International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
Volume No.3 Issue No.8, pp : 1036-1042 1 Aug 2014

A Novel Approach for Transmitting Secret Data Based on Chaotic Map and Spread Spectrum Watermarking in Frequency Domain

Maryam Abbasi, Saeed Shaerbaf Tabrizi, Payman Goli
Department of Electrical engineering, The Khavaran Institute of Higher Education, Mashhad, Iran
Email : m.abbasi304@yahoo.com

Abstract: ***Given the ever-increasing applications of the Internet and the growing volume of exchanged information, preserving the security and authentication transmitted images (that may have business, military, or even medical applications) are also gaining importance by the day. In this paper, we have proposed a robust watermarking algorithm for the protection and authentication of medical images in which the capabilities of chaotic maps have been utilized. The scheme obtains the feature vectors of the host image using discrete wavelet transform (DWT) and discrete cosine transform (DCT). The watermark image is encrypted by modified logistic map, and the initial conditions of the chaotic map used are embedded as a key in the frequency coefficients of the original image in the form of a spread spectrum to increase the security of the algorithm. Simulation results show that the proposed method has high security and robustness against image processing.***

Keywords: watermarking, chaotic map, encryption, discrete wavelet transform, discrete cosine transform

I. Introduction

With the rapid development and use of the Internet and multimedia, the digitalization process of medical systems has increased and digitized medical information helps in its storage and transmission. However, when these medical images are transmitted in public networks [1], the patient's personal information may be easily attacked and changed [2]. Therefore, the security of medical systems must be enhanced. The digital watermarking technology embeds the patient's personal information as watermarks into the medical images [3]. In these techniques, high robustness and security guarantee in the correct extraction of watermarks even after an attack has occurred. Watermarking techniques are focused on spatial domain or frequency domain [4]. Spatial domain techniques embed information in the intensity of the original image pixels directly. While frequency domain based algorithms embed sensitive information in the host image by modulating coefficient in a frequency domain, such as the Discrete Wavelet Transform (DWT) [5], Discrete Cosine Transform (DCT) [6], Discrete Fourier Transform (DFT) [7], Singular Value Decomposition (SVD) [8], or a combination of them [9, 10]. In some algorithms, the process of selecting regions of non-interest (RONI) is emphasized [11, 12] because the regions of interest (ROI) are the sensitive regions of medical images which are used in making accurate diagnoses. Although watermarking techniques has been developed well, we may not be able to use them for medical images because these images are important basis for doctors and for diagnosing the disease. The method proposed in this paper can be used for cases where a high peak signal to noise ratio (PSNR) and a complete retrieval of watermarking information are required; and depending on the type of the image, it can be used for military and judicial purposes.

One of the methods of increasing security is the watermark encryption before they are embedded [6, 7, 9]. In this article too, modified logistic map encrypts the watermark before it is sent.

The combined use of the feature vector of the medical image and the watermark encryption by utilizing the modified logistic map, together with watermarking of initial conditions in the image, have caused enhanced the security of the proposed algorithm.

Results of simulation show that the proposed algorithm also resists well against various attacks. The rest of the article is organized as follows. In section II the requirements of the proposed method will be reviewed, and the proposed method is described in section III. Finally, the simulation results and the conclusions are presented in sections IV and V, respectively.

II. The requirements of the proposed method

2.1 Discrete wavelet transform: The discrete wavelet transform (DWT) is a suitable transform for providing multiresolution image descriptions. Using this transform, the image is decomposed into an approximation having a lower resolution (LL) and three subbands containing the horizontal, vertical, and diagonal details (HL, LH, HH respectively) (Figure 1). The approximation subband is more robustness against attacks compared to the other three subbands. It is possible to obtain higher levels of details by reapplying the discrete wavelet transform to each of these subbands.

