These are mostly used in content authentication. The semi-fragile watermarks are such watermarks which are robust to incidental attacks but are fragile to malicious attacks. By the use of semi-fragile watermarks, the nature of attacks on the content can be judged.

The watermarking can be done in two domains spatial and transform domain. In spatial domain, watermark is embedded by directly modifying the pixel values, while in transform domain, the watermark is embedded by modifying the coefficients of transform domain by taking Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) or some other transform. However, transform domain embedding techniques are more robust than spatial domain techniques, but are more complex. Now, we shall first present some short review about the watermarking of medical images and then on their reversible watermarking.

In hiding Electronic Patient Record (EPR), three mandatory security measures namely, confidentiality, availability and reliability should be met [4]. Keeping in mind these security measures, each method is categorized as fragile, robust or semi-fragile. A novel robust and fragile medical image watermarking scheme is presented in [7] in which the multiple watermarks are embedded by taking the wavelet transform of the image. The robust watermark is used for copyright protection and the fragile watermark is used for image authentication. The watermarking scheme can be made more secure by employing steganographic methods in which the researcher embeds the watermark into two phases, forward phase and reverse phase by taking DCT of the original image. In the forward phase, the watermark is inserted into the background parts of the image since the background portion of the mammogram does not contain any information about the patient [12]. Moreover, the scheme is blind as there is no need of original image to get watermark at receiver end.

Zhou *et al*. [27] presented a watermarking scheme for verifying authenticity and integrity of digital mammographic images. The author used digital envelop as a watermark and the Least Significant Bits (LSB) of one random pixel of the mammographic is replaced by one bit of the digital envelope bit stream. Instead of the whole image data, the MSB of each pixel is used for verifying integrity. Other researchers adapt digital watermarking for interleaving patient information with medical images to reduce storage and transmission overheads [1]. Again the LSB's of the image pixels are replaced for embedding. Chao *et al*. [3], proposed DCT based data-hiding technique that is capable of hiding EPR related data into marked image. The information is embedded in the quantized DC coefficients. Another scheme is also presented by the author which separates the Region Of Interest (ROI) and Region Of Non-Interest (RONI) and embeds the watermark in RONI part after taking the Discrete Wavelet Transform (DWT) since RONI part of image does not make contribution in diagnosis [8]. In [11] secure Spread Spectrum (SS) watermarking scheme is presented for medical images by embedding the watermark in transform domain. In this scheme, author spreads the watermark and then embeds the watermark by taking DWT of the original image based on secret key. The drawback of the above watermarking schemes is that the original image is distorted in non-invertible manner after watermarking. Therefore, it is impossible to recover original image from the watermarked content.

The reversible watermarking scheme involves inserting a watermark into an invertible manner in such a way that when watermark is extracted from the watermarked image, the original image pixels are also, recovered exactly [2, 5, 6, 24]. Trichili *et al*. [25] presented a watermarking scheme by using an image virtual border as a watermarking area. Patient data is then embedded in the LSB's of borders. Another author presented a scheme in which the digital signature of the whole image together with patient data is embedded. Chao *et al.* [3], extend their work on the digital envelop and embed their DE by making a random walk sequence and replace LSB of selected pixel with the watermark.

The most important requirement in the medical image watermarking should be that after watermarking, the image should not be visible to the naked eye, in order to enhance security. Keeping this requirement in mind, fragility and reversibility for watermarking of medical images using chaotic key has already been done by Naseem *et al.* [16] 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 4bits hence, representing each pixel with 12bits. This overhead was also removed by the author by applying some trick on the residues and by choosing different scheme for watermark embedding [15].

The data hiding capacity for colored and grayscale natural images has also been enhanced in [18] by using the histogram modification technique. The scheme embeds the more capacity by taking the difference of adjacent pixels. Histogram technique is applied to prevent the watermarking system form overflow and underflow. The capacity is increased three times for colored images as compared to the grayscale images. Secure and medical image authentication watermarking scheme is also presented by using Particle Swam Optimization (PSO) technique [21]. The author used PSO in adaptive quantization index modulation scheme conjunction with Singular Value Decomposition (SVD) in transform domain. The scheme shows good PSNR value as well as robustness. Another author presented some important properties of digital watermarking for different models of digital watermarking in order to make the data secure like encryption and decryption. [20]. Author also, described various codes of digital watermarking in order to implement in MATLAB.

