ROBUST AND FRAGILE WATERMARKING FOR MEDICAL IMAGES USING REDUNDANT RESIDUE NUMBER SYSTEM AND CHAOS

M.T. Naseem[*], *I.M. Qureshi*[†], *Atta-ur-Rahman*[‡], *M.Z. Muzaffar*[§]

Abstract: This research discusses a novel watermarking scheme using redundant residue number system and chaos. The salient feature of said research is that image remains fragile while the watermark information is made robust. Image pixels are converted into residues so that the unaided eye could not see the image contents. To make the image invisible to the unaided eye, only the ROI part of image is passed through the Residue Number System thus, to enhance the secrecy of the image. While converting the ROI part of image into residues, there are some residues which exceed eight bits so, these residues are converted to exact eight bits by pertaining some intelligent mechanism. To achieve the robustness of watermark, firstly redundant residues of watermark are made and then the resultant watermark is encoded through error correcting codes. To achieve the fragility of image, hashing technique is utilized. Hash of the entire image but with the residued ROI is combined with the encoded and redundant residued watermark and then resultant watermark is embedded in the Region of non-interest (RONI) zone of native image rooted on the chaotic key in order to enhance the security of the watermark. In case of no tampering, fragile watermark can be successfully recovered as well as exact recovery of the original image but if the image is attacked, the fragile watermark is destroyed while the robust watermark is extracted with better readability.

Key words: *medical image watermarking, fragility, robustness, RNS, RRNS, Chinese Remainder Theorem (CRT), chaotic function*

Received: March 12, 2019
Revised and accepted: June 30, 2020

DOI: 10.14311/NNW.2020.30.013

[*]Muhammad Tahir Naseem; Department of Computer Science, Faculty of Computing, Riphah International University, Lahore, Pakistan, E-mail: tahir.naseem@riphah.edu.pk

[†]Ijaz Mansoor Qureshi; Department of Electrical Engineering, Air University, Islamabad, Pakistan, E-mail: imqureshi@mail.au.edu.pk

[‡]Atta-ur-Rahman – Corresponding author; Department of Computer Science, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam, 31441, Saudi Arabia, E-mail: aaurrahman@iau.edu.sa

[§]Muhammad Zeeshan Muzaffar; Barani Institute of Information Technology, Rawalpindi, Pakistan, E-mail: Email: zeeshan@biit.edu.pk

1. Introduction

Watermarking is defined as a process of embedding some secret watermark into multimedia contents such as image, audio, and video to protect the owner's right to that content. Later the watermark is extracted from the suspected image and is used to verify the ownership identification. Watermarking can be broadly classified into three categories: Fragile, Robust and Semi-fragile. Fragile watermarks are very sensitive and can be easily affected by tampering any bit in an image, while robust watermarks stuck into the document and can withstand the attacks. Such watermarks are Semi-fragile which are fragile to malicious attacks but are robust against incidental attacks. Watermarking spans over two domains; namely spatial transform domains. In the former, the secret watermark information is inserted in the image by means of altering its pixels while in the latter case, the secret information is embedded after taking the transforms like discrete wavelet transform (DWT) etc. Though the transform domain watermarking in is complex but provides more robustness than the techniques in spatial domain.

Diagnosis is done on the medical images before storing in order to preserve ROI [25]. Although the new trends in communicating and sharing the information opens the new ways to retrieve process and move the medical images so that the manipulation and replication can be done easily [8]. Whether the aim is to store or to transfer the medical information from source to destination for further diagnosis, security is the key issue which should not be compromised in any sense so, there is a need of strong security measures for preserving the medical information. Watermarking for natural images embeds the digital information without much altering the image pixels which is often called imperceptibility which is an important requirement in the watermarking of digital data [11]. A novel watermarking scheme to verify the authenticity and integrity of the digital mammographic images is presented in [30]. The digital envelope as a secret watermark information is used and one bit of the digital envelope was embedded in the LSB's of one random pixel of the mammogram image. To check the integrity, instead of considering the whole image, some portion of the image i.e. the MSB of each pixel is used. Patient information can also be interleaved with the medical images to avoid from overheads such as channel noise etc [1]. For embedding the data in the image, LSB replacement was adapted as discussed previously. Furthermore in [6], a DCT based watermarking scheme is presented which hides Electronic Medical Record (EMR) related data into the medical image. The DCT coefficients are quantized first and then the information is embedded. Limitation in the above discussed scheme is that, it is impossible to recover the coefficients of host original image in the said technique because after embedding host image is altered in non-invertible manner.

In this modern era, much attention has been given in the area of invertible watermarking of medical images because in order to make proper diagnosis for a forensic pathologist, original image is also needed at receiver end. In invertible watermarking, the digital watermark is inserted into the original image in such a way that later on, after extraction of watermark, contents of the original host image can also be recovered back completely [5,9,10,22]. A novel watermarking scheme is presented in [23], in which the border of the image is used as a watermarking area and then the patient information is embedded into the LSB's of the border pixels of

original image. Another watermarking scheme is also presented in which the digital signature of the whole image combining with patient information is embedded in the image but the work was enhanced in [4] in which the difference expansion of digital envelope is embedded by replacing the LSB of each pixel selected randomly. A watermarking scheme for telemedicine application has also been presented in [2]. The scheme embeds the patient information in DWT domain of the medical image using hospital image as a reference. The advantage of scheme is that original image is not needed at receiver end for retrieval of patient information.