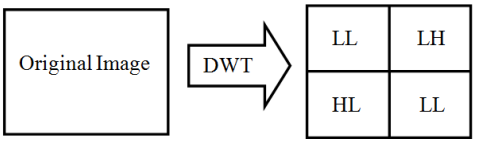


Figure 1. Subbands obtained by applying one level of the discrete wavelet transform to an image

2.2 The discrete cosine transform: The discrete cosine transform (DCT) represents the image as the sum of a number of cosine functions with different amplitudes and frequencies. This transform is used in the compression standards of the Joint Photographic Experts Group (JPEG) and new Moving Picture Experts Group (MPEG). The relation for calculating the two-dimension discrete cosine transform for an image with the dimensions of M×N is as follows:

$$B_{pq} = a_p a_q \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} A_{mn} \left(\cos \frac{\pi(2m+1)p}{2M} \cos \frac{\pi(2n+1)q}{2N} \right) \quad (1)$$

$$0 \le p \le M-1$$
$$0 \le q \le N-1$$

$$a_p = \begin{cases} 1/\sqrt{M}, & p = 0 \\ \sqrt{2/M}, & 1 \le p \le M-1 \end{cases}$$

$$a_q = \begin{cases} 1/\sqrt{N}, & q = 0 \\ \sqrt{2/N}, & 1 \le q \le N-1 \end{cases}$$

Where m, n is the spatial domain sampling and p, q is the frequency domain sampling.

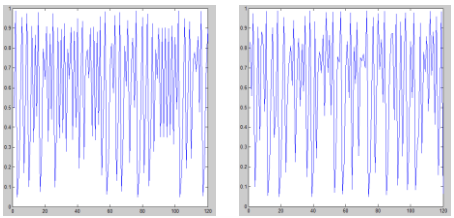
2.3 Logistic map: The definability of the chaotic system during its pseudo-random behaviour has caused this phenomenon to be of great interest in encrypting images because attackers see the system output as something random while for the intended receiver this output is definable and decipherable. In fact, chaotic maps have many applications in providing suitable security in encryption and watermarking systems given their seeming randomness and great sensitivity to initial conditions [13].

The simple logistic map is one-dimensional and non-linear and is defined in relation 2.

$$X_{n+1} = rX_n(1 - X_n) \qquad n=1,2,3,\ldots \qquad (2)$$

In this map, the initial values x_0 and r are used as control parameters. In this formula, x_0 takes on a value in the [0,1]. Research on chaotic dynamical systems has shown that the logistic map will be in the chaotic state when $3.5699456 \le r \le 4$. The sequence produced in logistic map is non-periodic and non-convergent too [14, 15].

In modified logistic map that is used in this paper, the values of STEP and S are added to the initial conditions. These values respectively represent the number of chaotic elements produced at each stage and the value in question to be added to the last member of the chaotic map of the previous stage and to be used as the x_0 of the new stage. These two values are finally hidden as a key in the DWT-DCT of the host image in the form of a spread spectrum. In this section, besides using the simplicity of the logistic map, we have increased the space of the key and, hence, have introduced greater security in the use of this map, by adding two other control parameters (S, STEP). Figure 2 shows the chaotic state of the sequence resulting from the logistic map and from the modified logistic map and the differences between the two. The correlation coefficient of these two sequences is – 0.04.



(a) **(b)**

Figure 2. (a) The chaotic sequence resulting from logistic map for the initial conditions of x_0=0.5, r = 3.95 (b) The chaotic sequence resulting from modified logistic map for the initial conditions of x_0=0.5, r = 3.95, S = 0.2 and STEP=9

III. The proposed method

In research [9], the KEY matrix resulting from chaotic encryption of the watermark and also the initial conditions of the chaotic map used are sent together with the medical image. In this article, we propose a very secure method for sending the watermark. Firstly the watermark image is multiplied into feature vector of the host image using DWT-DCT, then is encrypted using modified logistic map, finally is sent as a string of numbers and letters that is obtained by the chaotic sequence of the indexed. The initial conditions of the modified logistic map are also embedded in the form of a spread spectrum, and with very high security, in the frequency coefficients of the original image.