Another fragile and efficient tamper detection scheme is also presented by using block-based method where the watermark is generated from the hash code of blocks at final level [26]. The generated watermark is also inserted at hash code of blocks at final level. The scheme has capability to detect tampered area without checking the entire watermarked image. Robust watermarking scheme is also, presented by the author by combing DWT in conjunction with Discrete Fractional Random Transform (DFTR) [10]. The scheme used 2D bar code for hiding information and used block coding method to generate the watermark. By using quantization technique, watermark information is embedded into DWT-DFTR in order to achieve better imperceptibility and robustness. Another watermarking scheme is also presented by the author by using Back propagation neural network algorithm [23]. The coefficients of neural network are modified with the binary watermark information. The weights of neural networks were adjusted while picking the binary bits of watermark information. The scheme has high robustness as well as imperceptibility as compared to other schemes.

Watermarking scheme for efficient detection of watermark information in DCT domain is also, presented in [9]. The scheme applies pre-filtering technique before running the algorithm for watermark extraction. Scheme detects the watermark information with more accuracy after applying some attacks. Video watermarking scheme by using Code Division Multiple Access (CDMA) technique is also, presented in [13] in DWT domain. The scheme embeds the watermark information into the middle frequency components. Four keys are also used to enhance the security of watermark information. Video is imperceptible after embedding watermark information. The scheme is robust to variety of attacks.

In this paper, we are presenting SS watermarking scheme based on Residue Number System (RNS) for medical images along with chaotic key to make watermark robust while keeping the image fragile. Residues of the image are made to make it secure so that the naked eye cannot perceive it. Only the ROI part of the image is residue. Moreover, when the ROI part of image is residue, 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. Two watermarks are used which are embedded in two stages; fragile watermark which is the basis for the authentication of image and the other is the robust watermark used for copyright protection which contains patient information. On the basis of chaotic key, chaotically spreaded watermark is embedded in RONI pixels in the first stage and then the hash is calculated from the stage 1 which is again embedded by replacing the corresponding bit of pixel chosen chaotically in stage 2. On the basis of same chaotic key, both the watermarks are extracted on the receiver side. Once the authenticity of image has been checked, patient information is retrieved as a robust watermark. Moreover, original image is not needed on the receiver side, which makes the proposed scheme blind.

Other sections of the paper are organized as follows: SS technique for watermarking is discussed in section 2. In section 3, RNS is described. Section 4 describes about chaotic systems and section 5 describes the brief introduction about Arnold transform. Section 6 describes the proposed watermarking scheme and some objective measures to check the robustness of watermark are discussed in section 7. Section 8 describes the experiment results finally section 9 concludes the paper.

2. Spread Spectrum Watermarking

In SS watermarking technique, the pseudo-random signal is added to the image that is below the threshold of perception and that cannot be identified and thus removed without knowledge of the parameters of the watermarking algorithm [14].

2.1. Scheme of Embedding

Suppose A is the information that we want to hide in the image as follows: $A=\{a_i | a_i \in \{-1, 1\}\}$.

Each bit a_i is spread by a large factor chip-rate to obtain the spread sequence as follows: $B=\{b_i | b=a_j; j.cr \leq i < (j+1.cr)\}$.

The spread bit b_i is modulated by a binary pseudo-noise sequence as: $C=\{c_i | c_i \in \{-1, 1\}\}$.

After performing modulation, the result is amplified with a scaling parameter α to perform SS watermark as follows: $w_i=a.b_i.c_i$.

The watermark w_i is added to the original image to make watermarked image as follows:

$$w'_i = v_i + w_i \tag{1}$$

Due to the noisy nature of c_i, w_i is also a noise-like signal and thus difficult to detect, locate, and manipulate.