Image authentication watermarking scheme providing stringent constraint on medical images has also been presented in [3]. The scheme presents modified difference expansion watermarking scheme using LSB replacement method in the difference of virtual border for data hiding. To increase the embedding capacity, scheme also uses the class dependent coding scheme (CDCS) to encode the patient data. The scheme provides high imperceptibility as compared to the other schemes. The drawback of scheme is that only the watermark information is retrieved. Another medical image watermarking scheme is also presented which increases the data hiding capacity as well as security in [14]. Data is hidden by using the technique of difference pair mapping (DPM) which is based on predicting the pixel values. The scheme is also reversible as original image contents are also retrieved at the receiver side. Another watermarking scheme is also presented in [15] which embed the watermark information in the discrete wavelet packet transform (DWPT) of the medical image. To enhance the robustness, scheme also uses ECC. The scheme has an advantage of its blindness, but the drawback is that only the watermark information is recovered.

The most significant condition in the medical image communication is that, the image should not be evident to the naked eye [31]. This in fact enhances the privacy as the visibility of medical images should not be provided according to Health Insurance Portability and Accountability Act (HIPAA) 1996 US standard [32]. According to HIPAA Act patient's information that is usually named as patient health record (PHR) must not be intercepted by the third party (other than patient and the concerned doctor). Keeping this measurement in mind, fragility, and reversibility for watermarking of medical images using chaotic key and RNS has already been done by Naseem et al. in [17] 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. The overhead was also removed by applying some trick on the residues [16].

In this paper, to model watermark robust while keeping the image fragile at a same time, we are proposing RRNS and ECC along with the chaotic key. According to (HIPAA) Act 1996 US standard patient's information that is usually PHR must not be intercepted by the third party (other than patient and the concerned doctor). Keeping this measurement in mind, image is converted into residues to enhance its secrecy and sensitivity so that the human eye could not perceive it. To achieve the robustness, redundant residues of watermark are made while the ROI part of image is residued so that it is not visible to the naked eye, thus enhancing the security of the image. Moreover, there are some pixel pairs in an image which

are greater than size eight when the ROI part of image is converted into residues so, to bring them back to size eight ,some mapping technique is applied on those pairs. Paired watermarks are used; one to achieve the robustness of watermark and other to achieve the authenticity of image. As a pre-processing step, on the basis of chaotic equation, some pre-calculated pixels in RONI are made black by converting into zeros and then this RONI is repositioned with converted residues ROI part of image and then 128 bit hash is generated by using hashing algorithm. To achieve the robustness, the other watermark is passed through redundant residue number system and then is encoded using ECC and finally is bring together with the fragile watermark information. Once more, on the basis of same chaotic sequence generated by same chaotic key, combined watermark information is embedded in RONI pixels of image by restoring the 4 LSB's of pixels thus, enhancing the security of the watermark information. Based on same chaotic sequence generated by same chaotic key, at the receiver side both the watermarks are extracted. To make the proposed scheme blind, original image is not needed at receiver side.

Organization of the rest of the paper is described as follows: Section 2 describes the candidate schemes used in the said research. Section 3 describes the proposed watermarking scheme and objective measure for robustness of watermark is presented in Section 4.2. Section 4 is about simulation and results and finally Section 5 concludes the said research.

2. Description of candidate schemes

This section describes about the candidate schemes used in the said research. Detail of each scheme is given below.

2.1 Redundant Residue Number System

RRNS incorporates extra moduli which is helpful in detecting and correcting of errors in RNS system. In RNS, large numbers are represented using set of smaller integers to make computations more efficiently with reduced power consumption [21]. Mathematically, It is interpreted as the composition of small k fixed integers $(m_1, m_2, \ldots, m_k)$ which are termed as moduli which are co-prime. By using the set of unique k-tuple residues (x_1, x_2, x_k), the integer X can be represented as,

$$x_i = X \mod m_i, \tag{1}$$

The active span of RNS is 0 to $M-1$,

$$\text{where } M = \prod_{i=1}^{k} m_i. \tag{2}$$

Any positive integer X which lies in the range $\leq X < M$ can be represented by the distinct $k-$tuple residue sequence and then Chinese remainder theorem (CRT) is used to regain integer X from the residues by using the following mathematical equation as,

$$X = \left[\sum_{i=1}^{k} M_i |x_i L_i|_{m_i}\right] \mod M, \tag{3}$$

where M is defined in Eq. 2 and $M_i = \frac{M}{m_i}$ and L_i is the multiplicative inverse of M_i w.r.t m_i and $|a|_b$ denotes the modulo of a with respect to b.

The most important property in RRNS is that if any $n-k$ residues out of n residues are corrupted, then any k residues associated with k moduli could be used to calculate the decimal representation of integer X. In other words, RRNS can be used in detection and corrections of errors as discussed in [12,13,20,28,29]. Due to features of RNS, it has many applications in performing arithmetic functions like digital signal processing [19], image processing [26], RSA ciphering system [7] and in digital communication [18].