This article achieves three higher levels of security and occupies less bandwidth because it uses the chaotic sequence of the modified logistic map, the initial conditions are hidden in the frequency coefficients of the medical image, and KEY matrix is sent as a string of numbers and letters.

3.1 Sending the watermark

The watermark embedding procedure is represented in figure 3. Colour block is sent to the receiver.

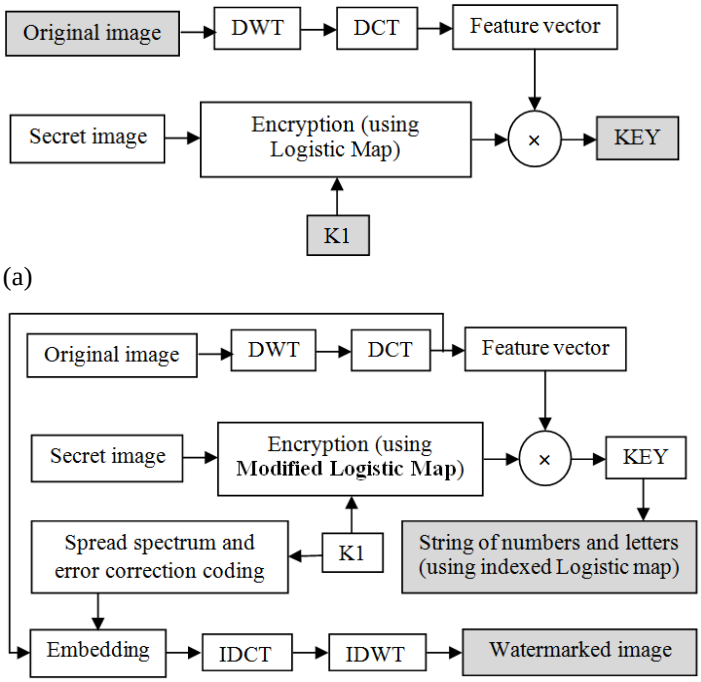


Figure 3. (a) watermark embedding in reference [9] (b) watermark embedding in proposed method

3.1.1 the watermark encryption algorithm

(1) Generate the chaotic sequence X (j) with the initial conditions of x_0 , r, S, and STEP by the modified logistic map that was explained in section 2.3.

(2) Transform the one-dimension sequence X (j) into the two-dimension matrix Y (i, j) in order match the two-dimension watermarking image.

(3)Transform the number sequence into "0" and "1" and obtaining C (i, j) as equation 3 (in this article, the threshold value of "th" is taken to be 0.5).

$$C(i,j) = \begin{cases} 1, & \text{if } Y(i,j) \ge th \\ 0, & \text{if } Y(i,j) < th \end{cases} \qquad (3)$$

(4) Obtain the encrypted watermark image by using equation 4.

$$EW(i,j) = W(i,j) \oplus C(i,j) \qquad (4)$$

In which W is the original watermark image, C the two-dimension chaotic matrix consisting of "0" and "1", and EW the encrypted image. On the receiver side, this relation is quite reversible because it includes the initial conditions of the modified logistic map. The correlation coefficient of the

original watermark image and the encrypted one seen in Figure 4 is – 0.1.

Figure 4. (a) the original watermark image (b) the encrypted watermark image

In blind watermarking methods, the watermarked image is sent with a key. In article [9] also, the KEY matrix and the initial conditions of the logistic map are sent to the receiver to be used as a key for extracting the watermark.

3.1.2 Extracting the feature vector of the host image

(1) Apply the DWT to the original image and obtain the four subbands of HH, LH, HL, and LL.
(2) Apply the DCT to the subband of approximation coefficients (LL).
(3) Apply the Zig-Zag transform to order the coefficients of the DCT for obtaining low, medium, and high frequencies.
(4) Select the M2 coefficient from among the low frequencies obtained in the previous stage to form the sign vector (M2 is the number of columns in the watermark image).
(5) Obtain the sign vector: if the selected low- frequency member is a positive coefficient or is zero, the number "1", and if it is a negative coefficient, the number "0" is represented in the sign vector. The obtained sign vector is robust against attacks such as noise rotation and changes in scale. This is shown in Table 1 for nine frequencies at the bottom of the 256 ×256 Lena image (coefficients are multiplied by 10^3).

