Provable Chaotically Authenticated Encrypted Biomedical Image Using OFDM Transmission

B. M. El-den
Department of Electronics and Communication Engineering, Faculty of Engineering, Delta University for Science& Technology, International Coastal Road, Gamasah City, Mansoura, Dakhliya, Egypt, Deltauniv.edu.eg
Email: Basant_moheyelden@yahoo.com

Abstract

In this research, a unique multiband random chaotic key generator based provable authenticated encrypted technique for biomedical picture for the healthcare biomedical system, which can be used in *5G* communication system is presented. In addition, the encryption method employed in this research is based on Multiband Random Chaotic Key Generator, and the proposed provable authenticated methodology is based on symmetric authenticated encryption data (*MBRCKG*). In the proposed proven Orthogonal Frequency Division Multiplexing (*OFDM*) communication system, the Authenticated Chaotic Encrypted Biomedical Image (*ACE-BI*) is utilized. This study uses discrete wavelet transformation (*DWT*) and discrete cosine transformation (*DCT*) to mask patient data and hospital watermarks in biological images. With various statistical and *OFDM* settings, channel analysis and statistical analysis have been examined for their effects on the collected hospital logo and patient data. The simulation studies demonstrate how resistant to communication signal processing the proposed *ACE-BI* method is. Additionally, the proposed algorithm is able to reduce encryption time to one quarter because the partial encryption based in one level *DWT* scheme.

Keywords: MBRCKG; SAEPD; biomedical image Encryption; Authentication; OFDM transmission

1. Introduction

In recent decades, the modern healthcare environment has increasingly evolved through digital information systems. Information is being digitized in many fields, such as broadcasting, medical storage systems and patient data, banking, and shopping. The digitization of clinical data empowers the capacity and transmission of clinical data through correspondence channels.

Normally utilized recurrence space changes incorporate the Discrete Cosine Transform (*DCT*), Discrete Wavelet Transform (*DWT*), and Discrete Fourier Transform (*DFT*). Nonetheless, *DWT* is all the more broadly utilized in watermarking computerized pictures because of its phenomenal spatial direction and multi-goal properties like the hypothetical model of the human visual framework. Consolidating *DWT* and *DCT* can additionally work on the exhibition of *DWT*-based computerized picture watermarking calculations. Applying two changes depends on the way that the joined change can make up for the weaknesses of the other, bringing about a successful watermark.

Due to its superior spatial and frequency energy compression features, the wavelet transform has become a crucial tool in watermarking and image processing. At each *DWT* level, the biomedical image can be decomposed into four sub-bands. A low-resolution approximation component (*CA*) and three other spatial direction components corresponding to horizontal (*CH*), vertical (*CV*), and diagonal (*CD*) detail components. The *CA* sub-bands are obtained by low-pass filtering both horizontally and vertically. Contains an approximate description of the image. The *CH* sub-bands are obtained by applying high-pass filters both horizontally and vertically. It contains high frequency components along the

Doi : https://doi.org/10.54216/FPA.090201
Received: May 10, 2022 Accepted: October 22, 2022

diagonal. The *CV* and *CD* sub-bands are obtained by low-pass filtering in one direction and high-pass filtering in the other direction.

Find edges and texture patterns in each image by using high-resolution sub-bands. *DWT*-based watermarking technology enables superior spatial localization and provides multi-resolution properties consistent with the human visual system (*HVS*). Resemble wireless digital communications is growing rapidly, requiring reliable and spectrally efficient wireless systems. Orthogonal Frequency Division Multiplexing (*OFDM*) is suitable for most of today's wireless communication systems due to its high immunity to multipath signals and high spectral efficiency.

Due to its ability to provide low-complexity equalization for highly dispersed channels, *OFDM* is becoming more widely used in contemporary broadband wireless systems. In situations with flat fading, additive white Gaussian noise (*AWGN*), and frequency selective fading, *OFDM* is a useful high-speed transmission method. Currently, it serves as the industry standard for Wireless Local Area Networks *(WLAN)*, European Digital Video Broadcasting (*DVB*-T), and Digital Audio Broadcasting (*DAB*) [1*]*. In summary, the main contributions in this paper are:

- Design of highly nonlinear multiband chaos maps for biomedical image encryption.
- Introduced a new image authentication proposal based on optical authentication cryptography.
- Analysis of multi-carrier health communication systems for different channel effects.
- A study of the effectiveness of statistical analysis in biomedical image archiving applications.