2.2 Chaotic systems

Chaotic systems are very famous systems and are suitable to model the practical systems on account of their higher sensitivity to its initial conditions. There are so many other characteristics of chaotic systems but the most salient one is sensitivity so, from all these characteristics makes chaos a good candidate for security [24,28]. Chaotic actions are very tough to forecast by using analytical methods and without understanding of demanded secret key.

One of the simplest Logistic maps is given in Eq. 4 as

$$x_{n+1} = (1 - 2x_n^2), \tag{4}$$

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

The other Logistic map which is the enhanced version of above Logistic map is given as

$$x_{n+1} = rx_n(1 - x_n), \tag{5}$$

where $x_0 \in (0, 1)$ and r is called a bifurcation parameter also used as a security key and for chaotic actions, the strict range is; $3.57 < r \leq 4$. In order to generate chaotic behavior from the logistic map, the value of r should be greater than 3.57 and less than or equal to 4. In the literature, there are also other chaotic maps as well the researchers has used.

2.3 Error correcting codes

Error detection and correction is such a novel technique that enables reliable transfer of digital data over fly-by-night communication channels like Mobile Cellular [33] and Satellite channels [34,35]. In this regard, several error correcting codes exist in the practice like Reed Solomon codes, Low Density Parity Check (LDPC) codes, convolutional codes and BCH codes. BCH codes are systematic and Hamming codes, that can detect as well as correct the errors on the receiver side [36].

3. Proposed watermarking scheme

In the said research, the proposed methodology can be divided into two phases: embedding the watermark information phase; logo in our case and watermark & original image extraction phase which can be depicted in Fig. 1 and Fig. 2 respectively.

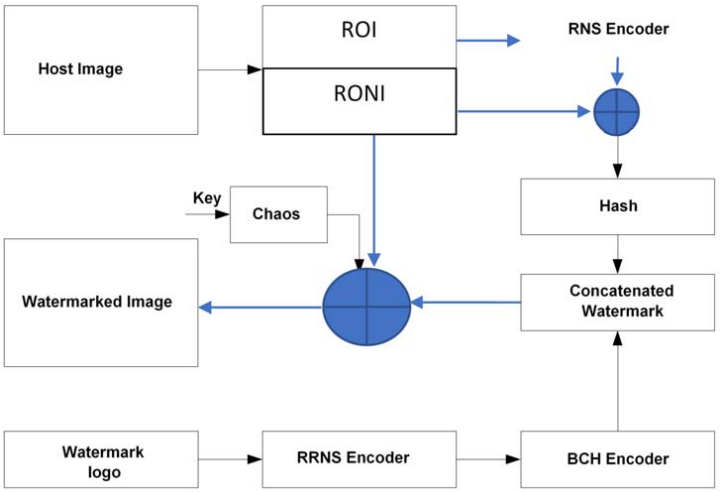

Fig. 1 *Proposed watermark embedding scheme.*

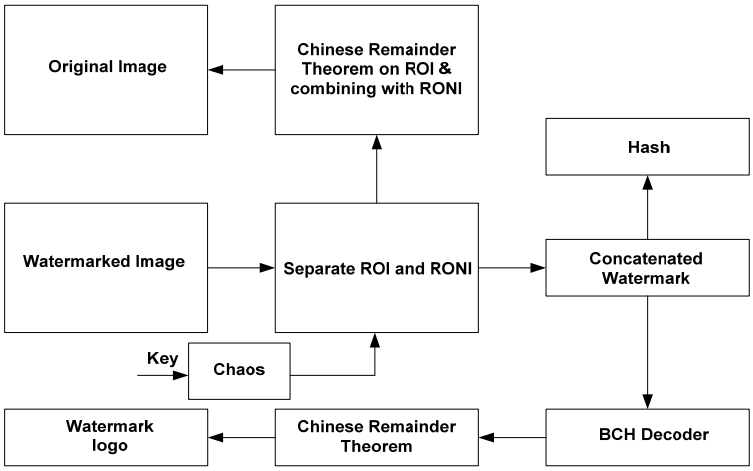

Fig. 2 *Proposed watermark & original image extraction scheme.*

3.1 Watermark embedding

Following are the key steps for embedding the watermark information.

1. By narrowing the small-scale possible rectangle all over the place of desired area from the original image, pull out the smallest possible area of ROI.

2. The maximum grey scale value in an image is 255 which is factorized to two numbers; 15 and 17 which corresponds to (m_1,m_2) the pair of moduli of the RNS applied to the image. As discussed above, since, the active span of RNS is between 0 and 254 so every pixel with intensity value 255 is handled

separately. Here, the pre-processing of the converted pixels into residues is a key to get the pixels values back. For every intensity value pixel from ROI, we get residue pairs (x_1,x_2) where $x_i = X \mod m_i$ such that $x_1 \leq 16$ and $x_2 \leq 14$. As an exceptional case when $x_1 = 16$, it is noticed that x_1 and x_2 needs 4 bits each making the 8-bits pair representation. To handle the scenario and making it compatible with the existing RNS setup, following smart mapping is introduced. It is a reversible mapping, hence there is no harm in terms of pixel values.

$$\text{Forward conversion procedure} \quad (16, 12) \rightarrow (12, 16) \xrightarrow{16-1} (12, 15)$$

$$\text{Reverse conversion procedure} \quad (12, 15) \rightarrow (15, 12) \xrightarrow{15+1} (16, 12)$$

3. After passing these pixels to RNS, pixel value 255 has residue $(0, 0)$. There must be differentiation of pixel value 0 which also has residue $(0, 0)$ from pixel value 255 as both have same residue. To get rid of this, pixel pair $(15, 15)$ will be transmitted as 255 intensity value which can be represented by 8 bits most. Thus, this distinct set cannot occur normally in this residual scheme with moduli set 15 and 17.