2.2. Scheme of Extraction

Extraction of watermark information is accomplished by multiplying the watermarked image with c_i:

$$\sum_{i=j.cr}^{(j+1).cr-1} w'_i.c_i = \sum_{i=j.cr}^{(j+1).cr-1} v_i.c_i + \sum_{i=j.cr}^{(j+1).cr-1} \alpha.b_i.c_i^2 \tag{2}$$

Since, c_i is random, chip-rate is large and deviation of v_i is large so it can be expected that the first term in Equation 2 which is: $Lim \sum_{i=j.cr}^{(j+1).cr-1} v_i.c_i \approx 0$.

Since, $c_i^2=1$, so the Equation 2 yields the correlation sum as: $\sum_{i=j.cr}^{(j+1).cr-1} w'_i.c_i = \alpha.cr.a_j$.

Therefore, the embedded bits can be recovered as follows:

$$C(i) = \begin{cases} 1 & if \quad P(i) \geq 0 \\ -1 & if \quad P(i) < 0 \end{cases} \tag{3}$$

3. Residue Number System

Computation can be performed more efficiently by using RNS which expresses the large integer using a set of smaller integers. RNS is defined by the k integer constants set: (x_1, x_2, ..., x_k) referred to as moduli which are co-prime the integer X can be uniquely expressed by the set of *K-tuple* residues set: (r_1, r_2, ..., r_k), Where:

$$r_i = X \bmod x_i \tag{4}$$

The dynamic range of RNS is 0 to *M-1*, Where:

$$M = \prod_{i=1}^{k} x_i \tag{5}$$

Any positive integer X which lies in the range $0 \leq X < M$ can be represented by the unique *K-tuple* residue sequence as: To convert every integer X to residues, RNS is used and to get integer X back from residues Chinese Remainder Theorem (CRT) is used which is in Equation 6 as:

$$X = [\sum_{i=1}^{k} M_i \, | r_i L_i |_{m_i}] mod M \tag{6}$$

Where M is defined in Equation 5 and

$$M_i = \frac{M}{x_i} \tag{7}$$

And

$$|L_i M_i|_{x_i} = 1$$

Where L_i is the multiplicative inverse of M_i w.r.t x_i.

4. Chaotic Systems

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 [14].

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

One of the simplest logistic maps is:

$$X_{n+1} = (1 - 2X_n^2) \quad (7)$$

Where $x_0 \in (0, 1)$.

The other logistic map which contains an additional security parameter is:

$$X_{n+1} = rX_n(1 - X_n) \quad (8)$$

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

5. Arnold Transform

Arnold transform has special property that a given image comes to its original state after specific number of iterations. Hence, Arnold transform is used as efficient technique for increasing security in watermarking schemes [17]. The Arnold transform of image is:

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} (mod\ N) \quad (9)$$

Where $(x, y) = \{0, 1, 2, \ldots, N\}$ are the pixel coordinates from the original image and (x_n, y_n) denotes the pixel coordinates after performing Arnold transform.

6. Our Method

Our proposed watermarking scheme consists of two stages, embedding scheme and extraction scheme as seen in Figures 1 and 2, respectively. Main steps of embedding and extraction as under.

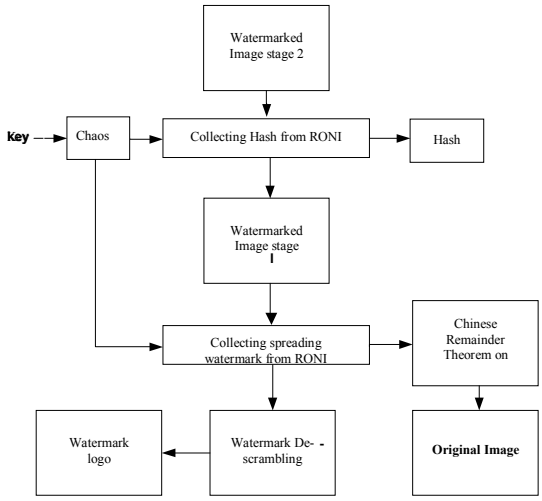

Figure 1. Proposed embedding scheme.