As can be seen in the table1, their correlation coefficient is one; therefore, the sign vector obtained from the DWT-DCT coefficients can be used as a feature vector to scramble the watermark image. A summary of the steps of obtaining the sign vector is as follows in which N is the host image.

$$NA(i,j) = DWT2(N(i,j))$$
$$ND(i,j) = DCT2(NA(i,j))$$
$$Z(j) = zig-zag(ND(i,j))$$
$$V(j) = sign(Z(j))$$

The sign vector V(j) contains M2 members (M2 is the number of columns in the watermark image, and it is equal to 32 members in this paper). Using the encrypted image EW and the sign vector V, the KEY matrix is produced in the form of equation 5. This step can be considered as the second stage of the watermark encryption by the feature vector of the original image.

$$KEY(i,j) = EW(i,j) \oplus V(j) \quad (5)$$

In research [9], the KEY matrix must be sent to the receiver for the extraction of the watermark. In our paper, instead of sending the KEY matrix, an encrypted string is sent for the receiver and is meaningless for attackers. The encrypted string is produced as follows:

3.1.3 Production of an encrypted string in place of sending a KEY matrix using chaotic map

(1) Produce the n-member chaotic sequence by using logistic map (equation 2) with the initial conditions of x_0 and r and change it into a sequence containing zeros and ones, and with the threshold value of th= 0.5 (equation 3). In this paper, "n" is taken to be 10000 to spend little time and to obtain a shorter encrypted string.
(2) Index the chaotic sequence produced in stage one as is shown in Figure 5.

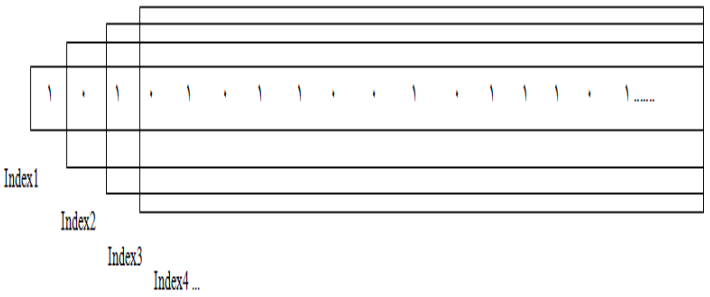


Figure 5. Indexing the chaotic sequence to obtain KEY matrix

(3) Compare the KEY matrix with all of the indices in stage three (when the first opposite bit is found between the KEY and the index, comparison with that index is finished. The number of the index is then placed in the "START" variable, and the bit number of the KEY in which the first error has taken place is put in the "First Error" variable).
(4) Store in cell array the maximum value of the First Error and the index number of the sequence (Start) for each part of the KEY.
(5) Consider four digits for the First Error and two for Start (if the number of obtained digits is fewer than six, a zero is put in place of them at the end. For example, if cell one is equal to 865598, it means that the maximum of the first error that has taken place compared to various indices from the beginning of the KEY has occurred in bit 98 and the index in question is 8655. If cell two is equal to 385890, it means that the maximum of the first error that has taken place compared to the various indices from bit 99 of the KEY has occurred in bit 89 and the index in question is 385).
(6) Change all of the cells of the obtained array to base-36 so that for each cell we have a string consisting of four numbers and letters (this is done to increase security and compress the sent string). Finally, a string of numbers and letters that have been obtained by the logistic map, and that have been indexed, is sent instead of KEY).

3.1.4 Placing the initial conditions of the modified logistic map in the host image

(1) Apply the DWT to the host image and obtaining the four frequency subbands of HH, LH, HL, and LL.
(2) Divide the approximate subband (LL) to 8*8 blocks and applying the DCT to each of the blocks.

(3) Apply the Zig-Zag transform to put in order the low, medium, and high frequencies.
(4) Select coefficients of the medium frequency from the block by using the mask shown in Figure 6.