4. Generate a chaotic sequence of 14,207 numbers using Eq. 5, multiply the generated sequence by 3 and take its ceil(.) to convert the real chaotic sequence into integers as,
$$S = \{x_1, x_2, x_3 \dots\}.$$
To make sum sequence, the above sequence can be converted as,
$$\begin{aligned} S &= \{x_1, x_1 + x_2, x_1 + x_2 + x_3, \dots\} \\ &= \{y_1, y_2, y_3, \dots\} \\ \text{where } y_i &= x_1 + x_2 + \cdots + x_i. \end{aligned}$$
After converting into sum sequence, divide each sequence by 2 so that its range corresponds within RONI and then take its ceiling value as:
$$Z = \text{ceil}(\{y_1/2,\ y_2/2,\ y_3/2, \dots\}).$$
This sequence which is an outcome of chaotic sequence will give locations for embedding the concatenated watermark in the RONI part of original image.

5. Organize all the pixels of RONI in an ordered set form. There are total 20,438 pixels in the RONI for watermark embedding and we need only 14,207 pixels for embedding. Make the first 4 LSB's of those corresponding pixels of RONI to zero by using the chaotic sequence obtained in step 3.

6. Rearrange the residued ROI obtained in step 2 with the RONI pixels obtained in step 4.

7. From the image obtained from step 5, compute the hash value. This will give 128-bit hash value which will be used to authenticate the image at receiver side.

8. Look through the second watermark logo which must be made robust and for each pixel calculate the residues (x_1, x_2, x_3) with respect to moduli $(m_1, m_2, m_3) = (17, 15, 19)$. Here m_3 is chosen as redundant moduli. Now the watermark pixel which is residued is represented by at most 14 bits and then concatenate 2 zeros to the left side of each residue so that each residue is converted into 16 bits.

9. Arrange the redundant residued watermark matrix into vector form.

10. Encode each entry of the redundant residued vector using Error correcting codes $(63, 16, 11)$ which gives us an encoded redundant residued watermark.

11. Organize the encoded redundant residued watermark in a vector and concatenate it with the hash computed in step 6 and call it a concatenated watermark W_{C} as,
$$W_c = [H, W_e]\,.$$

12. As in step 4, once more organize the pixels of RONI in an ordered form and insert the watermark W_c on the basis of chaotic sequence computed in step 3 by restoring the four LSB's of RONI with every four bits of the watermark W_c.

13. To obtain the watermarked image, regroup the RONI pixels in its original position.

3.2 Watermark and original image extraction

Following are the key steps for watermark and original image extraction.

1. Split both ROI and RONI parts from the watermarked image.

2. Store all the pixels of RONI part in some random vector. By using the same chaotic key, watermarked pixels are pointed as,
$$Z = \mathrm{ceil}(\{y_1/2,\, y_2/2,\, y_3/2, \dots\}).$$
This sequence of 14,207 indexes which is an outcome of chaotic key will give locations for extracting the combined watermark W_c from the RONI part of watermarked image.

3. From the chaotic sequence used in step 2, extract the combined watermark W_c from the first 4 LSB's of RONI pixels and store in some vector as,
$$W_c = [H, W_e]\,.$$

4. Apart the encoded redundant residued watermark W_e from the concatenated watermark W_c and decode its each pixel (16 bits) using $(63, 16, 11)$ error correcting code to get the redundant residued information. After discarding the two left most bits, we will get residues not the actual information. Now we have total 14 bits of residues in which first 5 bits corresponds to moduli m_1 second 4 bits corresponds to moduli m_2 and the last 5 bits corresponds to moduli m_3.

5. By considering the moduli pair associated with residues pairs out of three residues as (m_1, m_2) or (m_2, m_3) or (m_1, m_3) apply Chinese remainder theorem (CRT) expressed in Eq. 3 to get back actual pixels of watermark.

6. To describe an image, regroup these RONI pixels with the residued ROI. Then, compute the hash of this whole image and store it as hash_2. Also separate the hash from the combined watermark W_c and store it as hash_1.

7. Now collate first hash with the second hash. If both hashes are paired then it means the image is actual (no tempering) and proceed to step 7 and step 8 else we will conclude that the image is tampered.

8. While scanning the residued ROI part of image, the residue pairs with second residue as value 15 goes through the inversion process described in the step 2 of the embedding process. In this fashion, we will be able to convert all the residue pairs into 9 bits again. CRT given in Eq. 3 is applied to regain the original pixels of ROI part from the residues.

