VOL. 13, NO. 9, MAY 2018 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

AN IMPROVED CHAOTIC RADIAL BASIS RESONANCE THEORETIC NEURAL NETWORK INTEGRATED WITH GENETIC ALGORITHM FOR ENHANCING SECURITY IN IMAGE TRANSMISSION

Hayfaa Abdulzahra Atee
Institute of Administration/ Al-Rusaffa, Middle Technical University, Baghdad, Iraq
E-Mail: haifaa_atee@yahoo.com

ABSTRACT

Recent spread out of personal digital assistants (PDA) and mobile phones demanded fast plus highly secured digital transactions. Meanwhile, rapid technological advancement has allowed the transmission of the wealth of multimedia information from one device to another, especially in the field of medical, banking, defense, education, etc. to cite a few. The image file in the multimedia data often contains sensitive and confidential information, where the security and privacy need to utmost preservation without being accessed by the unauthorized users or adversaries. To overcome such security issues, we proposed an improved genetic algorithm integrated chaotic radial basis with resonance theoretic neural network (GA-CRB-RTNN) to generate the key sequences for encrypting the gray and color images before transmission. The network was further optimized via genetic algorithm (GA) that analyzed each image pixels by selecting various rows and columns. In this approach, mutation and crossover operations were used to generate the chaotic key sequence for successful encryption of the host images and subsequent generation of the cipher image. This scheme was shown to reduce the expectant attacks and enhanced the security appreciably while making the multimedia data transfer. Furthermore, the efficiency of the encryption process in the context of the medical and normal images was evaluated in terms of the mean square error rate (MSER), the correlation (vertical and horizontal), the structural similarity (SSIM) index, and the histogram.

Keywords: digital transactions, security, encryption, genetic algorithm, chaotic radial basis, resonance theoretic neural network.

1. INTRODUCTION

In recent times, the exponential growth of diverse digital communication technologies and cloud services lead to the innovation in digital transactions, where vast amount of personal data, confidential information and sensitive documents can easily be managed (storing and retrieving at faster rate) securely [1]. During the transaction, the digital system undertakes several security measures [2] via the authentication mechanism such as e-signatures certification to maintain the personal details. It is this security that convinces the public to trust on the digital transaction, especially for medical reports, bank payments, defense operation, etc. Amongst different types of electronic digital data transmission [3], medical reports transaction have been playing a vital role because in each year about $8 billion of such operations are performed (CAQH Index report, 2015).

The digital transactions of medical reports [4] is not only economic but also time saving. The senior manager of Reynard Washington acknowledged that the digital transaction based medical report contains several information related to care details, wherein its standard format can be used to save the labor cost while analyzing a particular patient [5]. Over the years, many cryptographic methods have been developed such as symmetric and asymmetric which are freely available when transmitting the electronic report in the cloud [6]. Despite several dedicated efforts an improved scheme for highly secured digital data transmission has not been achieved yet. So far, to protect the digital data from intermediate attackers the security remains one of the major issues [7]. Certainly, the unauthorized access can create numerous setbacks involving data reputation, patient life data theft, information alteration, loss of prestige and fame of company or individual, etc. Thus, the main objective of this paper in to introduce an accurate method for secure digital transaction of medical images [5].

In the past, intensive researches have been performed to achieve enhanced security measures related to digital transaction. Homomorphic cryptographic algorithm based electronic health record transformation protocol has been developed [8], where the medical image was encrypted pixel by pixel before being transmitted into the cloud. This process allowed to improve the image data confidentiality as well as maintained the security during transaction. A novel tailored visual cryptography encryption process [9] was introduced for avoiding the intermediate access of data during transmission. This encryption system followed four steps such as split, covert, pixel analysis and merging, which in turn assisted to compress the image without affecting its quality. After generating the encrypted image, decimal conversion process was applied for getting the original image with improved confidentiality, integrity and availability of the medical image. The performance of the system was evaluated using JPEG image to examine the security based transaction.

The crypto-compression approach based digital medical image transaction was introduced for maintaining the confidential data [10]. This crypto-system contained a chaotic map that utilized the DCT and encryption process while analyzing each image pixel. This process attained effective results, which were evaluated in terms of

sensitivity and statistical measures. Using tamper localization scheme, the confidentiality, integrity, availability and authenticity of the image transaction was improved [11]. This scheme used the symmetric encryption function and the hash code for generating the encrypted medical image. Additionally, elliptic curve, digital signature and whirlpool hash function were employed to analyze the integrity of the medical image during the digital transaction. The system also utilized the watermarking process to examine the image pixel in terms of least significant bit (LSB). Many divisions of the entire image into different blocks could enhance the security level, because it was difficult for the unauthorized user to find exact blocks. The system performance was evaluated by conducting experiments.