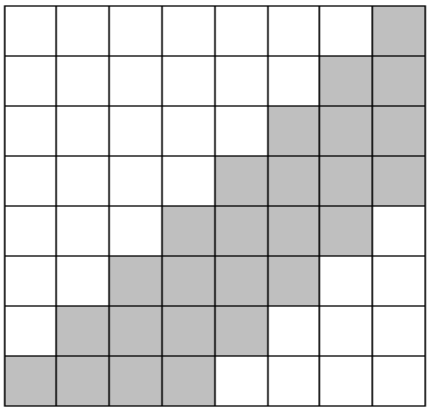


Figure 6. The mask of DCT coefficients for watermarking

(5) Form the reference matrix ECC in order to error correction (that includes 10 rows in each of which the last four bits are in the binary form of the numbers zero to nine and the other nine bits are used to correct errors).
(6) Form a binary sequence of the digits of the key (initial conditions of the logistic chaotic map) considering the ECC.
(7) Embed the resulting sequence in the medium frequencies of the DCT coefficients as shown in Figure 5 as follow:

$$x' = \begin{cases} x + a * p0, & \text{if } watermark\ bit = 0 \\ x + a * p1, & \text{if } watermark\ bit = 1 \end{cases} \quad (6)$$

In the equation above, "a" denotes the scale factor to control the strength of the inserted watermark (in this article, "a" is taken to be 10), x is the value of DCT of the masked coefficients, and x' the value of the resulting DCT that replaces the previous value.
The idea of spread spectrum watermarking for digital images requires the addition of pseudo-random signals to it. In this article, we have used the two totally uncorrelated signals P1 and P0 consisting of 1 and -1 and known by the sender and the receiver.
(8) Apply inverse DCT to each block.
(9) Apply inverse DWT to obtain the original image in which the initial conditions has been embedded.

3.2 Retrieving the watermark

3.2.1 Retrieving the KEY from the encrypted string

(1) Separate the string into 4-element segments and change from base-36 to base-10.
(2) Retrieve the "First Error" and the "Start" from numbers obtained in the previous stage.
(3) Produce an n- number of chaotic sequences by using logistic map (equation 2) with the initial conditions of x_0 and r and transforming it into a sequence containing "0" and "1" with the threshold value of th =0.5(equation 3).
(4) Index the chaotic sequence produced the same way the sender does.
(5) Put side by side the chaotic sequences having the Start index and the length of the First Error.
(6) Obtain the KEY matrix.

3.2.2 Extracting the initial conditions

(1) Apply the DWT to the host image and obtain the four subbands HH, LH, HL, and LL.
(2) Divide the approximate subband (LL) into 8*8 blocks and apply the DCT to each block.
(3)Apply the Zig-Zag transform for putting in order the low, medium, and high frequencies.
(4) Select medium frequency coefficients from among the block using the mask shown in Figure 6.
(5) Calculate the correlation coefficient of the stage 4 frequencies with P1 and P2: if the correlation coefficient with P1 is greater than the correlation coefficient with P0, the extracted bit will be "1," otherwise it will be "zero" .
(6) Obtain the initial conditions of the modified logistic map using the reference matrix ECC.
(7) Obtain the chaotic sequence X'(j) using the initial conditions.
(8) Transform the one-dimension sequence X'(j) into the two-dimension matrix Y'(i,j).
(9) Transform the number sequence into "0" and "1" and obtain Y'(i,j) in the form of the following equation:

$$C'(i,j) = \begin{cases} 1, & \text{if } Y'(i,j) \geq th \\ 0, & \text{if } Y'(i,j) < th \end{cases} \quad (7)$$

3.2.3 Producing the feature vector

(1) Apply the DWT to the original image and obtain the four frequency subbands HH, LH, HL, and LL.
(2) Apply the DCT to the LL subband.
(3) Apply the Zig-Zag transform to put in order the elements of the DCT for obtain the low, medium, and high frequencies.
(4) Form the sign vector like the stage of embedding (V'(i,j)).
(5) Extract the encrypted watermark using equation 8.