2. Multiband Chaotic Random Key Generator (MBCRKG)

In [3], the author introduced a new broad parameter setting, the main concept of cryptographic key parameters. The authors not only prove that a wide range of parameter adjustments is a uniformly distributed variant density function. Thanks to his one-dimensional chaos map featured in [4]. Floating point iteration is used to satisfy a wide range of control parameters. This section, described the chaos map which introduced in [5] and prove it to be long-range. In addition to introducing the novel concept of a chaotic multiband generator. Mathematically, the system is simply defined as:

$$x_{n+1} = rx_n(1 - sin\pi x_n) mod 1 \quad \ldots\ldots(1)$$

The old logistic map is quite identical to the new logistic chaos map as defined below, with the exception that the linear function is substituted with the transcendental sine function. As a result, the suggested new system is naturally more nonlinear and, as predicted, exhibits complex and desirable chaotic behavior over a considerably wider range of system parameters. Applications for effective, economical, and more secure data encryption benefit from the growing complexity of dynamic chaotic behavior of systems and the expanding range of system parameters across which complex chaotic behavior occurs.

Mathematical calculations can be used to establish the maximum and lowest values of the new system that is being proposed without using the modulo operation for each given value of r. Since $x_{n+1} = rx_n(1 - sin\pi x_n)$ the derivative becomes $dx_{n+1}/dx_n = r(1 - sinx_n - x_n \cos x_n)$ then, by letting the derivative be zero $r(1 - sinx_n - x_n \cos x_n) = 0$ the x_n values in the range become 0.5596843072 and π/2 corresponding to a maximum value of x_{max}= 0.26254712771 r and a minimum value of $xmin$ = 0.

Additionally, modulo arithmetic was developed to potentially eliminate these periodic windows in order to significantly increase security when used to address such issues with picture encryption. Modulo arithmetic can be viewed as discontinuities and time-varying nonlinearities, the most potent nonlinear physical phenomena you might come across in practice, from a system dynamics perspective. We may anticipate that the addition of such additional nonlinear mechanisms will result in enhanced chaotic features. For applications involving picture scrambling, this is beneficial. The definition of modulo-1 arithmetic is utilized (eq.1). This is due to the fact that each time it wraps the data to the appropriate range [0, 1].

The bifurcation map and Lyapunov exponents of the completely new system due to the very large range of system parameters (r = 0 – 1016), characteristically pronounced dynamic behavior was observed in regions different from this case. The bifurcation map is displayed in interval format to better show the key performance of the system.

3. The proposed Authenticated Encrypted and Watermarked Biomedical Image (AEWBI)

In this section, a *DWT-DCT* watermarking scheme based on a proposed biomedical encryption and watermarking system is presented. This method can be divided into stages. First by describing the patient's biomedical X-ray image. This image can be encrypted by a chaotic multiband map (embedding method), but the second stage consists of a

Doi : https://doi.org/10.54216/FPA.090201
Received: May 10, 2022 Accepted: October 22, 2022

watermark embedding method. Encrypted biomedical images with watermarks can be transmitted over *OFDM*. An overview of these methods can be seen in Fig. 1.
DWT is a partial transform with multi-scale analytical capabilities. By using *DWT*, the original image is divided into four sub-band images. Low frequency portion and three high frequency parts (*HL*, *LH* labelled, and *HH*, detail sub-image) (*LL*, approximated and labelled sub-image). While the approximation sub-image represents the intensity convergence of the source pictures, the detail sub-image contains the streak information. Since the majority of the picture energy is concentrated here, relative and detail sub-images are much more stable. As a result, we embed the watermark in about sub-images for increased robustness.