To attain the high level security and extreme confidentiality during medical images while transaction, diverse cryptographic algorithms were proposed. It is realized that managing the secret information in medical images is difficult from the threat of intermediate attacks and unauthorized access. Driven by this need, we proposed an improved genetic algorithm integrated chaotic radial basis with resonance theoretic neural network (GA-CRB-RTNN) for managing the security issues involving the digital image transaction. In this approach, the neural network was combined with the genetic algorithm [12] to minimize the error rate while generating the key sequence for image to be transacted. The efficiency of the encryption scheme was analyzed for both the medical and the normal images. The performance evaluations were made in terms of the mean-square error rate (MSER), correlation (vertical, horizontal), structural similarity (SSIM) index, and histogram. This paper is organized as follows. Section 2 depicts the improved GA-CRB-RTNN based secure medial image transaction. Section 3 analyzes the performance efficiency of the developed system. Section 4 concludes the paper.

2. IMPROVED GA-CRB-RTNN BASED SECURED IMAGE TRANSACTION

Generally, a transacted image encloses several confidential and sensitive information [4]. Particularly, medical images that contain rich information must be hidden from the illegal access via utmost security measures. Thus, original images must be altered into other unreadable format so that it becomes incomprehensible to the access of intermediate users. To provide the security into the transmitted images, chaos theory was used, which was comprised of nonlinear dynamical [5] concept and conditions. These conditions allowed the generation of a particular sequence called chaotic sequence that was further used to attain an effective encrypted and decrypted image along with the improved RTNN. The same chaotic NN that was used to the sender and the receiver for encryption and decryption process in turn led to secured image transmission with integrity and authenticity [13].

In the encryption-decryption scheme, a set of initial parameters were chosen to generate the chaotic sequences. Let r(n) be the digital signal of length L and one-byte value of the signal is ranged from 0 to (L-1). After making the initial arrangements, control unit U value was determined together with the initial point, i(0) of the (1-T) logistic map. From the defined parameters, the generated chaotic sequence can be written as i(1),i(2),……i(L) by $i(n+1) = \mu(n)(1 - x(n))$. Based on the chaotic sequence, binary representation b(O) of the sequence can be generated as $b(1), \ldots . b(8l-1)$ from i(1),i(2),……i(L). Then, the generated binary representation of image can be denoted as, $b(8l-8)b(8l-7) \ldots . b(8l-2)\, b(8l-1)$ According to the initial chaotic conditions, the digital signal value of the control sequence can be estimated as:

$$r(n) = \sum_{j=0}^{7} t_i * 2^j \quad (1)$$

$$w_{ij} = f(x) = \begin{cases} 1 \; if \; j = 1 \; and \; b(8 * n * i) = 0 \\ -1 \; if \; j = i \; and \; b(8 * n * i) = 0 \\ ij \neq i \end{cases} \quad (2)$$

$$\theta_j = \begin{cases} -\frac{1}{2} \; if \; b(8 * n + j) = 0 \\ \frac{1}{2} \; if \; b(8 * n + j) = 1 \end{cases} \quad (3)$$

for$j = 1$ to 7 one obtains:

$$t_i' = f\left(\sum_{j=0}^{7} w_{ji} * t_j + \theta_j\right) \quad (4)$$

Using the above chaotic sequence and logistic control map value, the following digital signal can be generated:

$$r(n) = \sum_{j=0}^{7} d_j * 2^j \quad (5)$$

The generated signal was considered as the encrypted value. During the encryption process, the network was trained by RB-RTNN [12] to achieve the effective chaotic sequence, which in turn reduced the efficiency of the unauthorized access while transmitting the images. The NN was trained the generated chaotic sequence using the comparison field, recognition field, vigilance parameter and reset module. The generated sequence was taken as input in the comparison field that checked the observer expectation in the recognition field, which was performed via the network weights value matching process. During the training process, the network simultaneously utilized the radial basis as the activation function which performed well even if the generated sequence varied according to the image pixel values. The activation function can be defined as:

$$\boldsymbol{y(X)} = \sum_{\boldsymbol{i=1}}^{\boldsymbol{N}} \boldsymbol{\omega_i \varphi(\|x - x_i\|)} \quad (6)$$

where $\boldsymbol{y(X)}$ is the closest trained output of the chaotic sequence, $\boldsymbol{N}$is the number of sequence, $\boldsymbol{\omega_i}$is theweight of each data,$\boldsymbol{x}$ is the input data and $\boldsymbol{x_i}$ is the center of the dataset.