9. Merge these RONI pixels with ROI pixels with to restore the original image.

To measure the change between original watermark information and extracted watermark information, number of estimators are used by the researchers. From them, one of them is normalized correlation (N_c) which is defined as,

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

where W and W' represents the original and extracted watermark respectively while M and N denotes the size of watermark [36–38].

4. Simulation & results

Tests were run in the MATLAB tool to sight the effectiveness of said research. The trial image was taken as an ultrasound image of size 200×256 pixels and the watermark logo **A** was taken of size 30×30 to check robustness. BCH code $(63, 16, 11)$ was used to test the robustness of watermark information which is logo **A**. The said scheme affectionately embeds the encoded residued watermark into the native image and then draws out the watermark logo from the watermarked image. Logistic map 2 which is specified in Eq. 5 with initial conditions $x(0) = 0.25, r = 3.58$ is used at embedding side and SHA-128 hash algorithm is used to compute the hash of image. Given below, Fig. 3a shows the native ultrasound image in which ROI part is selected as a little rectangular region that leaps the ROI region and similarly, Fig. 3b shows the hash of image. Moreover, Fig. 3c shows the watermark logo and finally Fig. 3d shows the watermarked image. We have verified the robustness of the said research against various well defend attacks given in the literature as well the fragility was also checked.

4.1 Security analysis

Reliability exploration of the said research is shown primarily by using same initial conditions at and then by using minute modifying the initial conditions at extracting side in this test. Required hash and native image is retaken back when no attack is applied to the watermarked image. Fig. 4 given below indicates the reclaimed hash with initial conditions $x(0) = 0.25, r = 3.58$ which is quite same as shown in the Fig. 3b. Similarly, Fig. 5 shows the retrieved image with initial conditions $x(0) = 0.25, r = 3.58$ which is same as depicted in the Fig. 3a. Moreover, Fig. 6 indicates the recovered hash with initial conditions $x(0) = 0.250001, r = 3.58$. We can see from the above discussion that when initial conditions are modified to slight extent, required hash is not recovered which means the image is modified from somewhere which exhibits the high-rise secrecy of said research.

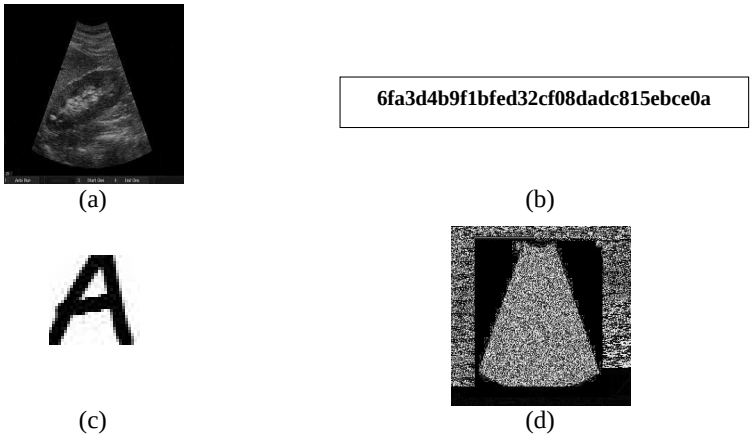

Fig. 3 *(a) Original image. (b) Hash (c) Watermark logo (d) Watermarked image.*

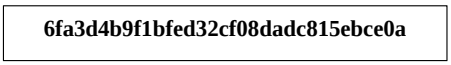

Fig. 4 *Recovered hash using exact initial conditions* $x(0) = 0.25, r = 3.58$ *at receiver side.*

4.2 Robustness analysis

This section highlights the robustness of the proposed scheme again several known attacks.

4.2.1 Salt & pepper noise

Robustness of a watermark with Salt and pepper noise with variance of (0.02, 0.2) is examined in this test. Normalized Correlation against salt & pepper attack is given in the Fig. 7 along with the respective watermarks. In consequence, when noise

Fig. 5 *Recovered image using exact initial conditions* $x(0) = 0.25, r = 3.58$ *at receiver side.*

A38c4529a5e607283d4c61a246ae838f

Fig. 6 *Recovered hash using slightly changed initial conditions.*

Normalized Correlation = 1 with variances of $(0.02, 0.2)$

(a)

Normalized Correlation = 0.9821with variances of $(0.02, 0.2)$

(b)

Fig. 7 *Extracted watermark with different variances.*

variance was enhanced to 0.2, the watermark is still understandably detectable which plainly illustrates the robustness of our said method.

4.2.2 Speckle noise

Robustness of a watermark with speckle noise with variance of (0.02, 0.2) are considered in this experiment. Normalized Correlation against speckle noise attack is given in the Fig. 8 along with the watermarks. We can easily see from the Fig. 8 that the watermark information is robust to speckle noise with high variance.

Normalized Correlation = 1 with variances of $(0.02, 0.2)$

(a)

Normalized Correlation = 0.9723with variances of $(0.02, 0.2)$

(b)

Fig. 8 *Extracted watermark with different variances.*

4.2.3 Median filtering

Robustness of a watermark in case of median filtering with window size of $(3 \times 3, 5 \times 5)$ are considered in this experiment. Normalized Correlation against median filtering attack is given in the Fig. 9 along with the watermarks. Experiment shows that the watermark logo is still readable with high value of Normalized Correlation.