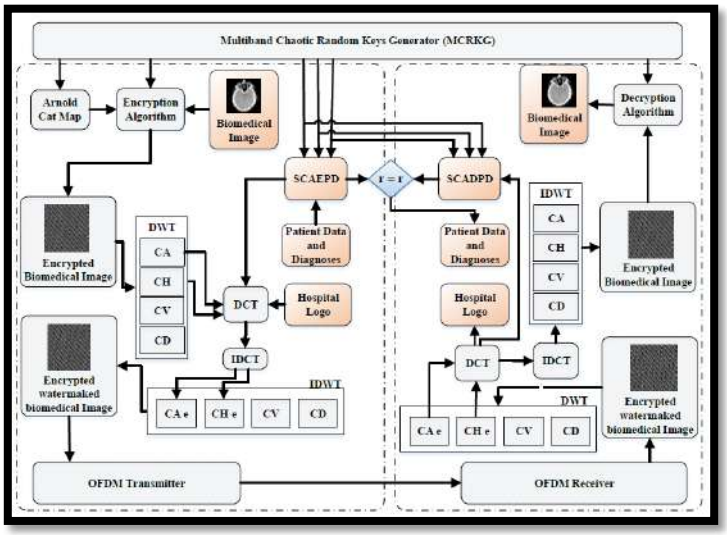


Figure 1: the (AEWBI) block diagram of the Proposed System

A. Biomedical Image Encryption

The suggested image scrambling demonstrates the memristor's chaotic behavior and makes use of it in the confusion and diffusion steps to jumble the image in the manner described below.

Step 1. Confusion process

A phase in the scrambling process is where the positions of the pixels are changed without the values being altered.
As confusion techniques for image scrubbing, Arnold [6], Hilbert curve [7], and Rubik's cube pixel transformation [8] can be employed. Find the two hidden parameters (a,b) of the Arnold Cat Map (ACM) by summing the final 100 floating-point values of the first two output states (x and y) of the memristor element. The two decimal values a,b of a dynamic parameter in an Arnold cat map that disguises the sum as [9] can be found using the method given below.

$$a = \sum_{1}^{100} x.10^{6} mod\ 64 \quad \text{.....(2)}$$

$$b = \sum_{1}^{100} y.10^{6} mod\ 128 \quad \text{.....(3)}$$

$$\begin{bmatrix} X_{m+1} \\ Y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} X_m \\ Y_n \end{bmatrix} mod 256 \quad \text{.....(4)}$$

Where Xm, Yn represent the original image old positions of the pixels. Xm+1, Yn+1 are the new positions of the pixels in the encrypted image. To boost security, cryptography needs a diffusion mechanism.

Step 2. Diffusion process

The scrambled image's pixel values are all altered by the diffusion process, therefore we may use memristor diffusion based on the last two output states, z and w, of the memristor element:

- Chose the last $M \times N$ floating point values of the z and w states and add z and w as:

Doi : https://doi.org/10.54216/FPA.090201
Received: May 10, 2022 Accepted: October 22, 2022

$q = (z + w)$ 1……………………………………………………………………………………………...……….(5)

- Convert the $M \times N$ q-values into a decimal value in the range of [1, 256] as:

$Q = (q * 10^{16})$ 256……………………………………………………………………………………...….(6)

- The exclusive-OR (XOR) operation, which involves bit-by-bit XORing each pixel of the original image with the scrambled image, is the foundation of the diffusion process.

With the same secret keys, the decryption method is the opposite of the encryption phases, and the inverse Arnold cat map is as follows [10]:

$$\begin{bmatrix} X_m \\ Y_n \end{bmatrix} = \begin{bmatrix} a*b+1 & -a \\ -b & 1 \end{bmatrix} \begin{bmatrix} X_{m+1} \\ Y_{n+1} \end{bmatrix} mod256 \quad (7)$$

B. Biomedical Authenticated Watermarking Scheme

As is known, the approximated subimages are smooth and have very little texture. Dividing it into smaller blocks he applies the *DCT* directly, and most of the *DCT* coefficients, except *DC*, are too small to be used for watermark embedding. Here the Arnold transform [11] is first applied to the approximate sub-image block or watermark image. A noisy version of z is generated for the first time for the approximated subimage block, yielding more significant coefficients of z than those generated in the transformed domain. For watermark security, the watermark appears a second time in the image. To achieve invisibility, watermarking algorithms frequently use JND to restrict the shifting range of DCT coefficients. Significant and balanced AC coefficients in the DCT transform domain are necessary for the combination of JND models. As a result, prior to the DCT conversion, each block is zigzag scanned and arranged in decreasing order.

Let $I=\{Ii,J ,i ,j=1,2,\ldots,N\}$ represent the host image, and $W=\{Wi,J ,i ,j=1,2,\ldots,M\}$ represent the binary with the size $M \times M$. The summarized of the new blind watermark scheme can be as follows.