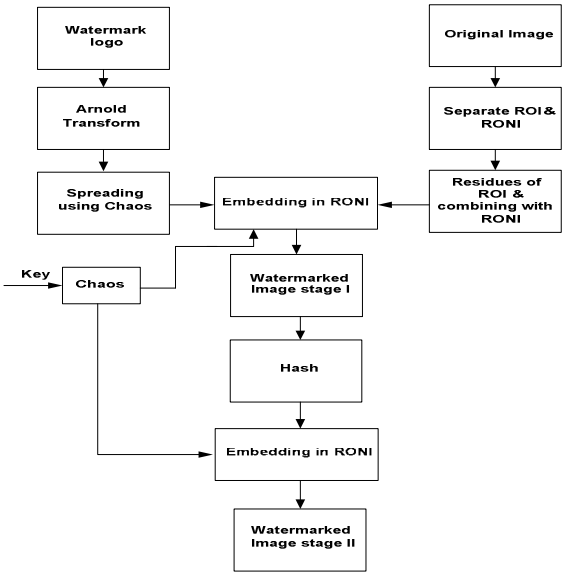

Figure 2. Proposed extraction scheme.

6.1. Embedding Scheme

Watermark embedding steps are as under:

1. Extract 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 has factors 17 and 15 which will be used as the moduli set (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 $x_1 \leq 16$ and $x_2 \leq 14$. 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.

   All of the above pairs which were to be represented by 9bits 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 pixels as pair (15, 15) which can be represented by 8bits. This unique pair cannot occur normally in this residual scheme with moduli 17 and 15.

3. Generate the chaotic sequence using Equation 8, multiply by 8 and take its ceil(.) so that the real chaotic sequences map into integers. For the sake of simplicity, chaotic integers from the logistic map are:

$$I_1=\{X_1, X_2, X_3, ...\} \tag{10}$$

Now, change the Equation 10 into sum sequences such as:

$$S=\{X_1, X_1+X_2, X_1+X_2+X_3, ...\}$$
$$=\{S_1, S_2, S_3, ..., S_k, S_{k+1}, ..., S_n\}$$

4. Read the watermark logo W which has to be made robust. Perform Arnold transform to scramble the watermark and convert it into binary vector.
5. Spread the binary watermark W by a factor cr to obtain a sequence. Suppose the length of obtained sequence is L.
6. Generate chaotic sequence P of length L using Equation 8 and then convert each real value of sequence into bipolar sequence C as:

$$C(i)=\begin{cases} 1 & if \quad P(i)\geq 0 \\ -1 & if \quad P(i)<0 \end{cases} \tag{11}$$

7. Modulate the bipolar sequence C with the spread watermark obtained in step 5 and store it in a vector W_s.
8. Arrange all the pixels of RONI in vector form and make the LSB's of $\{S_1, S_2, \ldots, S_k\}$ embedding positions to zero. Then embed the spreaded watermark W_s in RONI pixels based on chaotic key given in Equation 11 as described in section 2.1.
9. Again arrange all the pixels of RONI in vector form and combine it with residue ROI obtained in step 2.
10. Compute the hash of the image obtained in step this will give 128bit one way hash value which will be used as an authentication watermark H for the image.
11. Again arrange all the pixels of RONI in vector form and embed the authentication watermark H in $\{S_{k+1}, S_{k+2}, \ldots, S_n\}$ pixel positions by bit replacement method.
12. Rearrange the RONI pixels in its original position to obtain the watermarked image. Now, both the watermarks exist in RONI while ROI is residue.

6.2. Extraction Scheme

Watermark and original image extraction steps are as under:

1. Separate RONI from ROI in the watermarked image.
2. Arrange all the pixels of RONI in some arbitrary vector. Now, by knowing the same chaotic key as in embedding side, watermarked positions are indicated as:

$$\{S_1, S_2, ..., S_k, S_{k+1}..., S_n\}$$

Where $\{S_1, S_2, \ldots, S_k\}$ denotes the embedded positions for the spreaded watermark W_s and $\{S_{k+1}, S_{k+2}, \ldots, S_n\}$ denotes the embedded positions for hash.