The trained output value was transmitted to the reset module that compared the calculated data with the

observer data sequence expectation along with the vigilance parameter [14]. When the calculated data satisfied the observer expectation, it could predict the value in the recognition field. Otherwise, the process was repeated until it could predict the exact trained value. The weight connection of each layer can be defined as:

$$\Delta_p \boldsymbol{w_{jk}} = \boldsymbol{\delta_k^p y_j^p} \quad (7)$$

Based on the weight value, the output can be generated via the expression:

$$\delta_a^p = \left(d_a^p - y_a^p\right) F'\left(\delta_a^p\right) \quad (8)$$

During the output estimation process, in case any error value occurred in the network the radial basis activation function (6) was applied to minimize the network error rate. Next, the weighted update rule can be applied to the network via:

$$\Delta_p w_{jk} = \gamma \delta_k^p y_j^p \quad (9)$$

This process was repeated until the entire generated chaotic sequence was trained via the RBNNs. Using the obtained logistic map sequence can be written as $i(n+1) = \mu(n)\left(1 - i(n)\right)$ and $i\,(j) = mu * i(j-1) * (1 - x(j-1)$. The RRTNNweights based chaotic sequence and the output weight logic was defined as: $if(bc, i = 0)$and $i = j$, the weight value was 1; $if(bc, i = 1)$and $i = j$, then the weight value was -1; and $if\ i \neq j$ the weight value was 0.

Based on the weight value, the output can be estimated as:

$$output = sum\left(weight * I_{ij}\right) + \Theta \quad (10)$$

According to the output of the generated sequence, the input image was encrypted using the GA [15]. Being one of the optimized algorithms, GA was used to find the approximate solutions from the collection of problem space. During the searching process, the network utilized the selection, the crossover and the mutation operator together with the fitness value to attain the effective results. First, the height and the width of the image input image that needed to be transmitted in the network was obtained. From the obtained image values, the module operation was performed as H mod 8 and W mod 8. When the estimated value was equal to 0 then the image was divided into different blocks each of dimension (8 × 8). When the module value was not 0, then the operations such as H=H+(8-(H mod 8)) and W=W+(8-(W mod 8)) were performed and the image was divided into different blocks [13, 16]. After dividing the blocks, crossover operation was performed by randomly selecting two strings (vertical and horizontal) from the block. The location was identified together with these strings, wherein the portions [16] of the string was swapped to get the encrypted image. During the crossover operation, secret key was obtained from the above NN generated chaotic sequence. The mutation operator was applied to each pixel presented in image via the operation:

$$V_i[black] = 255 - V_i[black] \quad (11)$$

Using this process, the encrypted image was generated corresponding to the information of each block. This process was repeated continually to obtain the excellent encrypted image before being transmitted in the network successfully. In the receiver side, the reverse operation was performed for decrypting the image using the mutation and the crossover operator together with the generated chaotic key sequences. Finally, the system performance was evaluated via experiments as discussed underneath.

3. PERFORMANCE ANALYSIS

The performance evaluation of the proposed system was evaluated in terms of MSER, vertical and horizontal correlation, MSER, SSIM index and histogram based security metrics. A set of medical and normal images those are effective for information transmission process were used. Entire coding was performed using MATLAB [17] programming software. The MSER metric is the simplest and the most widely used measure for the full-reference image quality [18]. It determines the average of the square error which is defined as the difference between the error by pixel value of the original image from the transacted encrypted-decrypted image. This metric is frequently used in signal processing and can be defined as:

$$MSE = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} \left(f(i,j) - f'(i,j)\right)^2 \quad (12)$$

where $f(i,j)$ is the original image, $f'(i,j)$ is the decrypted image after achieving the transferred image with security, M and N are respectively the image height and the width.

The error rate of the proposed GA integrated CRB-RTNN system (GA-CRB-RTNN) was compared with the existing art-of-the techniques including the chaotic cryptosystem (CC), NN based cryptosystem (NNC) and CNN based cryptosystem (CNNC) as depicted in Figure-1. It is evident that the error rate could improve the overall correlation in both horizontal and vertical direction.