Normalized Correlation = 0.9819 with window size of $(3\times3, 5\times5)$
(a)

Normalized Correlation = 0.9723 with window size of $(3\times3, 5\times5)$
(b)

Fig. 9 *Extracted watermark with different window size.*

4.2.4 Tampering

Robustness in case of tampering is demonstrated in the Fig. 10. Fifteen bits were altered in RONI part of watermarked image and watermark information is pulled out with Normalized Correlation 0.9887 and watermark logo is still acceptable as shown in Fig. 10a. When the altered bits were enhanced to thirty bits, the watermark is still clear as shown in Fig. 10b with high value of Normalized Correlation which shows the excessive robustness of our said model.

Normalized Correlation = 0.9887
(a)

Normalized Correlation = 0.9819
(b)

Fig. 10 *Extracted watermark with tampering (a) 15 bits are tampered in ROINI. (b) 30 bits are tampered in RONI.*

Fig. 11 shows different original images from medical domain each with size of 512×512 pixels. Tab. I indicates the comparison of said model in case of different attacks with the work given in [15] in terms of N_c for embedding the capacity of 2048 bits. For MRI1 image, when the watermarked image is passed through median filtering attack for the window size of 3×3, Normalized Correlation of scheme in [15] is 0.9736 while for our scheme, Normalized Correlation is 0.9837 which is higher than the existing scheme. Similarly, for the other images our scheme has performed better than the scheme in [15]. When the MRI1 watermarked image is passed through contrast attack with factor of 30, Normalized Correlation of scheme in [15] is 1 while our scheme is 0.998. Similarly, when the MRI1 watermarked image is passed through compression attack with quality factor (QF = 30), Normalized

Correlation of scheme in [15] is 0.9606 while Normalized Correlation of our scheme is 0.977 which is higher than the existing scheme. Hence, our proposed scheme has performed well than the scheme discussed in [15].

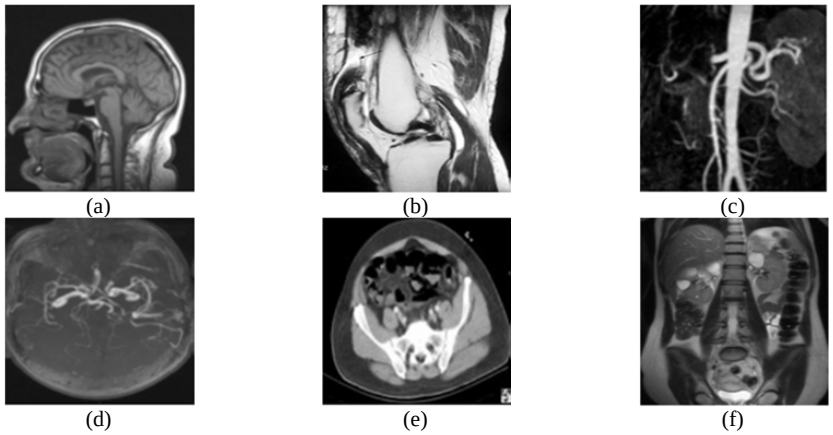

Fig. 11 *Different images of size* 512×512 *(a) MRI1, (b) MRI2, (c) MRA1, (d) MRA2, (e) CT1, (f) CT2.*

Images	Median Filtering attack with window size of 3×3		Contrast Attack with factor = 30		JPEG Compression Attack with QF = 60%	
	Scheme in [15]	Proposed Scheme	Scheme in [15]	Proposed Scheme	Scheme in [15]	Proposed Scheme
MRI1	0.9736	0.9837	1	0.998	0.9606	0.977
MRI2	0.9645	0.9745	0.982	0.998	0.9890	0.998
MRA1	0.9902	0.9941	0.979	0.978	0.8575	0.867
MRI2	0.9915	0.9926	0.995	0.997	1	0.999
CT1	0.9439	0.9739	0.888	0.987	0.9590	0.996
CT2	0.982	0.9943	0.996	0.997	0.9939	0.994

Tab. I *Quantitative Comparison of proposed scheme with the scheme in [15] in terms of Normalized Correlation by embedding capacity of 2048 bits (2Kbits).*

Tab. II shows the qualitative measure of our proposed scheme with the scheme given in [15]. It is crystal clear from the previous discussion that the proposed scheme has more features than the scheme discussed in the literature [15]. Tab. II also handouts the enhanced features which alters the said model with the work given in [15] in terms of recovery, robustness, and secrecy.

Scheme in [15]	Proposed Scheme
Recovers watermark information only	Recovers watermark information along with the original image
Image is visible to the naked eye	Image is not visible to the naked eye thus increasing security
Makes the watermark information robust only	Makes the watermark information robust while making the image fragile

Tab. II *Qualitative Comparison of proposed scheme with the scheme in [15].*

5. Conclusion

A novel watermark embedding model for securing the medical images by making the watermark robust using RRNS and ECC codes, while keeping the image fragile by means of Chaotic key, is proposed. In the proposed scheme, RNS model takes advantage to modify the image so that the host image becomes secure, sensitive and hidden from the naked eye thus achieving privacy and security. Moreover, embedding positions give rise to the chaotic sequence generated from chaos for embedding the watermark information, which is highly sensitive to the initial conditions. Thus, the security of the watermark is enhanced, and the schemes becomes align to the medical imaging requirements for today's picture archiving and communication system (PACS). The proposed watermarking scheme is evaluated against variety of attacks and robustness is shown. Finally, the important feature of the said research is to make it blind as it does not need original image at the receiver end.