3. Extract hash from the LSB's of $\{S_{k+1}, S_{k+2}, \ldots, S_n\}$ pixel positions and place a bit zero at that position. Hash extracted from LSB's is stored as hash_1.
4. Again arrange all the pixels of RONI with the ROI and compute the hash. Hash collected from this image is stored as hash_2.
5. Again arrange all the pixels of RONI in vector form and collect the de-spreaded watermark from $\{S_1, S_2, \ldots, S_k\}$ pixel positions using method described in section 2.2 and then perform inverse Arnold transform to get final watermark W_s
6. Compare hash_1 with hash_2. If the hash is same then the image is authentic and go to step 7 and step 8 to get the actual pixels of ROI else the image is tampered.
7. 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 9bits again. Then apply CRT to get back original pixels of ROI from residues.
8. Combine these ROI pixels with RONI pixels to get the original image.

7. Objective Measures for Robustness

To measure the degradation between original watermark and extracted watermark numbers of general objective measures are defined such as Normalized correlation (N_c), Structure Similarity Index (SSI) etc. In our scheme, we have measured robustness in terms of N_c which is defined as:

$$N_c(W, W') = \frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} W(i,j)W'(i,j)}{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left[W(i,j)\right]^2} \tag{12}$$

Where W and W' represents the original and extracted watermark respectively. M and N is the dimension of watermark. More the value of N_c closed to 1, more is the robustness of watermark.

8. Simulation Results

Experiments were conducted in MATLAB to see the effectiveness of our proposed system. The test image ultrasound image of size 194×259 and the watermark logo A of size 50×50was used. Logistic map2 as in Equation 8 with initial conditions $x(0)=0.25$ and $r=3.58$ is used. The value of α was chosen 6. Figure 3 shows the original ultrasound image and Figure 4 shows the watermark logo. Similarly, Figures 4, 5 and 6 show the hash, scrambled watermark and the watermarked image respectively.

Figure 3. Original ultrasound image.

Figure 4. Watermark logo.

7836411f512d c4d328ea2e40f a1654fe

Figure 5. Hash.

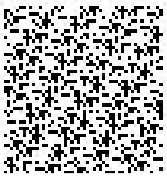

Figure 6. Scrambled watermark.

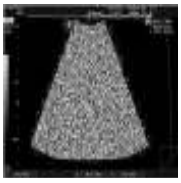

Figure 7. Watermarked Image

8.1. Security Analysis

In this experiment, security analysis of the proposed scheme is demonstrated firstly by using same initial conditions as in embedding side and then by using slightly different initial conditions at decoding stage. Exact hash and the original image is recovered with exact initial conditions $x(0)$=0.25, r=3.58 as shown in Figures 8 and 9 respectively. Figure 9 shows the recovered image with initial conditions $x(0)$=0.25, r=3.58 which is exactly same as in Figure 3. Recovered hash is shown with slightly modified initial conditions $x(0)$=0.250001 and r=3.58 in Figure 10. As we have seen that when initial conditions are slightly modified, exact hash is not recovered hence, the image is tampered which demonstrates the high secrecy of our proposed system.

7836411f512d c4d328ea2e40f a1654fe

Figure 8. Recovered hash with exact initial conditions $x(0)$=0.25, r=3.58.

Figure 9. Recovered image with exact initial conditions $x(0)$=0.25, r=3.58.

168ea2783641f512d 5c4d123e40f a 4fe

Figure 10. Recovered hash with initial conditions $x(0)$=0.250001 and r=3.58.

8.2. Robustness Analysis

Robustness of proposed scheme against speckle noise attack, Gaussian noise attack, salt and pepper noise attack, rotation attack, cropping attack and tampering attack is shown in Figures 11, 12, 13, 14, 15 and 16 respectively. The N_c value of extracted watermark is still good and watermark is easily detectable which shows high robustness of our proposed scheme.

Figure 11. Extracted watermark after adding speckle noise of variance 0.01showing N_c= 0.873.

Figure 12. Extracted watermark after adding gaussian noise of variance 0.01showing N_c= 0.794.

Figure 13. Extracted watermark after adding salt & pepper noise of variance 0.01showing N_c= 0.863.

Figure 14. Extracted watermark after rotation of 2 degree showing N_c= 0.851.

Figure 15. Extracted watermark after cropping some portion of watermarked image showing N_c= 0.651.

Figure 16. Extracted watermark after tampering some bits showing N_c= 0.764.