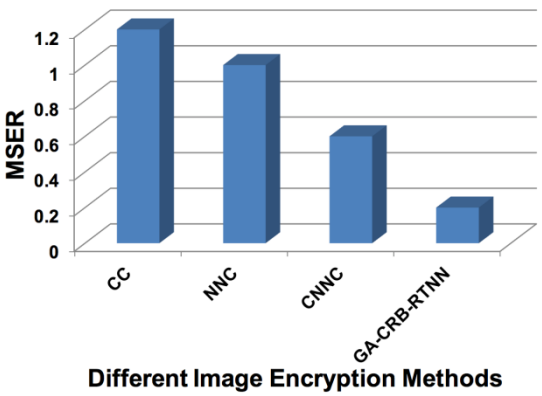

Figure-1. Comparison of the MSER of the proposed system with the existing techniques.

The normalized correlation (NC)thatmeasures the similarity between the original image ($f(i,j)$) and decrypted image ($f^{'}(i,j)$) was calculated using the expression:

$$NC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(f(i,j)f^{'}(i,j)\right)^2}{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(f[i,j]\right)^2} \quad (13)$$

where M and N are respectively the image height and the width. The proposed GA-CRB-RTNN system error rate was compared with the some of the existing systems such as CC, NNC and CNNC as illustrated in Figure-2.

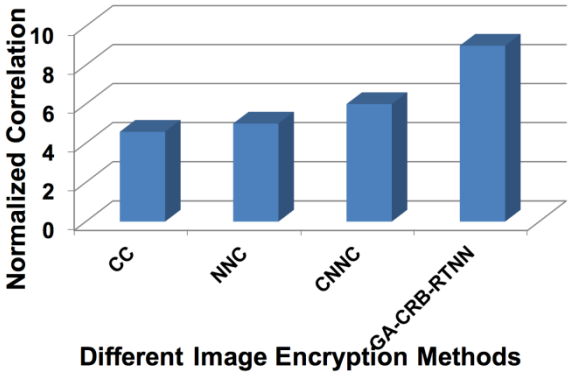

Figure-2. Comparison of theNC of the proposed system with the existing techniques.

Figure-3 compares the SSIM of the proposed system with the existing art-of-the techniques. In fact, the achievement of strong NC between the transmitted and the received image allowed us to improve the overall structural similarity during the image transaction.

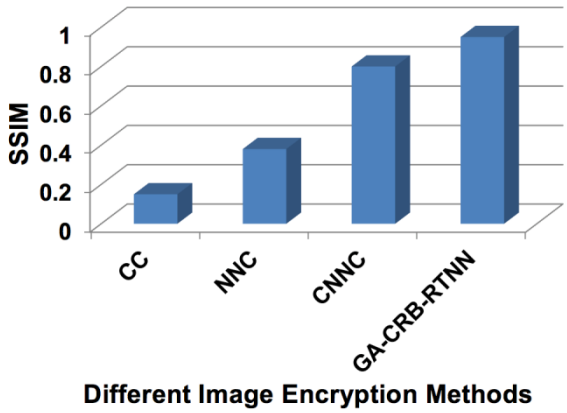

Figure-3. Comparison of theSSIM of the proposed system with the existing techniques.

Figure-4 displays the estimated histogram image, indicating clear distribution of the image pixels according to the pixel color intensity value. In fact, the histogram of the image pixels was found to be distributed among the number of pixels at each intensity level in an effective manner. In short, the proposed GA-CRB-RTNN could effectively maintain the security, integrity, authentication and availability of the images with effectiveness.

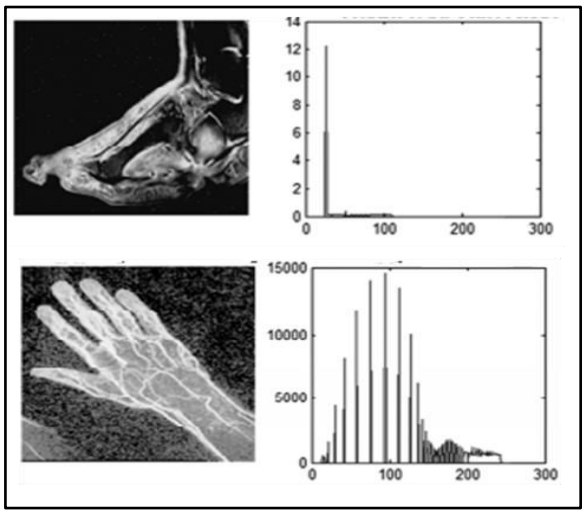

Figure-4. Histogram distribution of the proposed GA-CRB-RTNN system.