$$EW'(i,j) = KEY(i,j) \oplus V'(j) \quad (8)$$

(6) Decrypt the obtained watermark using relation 9.

$$W'(i,j) = EW'(i,j) \oplus C'(i,j) \quad (9)$$

IV. Results of simulations

The first objective in [9] is to obtain a high peak signal to noise ratio (PSNR) so that the medical image does not change. A high PSNR can also be obtained through our proposed method. The second objective in this paper is to obtain a high Normalized Correlation (NC) for the watermark image, which can be achieved through sending KEY to the receiver. In our article too, the KEY is retrieved in the receiver; but the security is higher and less bandwidth is occupied. The third objective is encrypting the watermark to increase security. In this paper modified logistic map is used instead of logistic map, and watermarking of the initial conditions of the modified logistic map is employed as a key in the medical image, to further increase security.
Results of simulations in the proposed method on grey image "medical_ MRI_ Head" with the dimensions of 256×256 as the host image, and "HN" with the dimensions of 32*32 as the secret image, are presented in Figure 6. The selected initial conditions of the modified logistic map for encrypting the watermark are x_0=0.5 , r= 3.95, S=0.2, and STEP=9; and after being inserted in the host image, they are also retrieved in the receiver.

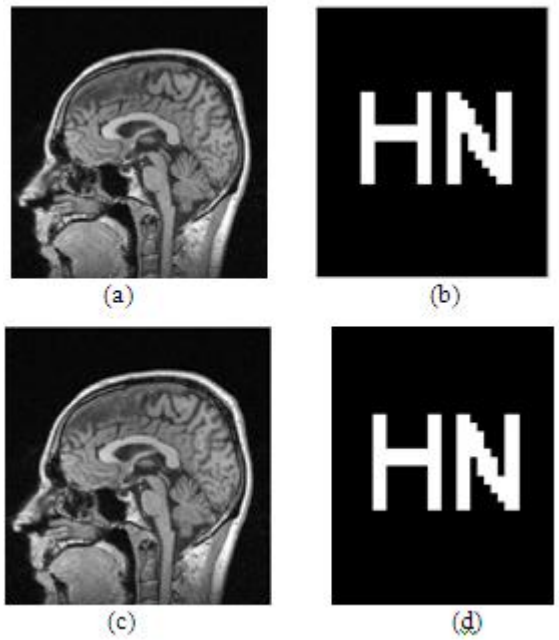


Figure 7: (a) the original host image, (b) the original secret image, (c) the watermarked image, (d) the extracted secret image

All sequences produced by the modified logistic map are very sensitive to initial conditions. That is, any two sequences produced under different initial conditions are not statistically correlated. For example, just by changing the value of the STEP variable (STEP=10), the extracted watermark will be completely scrambled and will appear as shown in Figure 8.

Figure 8: Result of using the wrong key in retrieving the watermark

The evaluation criteria are reviewed below.

4.1 Transparency: secret information must be embedded in the host signal in such a way that the signal is not so distorted as to attract the attention of the viewer. Given the characteristics of human visual system, if changes made in the host signal are up to a certain extent, the human eye cannot notice these changes. The PSNR is used as a criterion for determining the Transparency and measuring the quality of the watermarked image, which can calculated in decibels as follows (MSE is the mean- square error):

$$\mathrm{PSNR\,(dB)} = 10\log10\left(\frac{255^2}{\mathrm{MSE}}\right) \qquad (10)$$

$$\mathrm{MSE} = \frac{1}{N_1 * N_2} \sum_{i=1}^{H_{length}} \sum_{j=1}^{H_{width}} (N(i,j) - N'(i,j))^2 \qquad (11)$$

In the above relation, N is the host image, N' the watermarked image, and N1 and N2 the length and the height of the host image, respectively. As can be seen, in our article the PSNR is high (PSNR=45.13) and acceptable.