Table 1 shows the robustness of our proposed watermarking scheme for watermark logos given in the Figures 17, 18 and 19 respectively. N_c for watermark logo M given in the Figure 17 is shown in the first column of Table 1. When the image embedded with logo M of size (50×50) is compressed with QF=80, N_c comes to 0.893. Similarly when the QF becomes 70 and 70, N_c comes to 0.822 and 0.791 respectively. Similarly, N_c against salt and pepper noise, speckle noise and Gaussian noise attacks comes to 0.870, 0.870 and 0.781 respectively. When the image is embedded with logo H of size (60×60) given in Figure 18, N_c for the same attacks performed is shown in the second column of Table 1. When the image is compressed with QF=80, there is slight increase in N_c as compared to the N_c for logo M. Similarly, when QF=70, N_c remains same as for logo M. When QF=60, again there is increase in N_c as compared to the logo M. Similarly, for noise attacks, again there is slight increase in N_c as compared to the logo M. N_c for logo C given in Figure 19 of size (40×40) is given in the third column of Table 1.

Table 1. Demonstration of robustness in terms of 30.8 N_c under different attacks for watermarks of different sizes.

Attacks Performed	*Nc* using Figure 17	*Nc* using Figure 18	*Nc* using Figure 19
Compression with QF= 80	0.893	0.894	0.893
Compression with QF= 70	0.822	0.822	0.817
Compression with QF= 60	0.791	0.799	0.792
Rotation with 2 degree	0.831	0.830	0.810
Cropping 4×4 window in RONI	0.722	0.721	0.701
Adding Salt and pepper noise with variance 0.01	0.870	0.872	0.870
Adding Speckle noise with variance 0.01	0.870	0.871	0.871
Adding Gaussian noise with variance 0.01	0.781	0.782	0.782
Median filtering3×3	0.623	0.682	0.865

Figure 17. Watermark logo of size (50×50).

Figure 18. Watermark logo of size (60×60).

Figure 19. Watermark logo of size (40×40).

Table 2 presents the pros and cons of proposed scheme with the scheme presented in the literature. It clearly demonstrates that the proposed scheme outperforms better in terms of security and robustness. Our proposed method has more features than the scheme presented in [11].

Table 2. Pros and cons of proposed scheme with the scheme in [11].

Scheme in [11]	Proposed Scheme
Recovers watermark only	Recovers both the watermark and original image
Image is visible to naked eye	Image is not visible to the naked eye, thus achieving security
Spreading of watermark is done by PN sequence which is pseudorandom	Spreading of watermark is done by Chaotic sequence which is true random
Scheme claims security but experiment demonstrating security is not shown	Experiment demonstrating security is shown with exact initial conditions and then by slightly changed initial conditions
Makes the watermark information robust only	Makes the watermark robust and at the same time authenticates the image
Watermark information is not embedded based on key	Watermark information is embedded based on chaotic key, thus enhancing security
Robustness against different noise attacks is not shown as SS scheme is highly robust against noise attacks	Robustness against different noise attacks is shown

9. Conclusions

This paper presents the novel SS watermarking scheme based on RNS and chaos. In the proposed scheme, image is kept fragile while the watermark is made robust. RNS scheme is utilized to alter the image because in this way, the image becomes more secure. Moreover, the naked eye could not be able to see the image after altering; hence, it offers more security. Moduli of RNS also act as a key hence, makes the image more secure. The security of watermark is achieved by using Arnold transform and spread-spectrum technique. Hashing technique is utilized which also, enhances the security of image. Performance of the scheme was tested and results shows that it outperforms some of the existing schemes given in the literature.

References

[1] Acharya D., Rajendra U., Subbanna P., and Niranjan C., "Compact Storage of Medical Images with Patient Information," *IEEE Transactions on Information Technology in Biomedicine*, vol. 5, no. 4, pp. 320-323, 2001.

[2] Celik U., Sharma G., Tekalp M., and Saber E., "Reversible Data Hiding," available at: http://www.ece.rochester.edu/~gsharma/papers/reversiblehidingICIP02.pdf, last visited 2002.