References

[1] ACHARYA R., ANAND D., BHAT S., NIRANJAN U.C. *Compact storage of medical images with patient information.* IEEE Transaction on Information Technology in Biomedicine. 2001, 5(4), pp. 320–323, doi: 10.1109/4233.966107.

[2] ANUSUDHA K., N. VENKATESWAREN N. *Energy Based Wavelet Domain Medical Image Watermarking.* Energy. 2014, 3(2), pp. 7132–7140.

[3] BRAR A.S., KAUR M. *High Capacity, Reversible Data Hiding Using CDCS Along with Medical Image Authentication.* International Journal of Signal Processing, Image Processing and Pattern Recognition, 2015, 8(1), pp. 49–60, doi: 10.14257/ijsip.2015.8.1.05.

[4] CAO F., HUANG H.K., ZHOU X.Q. *Medical image security in a HIPAA mandated PACS environment.* Computerized Medical Imaging and Graphics. 2003, 27(2), pp. 185–196, doi: 10.1016/s0895-6111(02)00073-3.

[5] CELIK M.U., SHARMA G., TEKALP A.M., SABER E. Reversible data hiding. In: *IEEE International Conference on Image Processing,* NY, USA. NY: IEEE, 2002, pp. 157–160, doi: 10.1109/icip.2002.1039911.

[6] CHAO H.M., HSU C.M., MIAOU S.G. *A data-hiding technique with authentication, integration and confidentiality for electronic patient's records.* IEEE Transaction on Information Technology in Biomedicine.2002, 6(1), pp. 46–53, doi: 10.1109/4233.992161.

[7] CIET M., NEVEL M., PEETERSL E., QUISQUATER J.J. Parallel FPGA implementation of RSA with residue number systems. In: *Proceedings of the 46th IEEE International Midwest Symposium on Circuits and Systems*. IEEE, 2003, pp. 806–810, doi: 10.1109/mwscas.2003.1562409.

[8] COATRIEUX G., SANKUR B., MAITRE H. Strict integrity control of biomedical images. In: *Proceedings of Security and Watermarking of Multimedia Contents III,* San Jose, CA. CA: SPIE, 2001, pp. 229–240, doi: 10.1117/12.435403.

[9] FRIDRICH J., GOLIJAN M., DU R. Invertible authentication watermark for JPEG Images. In: *Proceedings of Security and Watermarking of Multimedia Contents III*, San Jose, CA, USA. CA: SPIE, 2001, pp. 197–208, doi: 10.1109/isspit.2010.5711776.

[10] FRIDRICH J., GOLIJAN M., DU R. *Lossless data embedding-new paradigm in digital watermarking*. EURASIP Journal on Applied Signal Processing. 2002, (1), pp. 185–196, doi: 10.1155/s1110865702000537.

[11] GUO X., ZHUANG T. A lossless watermarking scheme for enhancing security of medical data in PACS. In: *Medical Imaging, International Society for Optics and Photonics,* San Diego, CA, USA. CA: SPIE, 2003, pp. 350–359, doi: 10.1117/12.480450.

[12] JABERIPUR G., PARHAMI B., GHODSI M. A Class of Stored-Transfer Representations for Redundant Number Systems. In: *Conference Record of the Thirty-Fifth Asilomar Conference on Signals, Systems and Computers*, Pacific Grove, CA. Pacific Grove: IEEE, 2001, pp. 1304–1308, doi: 10.1109/acssc.2001.987701.

[13] KRISHNA H., LIN K.Y., SUN J.D. *A Coding Theory Approach to Error Control in Redundant Residue Number Systems I: Theory and Single Error Correction.* IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing. 1992, 39(1), pp. 8–17, doi: 10.1109/82.204106.

[14] KUMAR C.V., NATARAJAN V., POONGUZHALI P. Secured Patient Information Transmission Using Reversible Watermarking and DNA Encryption for Medical Images. *Applied Mathematical Sciences*, 2015, 9(48), pp. 2381–2391, doi: 10.12988/ams.2015.53219.

[15] MOSTAFA S.A., EL-SHEIMY N., TOLBA A.S., ABDELKADER F.M., ELHINDY H. M. *Wavelet packets-based blind watermarking for medical image management.* The open biomedical engineering journal. 2010, 4, pages. 93, doi: 10.2174/1874120701004010093.

[16] NASEEM M.T., QURESHI I.M., CHEEMA T.A., RAHMAN A. *Hash based medical image authentication and recovery using residue number system and chaos.* Journal of Basic and Applied Scientific Research. 2012, 3(6), pp. 488-495, Available from: http://www.textroad.com.

[17] 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. 2012, 10(2), pp. 10643–10651, Available from: http://www.textroad.com.