CONCLUSIONS

The paper proposed an improved GA-CRB-RTNN system for secured image transaction. Using the input image, a chaotic key sequence was generated via different layer of the NNs. The weights of the network were constantly updated along with the learning rule during the key generation process, which could avoid the error value in the generated keys. Using the chaotic key, the GA was applied to encrypt the image. The selection, mutation and crossover operators were utilized. The proposed algorithm decomposed the images into (8 × 8) block with respect to the height and the weight value. Each pixel was mutated to obtain the encrypted image by means of the key sequence; thereby it ensured the successful

authentication. The performance of the proposed system was evaluated using MATLAB simulation, wherein the medical and the normal images were examined. The achievement of high the high correlation and similarity together with low MSER value suggested that the proposed GA-CRB-RTNN system is advantageous for secured image transaction in the Internet network.

REFERENCES

[1] L. O. M. Kobayashi, S. S. Furuie, and P. S. L. M. Barreto. 2009. Providing Integrity and Authenticity in DICOM Images: A Novel Approach.in IEEE Transaction on Information Technology in Biomedicine. pp. 582-589.

[2] H. Yang and A. C. Kot. 2006. Binary Image Authentication with Tampering Localization by Embedding Cryptographic Signature and Block Identifier. IEEE Signal Processing Letters. 13: 741-744.

[3] G. Coatrieux, C. L. Guillou, J.-M. Cauvin and C. Roux. 2009. Reversible Watermarking for Knowledge Digest Embedding and Reliability Control in Medical Images. IEEE Transaction on Information Technology in Biomedicine. Vol. 13.

[4] X.-Y. Wang, L. Yang, R. Liu, and A. Kadir. 2010. A chaotic image encryption algorithm based on perceptron model. Published online: 22 June 2010, pp. 615-621.

[5] S. Bhowmik and S. Acharyya. 2011. Image Cryptography: The Genetic Algorithm Approach.in International Conference of Computer Science and Automation Engineering (CSAE).pp. 223-227.

[6] S. N. Kumar. 2015. Review on Network Security and Cryptography. International Transaction of Electrical and Computer Engineers System. 3: 1-11.

[7] A. Patle and N. Gupta. 2016. Vulnerabilities, attack effect and different security scheme in WSN: A survey.in International Conference on ICT in Business Industry & Government (ICTBIG).

[8] A. M. Vengadapurvaja, G. Nisha, R. Aarthy and N. Sasikaladevi. 2017. An Efficient Homomorphic Medical Image Encryption Algorithm for Cloud Storage Security. In: 7th International Conference on Advances in Computing & Communications, ICACC, Cochin, India. pp. 643-650.

[9] S. Manimurugan and C. Narmatha. 2015. Secure and Efficient Medical Image Transmission by New Tailored Visual Cryptography Scheme with LS Compressions. International Journal of Digital Crime and Forensics (IJDCF). 7: 26-50.

[10] M. Dridi, B. Bouallegue and A. Mtibaa. 2014. Crypto-compression of medical image based on DCT and chaotic system. Computer & Information Technology in IEEE. pp. 1-6.

[11] K. S. Aparna, R. Sreejith and T. A. Amma. 2016. An Advanced Crypto Based Security System for Medical Image/Data Transfer. International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET). 5: 10835-10840.

[12] Y.-F. Dong, J.-H. Gu, Na-Nali, X.-D. Hou and W.-L. Y. I. 2007. Combination of Genetic Algorithm and Ant Colony Algorithm for Distribution Network Planing. in Proceedings of the Sixth International Conference on Machine Learning and Cybernetics, Hong Kong.pp. 999-102.

[13] G. A. Sathishkumar, K. B. bagan and N. Sriraam. 2011. Image Encryption Based on Diffusion and Multiple Chaotic Maps. International Journal of Network Security & Its Applications (IJNSA). 3: 181-194.

[14] A. Kumar. 2008. A Novel Genetic Algorithm approach to solve Map Colour Problem.in International Conference of Emerging Trends in Engineering and Technology (ICETET).pp. 288-291.

[15] C. Gondro and B. P. Kinghorn. 2007. A simple genetic algorithm for multiple sequence alignment. Genetics and Molecular Research. 6: 964-982.

[16] A. Yayik and Y. Kutlu. 2014. Neural network based cryptography. Neural Network World. 24: 177.

[17] H. s. Uysal and S. Kurt. 2012. Automatic Decryption of Images through Artificial Neural Networks. Trends in Innovative Computing - Intelligent Systems Design.pp. 187-191.

[18] C. S. Varnan, A. Jagan, J. Kaur, D. Jyoti and Dr. D. S. Rao. 2011. Image Quality Assessment Techniques pn Spatial Domain. International Journal of Computer Science and Technology. 2: 177-184.