[3] Chao M., Hsu M., and Miaou G., "A Data-Hiding Technique with Authentication, Integration and Confidentiality for EPR Records," *IEEE Transaction on Information Technology in Biomedicine*, vol. 6, no. 1, pp. 46-53, 2002.

[4] Coatrieux G., Maitre H., Sankur B., Rolland Y., and Collorec R., "Relevance of Watermarking in Medical Imaging," *in Proceedings of IEEE EMBS Conference on Information Technology Applications in Biomedicine*, Arlington, Viginia, pp. 250-255, 2000.

[5] Fridrich J., Goljan M., and Du R., "Invertible Authentication," *in Proceedings of International Conference on Information Technology: Coding and Computing*, Las Vegas, pp. 197-208, 2001.

[6] Fridrich J., Goljan M., and Du R., "Lossless Data Embedding-new Paradigm in Digital

Watermarking," *the Journal on Advances in Signal Processing*, vol. 2002, no. 2, pp. 185-196, 2002.

[7] Giakoumaki A., Pavlopoulos S., and Koutsouris D., "A Medical Image Watermarking Scheme Based on Wavelet Transform," *in Proceedings of the 25th Annual International Conference of the IEEE Engineering in Medical and Biology Society*, Cancun, Mexico, pp. 856-859, 2003.

[8] Gunjal L. and Mali N., "ROI based Embedded Watermarking of Medical Images for Secured Communication in Telemedicine," *the International Journal of Computer and Communication Engineering*, vol. 6, no. 48, pp. 293-298, 2012.

[9] Kasmani A. and Sharifi M., "A Pre-Filtering Method to Improve Watermark Detection Rate in DCT based Watermarking," *the International Arab Journal of Information Technology*, vol. 11, no. 2, pp. 178-185, 2014.

[10] Kim M., Li D., and Hong S., " A Robust and Digital Watermarking Technique for Image Contents based on DWT-DFRNT Multiple Transform Method," *the International Journal of Multimedia and Ubiquitous Engineering*, vol. 9, no. 1, pp. 369-378, 2014.

[11] Kumar B., Singh V., Singh P., and Mohan A., "Secure Spread-Spectrum Watermarking for Telemedicine Applications," *the Journal of Information Security*, vol. 2, no. 2, pp. 91-98, 2011.

[12] Li Y., Li T., and Wei H., "Protection of Mammograms using Blind Steganography and Watermarking," *in Proceedings of the 3rd International Symposium on Information Assurance and Security*, Manchester, UK, pp. 496-500, 2007.

[13] Masoumi M. and Amiri S., "Content Protection in Video Data Based on Robust Digital Watermarking Resistant to Intentional and Unintentional Attacks," *the International Arab Journal of Information Technology*, vol. 11, no. 2, pp. 204-212, 2014.

[14] Munir R., Riyanto B., Sutikno S., and Agung P., "Secure Spread Spectrum Watremarking Algorithm based on Chaotic Map for still images," *in Proceedings of the International Conference on Electrical Engineering and Informatics*, Indonesia, pp. 17-19, 2007.

[15] Naseem T., Qureshi M., Cheema A., and Rahman A., "Hash based Medical Image Authentication and Recovery using Chaos and Residue Number System," *the Journal of Basic and Applied Scientific Research*, vol. 3, no. 6, pp. 488-495, 2013.

[16] Naseem T., Qureshi M., Cheema A., and Zubair M., "Invertible and Fragile Watermarking for Medical Images using Residue Number System and Chaos," *the Journal of Basic and Applied Scientific Research*, vol. 10, no. 2, pp. 10643-10651, 2012.

[17] Pradhan C., Saxena V., and Kumar Bisoi A., "Imperceptible Watermarking Technique using Arnold's Transform and Cross Chaotic Map in DCT Domain," *the International Journal of Computer Applications*, vol. 55, no. 15, pp. 50, 2012.

[18] Ramaswamy R. and Arumugam V., "Lossless Data Hiding based on Histogram Modification," *the International Arab Journal of Information. Technology*, vol. 9, no. 5, pp. 445-451, 2012.