[18] RAMIREZ J., GARCIA A., MEYER-BAESE U., LLORIS A. Fast RNS FPL-Based Communications Receiver Design and Implementation. In: *Proceedings of 12th International Conference on Field and Programmable Logic*, Montpellier, France. Springer, 2002, pp. 472–481, doi: 10.1007/3-540-46117-5_50.

[19] SODERSTRAND M.A., JENKINS W.K., JULLIEN G.A., TAYLOR F.J. Residue number system arithmetic: modern applications in digital signal processing. In: *IEEE Press*, New York. IEEE, 1986.

[20] SUN J.D., KRISHNA H. *A coding theory approach to error control in redundant residue number systems— Part II: Multiple error detection and correction.* IEEE Transactions on Circuits and Systems II, Analog Digit. Signal Processing. 1992, 39(1), pp. 18–34, doi: 10.1109/82.204107.

[21] SZABO S.N., TANAKA R.I. *Residue Arithmetic and its Applications to Computer Technology* [online]. McGraw-Hill, New York, 1967.

[22] TIAN J. High capacity reversible data embedding and content authentication. In: *IEEE International Conference on Acoustics, Speech and Signal Processing,* Tualatin, OR, USA. Tualatin: IEEE, 2003, pp. 517–520, doi: 10.1109/icassp.2003.1199525.

[23] TRICHILI H., BOUHLEL M., DERBEL N., KAMOUN L. A new medical image watermarking scheme for a better tele diagnosis. In: *IEEE International Conference on Systems, Man and Cybernetics,* Tunisia: IEEE, 2002, pp. 557–560, doi: 10.1109/icsmc.2002.1168035.

[24] VOYATZIS G., PITAS I. Chaotic mixing of digital images and applications to watermarking. In: *Proceedings of European conference on Multimedia applications, services and techniques,* Belgium, European. Belgium: 1996, pp. 687–695.

[25] WAKATANI A. Digital watermarking for ROI medical images by using compressed signature image. In: *Proceedings of the IEEE 35th Annual Hawaii International Conference on System Sciences,* Washington DC, USA. Washington DC: IEEE, 2002, pp. 2043–2048, doi: 10.1109/hicss.2002.994129.

[26] WANG W., SWAMY M.N.S., AHMAD M.O. RNS Application for Digital Image Processing. In: *Proceedings of the 4th IEEE International Workshop on System-on- Chip for Real-Time Applications,* IEEE, 2004, pp. 77–80.

[27] WATSON R.W., HASTINGS C.W. Self-checked computation using residue arithmetic. In: Proceedings of the IEEE, 1966, pp. 1920–1931, doi: 10.1109/proc.1966.5275.

[28] WU S., TAN Z. *Multiresolution watermarking scheme based on chaotic sequences.* JOURNAL-XIAN JIAOTONG UNIVERSITY. 2000, 34(6), pp. 35–39.

[29] YANG L.L., HANZO L. *Redundant residue number system-based error correction codes.* In: Vehicular technology conference, Atlantic City, NJ. IEEE, 2001, pp. 1472–1476, doi: 10.1109/vtc.2001.956442.

[30] ZHOU X.Q., HUANG H.K., LOU S.L. *Authenticity and integrity of digital mammography images.* IEEE Transactions on Medical Imaging. 2001, 20(8), pp. 784–791, doi: 10.1109/42.938246.

[31] RAHMAN A., NASEEM M.T., MUZAFFAR M.Z. *Reversible and Robust Watermarking using Residue Number System and Product Codes.* Journal of Information Assurance and Security, 2012, 7, pp. 156–163.

[32] RAHMAN A. *Optimum Information Embedding in Digital Watermarking.* Journal of Intelligent and Fuzzy Systems, 2019, 37(1), pp. 553–564.

[33] RAHMAN A., QURESHI I.M., MALIK A.N., NASEEM M.T. *Dynamic Resource allocation for OFDM Systems using DE and Fuzzy Rule Base System.* Journal of Intelligent & Fuzzy Systems, 2014, 26(4), pp. 2035–2046.

[34] RAHMAN A. *GRBF-NN based ambient aware realtime adaptive communication in DVB-S2.* Journal of Ambient Intelligence and Humanized Computing 2020, (12), pp. 1–11, 2020.

[35] RAHMAN A., DASH S., LUHANCH A.K. *Dynamic MODCOD and Power Allocation in DVB-S2: A Hybrid Intelligent Approach.* Telecommunication Systems, 2020.

[36] RAHMAN A., AZAM M., ZAMAN G. *Performance Comparison of Product Codes and Cubic Product Codes using FRBS for Robust Watermarking.* International Journal of Computer Information Systems and Industrial Management Applications, 8(1), pp. 57–66, 2016.

[37] RAHMAN A., SULTAN K., ALDHAFFERI N., ALQAHTANI A., MAHMUD M. *Reversible and Fragile Watermarking for Medical Images.* Computational and Mathematical Methods in Medicine, June 2018.

[38] RAHMAN A., SULTAN K., ALDHAFFERI N., ALQAHTANI A., ABDULLAH D., MAHMUD M. *Robust and Fragile Watermarking for Medical Images: A Joint Venture of Coding and Chaos Theories. Journal of Healthcare Engineering*, June 2018.