4.2 Robustness: The capability of a watermarking algorithm in extracting embedded information after attacks on the medium containing the secret information represents the robustness of the algorithm. The quantitative estimation for calculating the quality of the extracted watermark W'(i,j) with reference to the original watermark W(i, j) can be expressed with the help of the normal correlation (NC). NC can be calculated as follows:

$$\mathrm{NC} = \frac{\sum_{i=1}^{W_{length}} \sum_{j=1}^{W_{width}} (W(i,j) - W'(i,j))}{\sqrt{\sum_{i=1}^{W_{length}} \sum_{j=1}^{W_{width}} (W(i,j))^2} \sqrt{\sum_{i=1}^{W_{length}} \sum_{j=1}^{W_{width}} (W'(i,j))^2}} \qquad (12)$$

The table below shows the high efficiency of the proposed method and its robustness against attacks (rotation, change of scale, adding noise, etc

4.3 Security: In the proposed algorithm, security is improved by:

- using the modified logistic map
- sending initial conditions of the modified logistic map in the form of a spread spectrum and watermarked in the image
- sending an encrypted string instead of KEY matrix

V. Conclusion

In reference [9], KEY matrix (which results from multiplication by the feature vector of the image and from encryption by the logistic map) and the initial conditions of the chaotic map used are sent together with the medical image. In this article, a very secure method is proposed for encryption and sending the watermark. The watermark image, after being multiplied by the feature vector of the host image (a vector that is obtained using DWT-DCT), is encrypted using modified logistic map. It is then sent as a string of numbers and letters obtained by the chaotic sequence of the indexed logistic map. The initial conditions of the chaotic sequence used are also embedded as a spread spectrum, and with high security, in the frequency coefficients of the original image. The present paper yields three more stages of security and occupies less bandwidth because it uses the modified logistic map, it encrypts the initial conditions in the frequency coefficients of the host medical image, and it sends KEY in the form of a string of numbers and letters. Results of simulations show that the algorithm also exhibits good robustness against attacks.

References

i. S. Kaur, O. Farooq, R. Singhal and B. S. Ahuja, "Digital watermarking of ECG data for secur wireless communication,"IEEE International Conference on Recent Trends in Information, Telecommunication and Computing, pp. 140-144, March 2010.

ii. K. A Navas and M. Sasikumar, "Survey of Medical Imag Watermarking Algorithms," In Proceedings of the 4th Sciences of Electronic, Technologies of Information and Telecommunications International Conference, Tunisia, pp. 25-29, March 2007.

iii. C. Nagaraju, S.S. ParthaSarathy, "Quality Measure for Information Hiding in Medical Images," International

Journal of Computer Applications (0975 – 8887) Vol. 65, No.11,pp. 11-14, March 2013.

iv. Y. X. Zhou, W. Jin, "A novel image zero-watermarking scheme based on DWT-SVD,"IEEE International Conference on Multimedia Technology, pp. 2873- 2876, Dec. 2009.

v. R. Mavudila, Lh. Masmoudi, M.Cherkaoui, M. Hamri and N.Hassanain,"Medical image watermarking based on M-band Wavelet Transform," International Journal of Modern Engineering Research (IJMER, Vol.2, No.4, pp. 2711-2718, 2012.

vi. C. Dong, Jingbing Li, M. Huang and Y. Bai," The Medical Image Watermarking Algorithm with Encryption by DCT and Logistic," Web Information Systems and Applications Conference (WISA), pp. 119 – 124, Nov. 2012.

vii. J. Li, Y. Chen, " The Medical Image Watermarking Algorithm Based on DFT and Logistic Map,"IEEE International Conference on Computing and Convergence Technology,Vol. 7, pp. 1- 6, Dec. 2012.

viii. R. Elizabeth Philip, Sumithra M.G," SVD based Watermarking Method for Medical Image Security," International Journal of Computer Applications (0975 – 8887) Vol. 66, No.2,pp. 29-33,March 2013.