[19] Rey C. and Dugelay L., "A Survey of Watermarking Algorithm for Image Authentication," *EURASIP Journal on Applied Signal Processing*, vol. 6, no. 1, pp. 613-621, 2002.

[20] Saxena A., Sinha K., Chakrawarti S., and Charu S., "Digital Watermarking using MATLAB," *the International Journal of Advances in Science Engineering and Technology*, vol. 1, no. 3, pp. 39-42, 2014.

[21] Soliman M., Hassanien E., Ghali I., and Onsi M., "An Adaptive Watermarking Approach for Medical Imaging using Swarm Intelligent," *the International Journal of Smart Home*, vol. 6, no. 1, pp. 37-45, 2012.

[22] Song C., Sudirman S., and Merabti M., "Recent Advances and Classification of Watermarking Techniques in Digital Images," available at: http://dcalab.unipv.it/wp-content/ uploads/ 2015/02/ watermarking_articolo.pdf, last visited 2015.

[23] Sun G., Zhang Y., Yao H., and Wu P., "A Reversible Digital Watermarking Algorithm for Vector Maps," *International Journal of Network Security*, vol. 16, no. 1, pp. 40-45, 2014.

[24] Tian J., "High Capacity Reversible Data Embedding and Content Authentication," *in Proceedings of IEEE International conference on Acoustics, Speech and Signal Processing*, pp. 517-520, 2001.

[25] Trichili H., Boublel M., Derbel N., and Kamoun L., "A New Medical Image Watermarking Scheme for A Better Telediagnosis," *in Proceedings of IEEE International conference on Systems, Man and Cybernetics*, Tunisia, pp. 557-560, 2002.

[26] Woo I. and Lee D., "Digital Watermarking for Image Tamper Detection using Block-Wise Technique," *International Journal of Smart Home*, vol. 7, no. 5, pp. 115 2013.

[27] Zhou Q., Huang K., and Lou L., "Authenticity and Integrity of Digital Mammography Images," *IEEE Transactions on Medical Imaging*, vol. 20, no. 8, pp. 784-791, 2001.

Muhammad Naseem received the BS degree in Computer Science from University of the Punjab, Pakistan and MS degree in Electronic Engineering from International Islamic University, Pakistan in 2005 and 2008, respectively. He completed his PhD in Electronic Engineering in 2015 from Isra University, Islamabad campus. Currently he is working as Assistant Professor in department of computer science and software engineering in International Islamic University, Islamabad Pakistan. His research interests include digital watermarking, digital signal processing, information security and biomedical imaging.

Ijaz Qureshi has received his BE degree in Avionic Engineering from NED University Karachi, Pakistan. First MS degree in Electrical Engineering from Middle East Technical University (METU), Ankara, Turkey and second MS degree in High Energy Physics from Syracuse University, USA . He earned his PhD degree in High Energy Physics from University of Toronto, Toronto. He has more that twenty-seven year post PhD experience in teaching and research at different intuitions of good repute in Pakistan. More than fourteen PhD has been produced in his supervision. Currently he is Professor at Electrical Engineering departments, Air University Islamabad, Pakistan. His research interests include digital/wireless communications, digital signal processing, information and coding theory, soft and evolutionary computing.

Muhammad Muzaffar received the Msc degree in Computer Science from Bahauddin Zakariya University, Multan and MS degree in Electronic Engineering from International Islamic University, Pakistan in 2005 and 2008, respectively. He is working as Assistant Professor at National university of Modern Languages (NUML), Pakistan. Currently, he is a PhD research student at ISRA University Islamabad Campus, Pakistan. His research interests include audio steganography and information security.

Atta ur Rahman has received his BS degree in Computer Science from University of the Punjab Lahore, Pakistan in 2004; MS degree in Electronic Engineering from International Islamic University, Pakistan in 2008 and PhD degree in Electronic Engineering from ISRA University, Islamabad Campus, Pakistan in 2012. Currently, he is working as Associate Professor as well as Deputy Director at Barani Institute of Information Technology (BIIT), PMAS-AA University Rawalpindi, Pakistan. His research interests include digital/wireless communications, digital signal processing, information and coding theory, soft-computing, artificial intelligence, evolutionary computing and fuzzy and hybrid intelligent systems.