ix. Y. Liu, J. Li,"The medical image watermarking algorithm using DWT-DCT and logistic," IEEE International Conference on Computing and Convergence Technology (ICCCT),Vol. 7, pp. 599 – 603, Dec.2012.

x. L. P. Feng, L. B. Zheng, P. Cao ,"A DWT-DCT based blind watermarking algorithm for copyright protection," IEEE International Conference Computer Science and Information Technology (ICCSIT),Vol. 3, pp. 455 – 458, July 2010.

xi. M.K. Kundu, S, Das, "Lossless ROI Medical Image Watermarking Technique with Enhanced Security and High Payload Embedding," IEEE International Conference on Pattern Recognition (ICPR), Vol. 20 ,pp. 1457 – 1460, Aug. 2010.

xii. B. L. Gunjal, S. N. Mali," ROI Based EmbeddedWatermarking of Medical Images for Secured Communication in Telemedicine," World Academy of Science, Engineering and Technology,pp. 815-820, 2012.

xiii. Y. Dai, X. Wang,"Medical Image Encryption Based on a Composition of Logistic Maps and Chebyshev Maps", Proceeding of the IEEE International Conference on Information and Automation ,pp.210-214, June 2012.

xiv. R. Enayatifar, F. Mahmoudi, K. Mirzaei,"Using the Chaotic Map in Imagesteganography", IEEE International Conference on Information Management and Engineering, Vol. 9, pp. 491-495, April 2009.

xv. W. Yue, N. JosephP,"Image Steganography Scheme using Chaos and Fractals with the Wavelet Transform",International Journal of Innovation, Management and Technology, Vol. 3, No. 3,pp.285-289, June 2012.

Table 1. robustness of the sign vector against attacks

	V (1)	V (2)	V (3)	V (4)	V (5)	V (6)	V (7)	V (8)	V (9)	sign vector	NC
Original image	-5.21	3.54	-0.10	3.89	-1.21	4.94	-3.24	1.55	-0.85	10101010	1
Gaussian noise 2%	-5.14	3.54	-0.16	3.77	-1.16	4.83	-3.20	1.61	-0.85	10101010	1
Salt & pepper noise	-4.96	3.43	-0.06	3.78	-1.18	4.79	-3.17	1.49	-0.81	10101010	1
imadjust	-7.43	5.05	-0.16	5.59	-1.75	7.06	-4.65	2.25	-1.22	10101010	1
Median filter 3*3	-5.25	3.58	-0.09	3.93	-1.22	4.99	-3.26	1.56	-0.87	10101010	1
Scaling(×0.5)	-2.60	1.77	-0.05	1.94	-0.60	2.47	-1.62	0.77	-0.42	10101010	1
Scaling(×3)	-1.56	1.06	-0.03	1.16	-0.36	1.48	-0.97	0.46	-0.25	10101010	1
Rotation 0.2	-4.86	3.63	-1.13	3.76	-2.20	5.03	-3.20	1.62	-0.72	10101010	1

Table 2: The robustness of the proposed method against attacks

Type of attack	NC (of the proposed method)	NC (of reference [9])	Number of errors eliminated by error correction	Retrieved initial conditions
Gaussian noise 2%	0.8885	1	4	STEP=9 و S=0.2 ، =r 3.95 ، X_0=0.5
Salt & pepper noise	1	1	4	STEP=9 و S=0.2 ، =r 3.95 ، X_0=0.5
imadjust	1	1	0	STEP=9 و S=0.2 ، =r 3.95 ، X_0=0.5
Median filter 3*3	1	1	3	STEP=9 و S=0.2 ، =r 3.95 ، X_0=0.5
Scaling(×0.5)	1	1	0	STEP=9 و S=0.2 ، =r 3.95 ، X_0=0.5
Scaling(×3)	1	1	0	STEP=9 و S=0.2 ، =r 3.95 ، X_0=0.5
Rotation 0.2	0.8029	1	4	STEP=9 و S=0.2 ، =r 3.95 ، X_0=0.5
crop	0.3426	1	5	STEP=9 و S=0.2 ، =r 3.95 ، X_0=0.5