B.1 Watermark-Embedding

- Convert the binary watermark image W to W_1 using the Arnold transform. W_1 is scanned online and converted to a one-dimensional sequence W' $W'=\{Wi',i=1,2,\ldots\ldots,M \times M ,Wi'=0 \text{ or } 1\}$
- Transform the host image I using a one-level *DWT* transform and obtain the decomposed approximate subimage L as the embedding region. L is then permuted using the Arnold transform and split into non-overlapping 8×8 blocks $B = \{Bi\}$
- Scan each block B_k (where k stands for k_{th} block) into a *1-D* sequence Z using zigzag. Then the sequence Z is sorted in descending order and the corresponding position matrix P is saved. So the inverse zigzag creates a new matrix $B_{k'}$.
- Convert each new block (Bk') to the DCT coefficient matrix (Dk). The information about the hospital logo is embedded using the coefficients Dk (5,2) and Dk(4,3). The following is the embedding formula:

$$\begin{cases} D_k(5,2) = \overline{D_k} + a*j \\ D_k(4,3) = \overline{D_k} + a*j \end{cases} \quad if\ W'_k = 0 \quad (8)$$

$$\begin{cases} D_k(5,2) = \overline{D_k} + a*j \\ D_k(4,3) = \overline{D_k} + a*j \end{cases} \quad if\ W'_k = 1 \quad (9)$$

Where $D_k = (D_k(5,2) + D_k(4,3)) / 2$.

The weighting factor a represents the strength factor and *J* represents the *JND* factor for the corresponding location calculated by Watson's model. See [12] for more information on *JND*.

- The watermarked DCT coefficient matrix is transformed using the inverse DCT to reconstruct each block, and the saved position matrix P is used to restore each pixel's location.
- Repetition of steps 3 through 5 is necessary to incorporate all watermark bits. The watermark information is then combined with these new blocks to create a fresh chaotic DWT approximation image, L`.
- • Apply the inverse DWT to L` and use the inverse Arnold transform. We've reached watermark image I^* now.

B.2 Extract Watermark

Doi : https://doi.org/10.54216/FPA.090201
Received: May 10, 2022 Accepted: October 22, 2022

The extraction procedure is fairly straightforward and may be carried out blindly using only the private key and the Arnold transform's n iterations. The following steps:

- Apply a one-step DWT to the watermarked image I^* to obtain the decomposed approximatively sub-image L^*.In L^*, the Arnold transform is applied using a private key.
- Divide L^* into 8×8 non-overlapping chunks, scan each one, and then sort as with embedding.
- Create the DCT coefficients for each block. The watermark bits are extracted from each block using its coefficients (5,2)and $D_i(4,3)$. The result is the one-dimensional sequence $B = \{B,\ i = 1, 2, \ldots, M\times M\}$. The following formula yields the value of Bi:

$$B_i = \begin{cases} 1, D_i(5,2) \geq D_i(4,3) \\ 0, D_i(5,2) < D_i(4,3) \end{cases} \quad (10)$$

B.3 Symmetric Authenticated Encryption Patient Data (SAEPD)

Bellare and Rogaway introduced AEP (Optimal Asymmetric Encryption Padding) in 1994 [13]. In the random oracle model, it was demonstrated that a public-key cryptosystem based on OAEP offers semantic security against adaptive chosen-ciphertext attacks [14]. Additionally, the technique can be efficiently computed and has a high message expansion rate.

The one-way trapdoor permutation f: $\{0,1\}^k \rightarrow \{0,1\}^K$ Is used in the proposed *OAEP* denoted as *f-OAEP*. When *f* being *RSA* function, the cryptosystem is denoted as *OAEP*. The following are descriptions of how *f-OAEP* is encrypted and decrypted.

MBRCKG of OAEP:

- Used *MBRCKG* to generate Key_0,$Key_1$for two cryptographic hash functions G,H where $k_0$and k_1 are two security parameters and the length is 1000 bit for Encryption and Decryption steps
- Used *MBRCKG* to generate authenticator value (r) where r is 861 bit.

Encryption of f-OAEP:

- OAEP is a one-way trapdoor permutation's domain-to-patient data space transformation and randomized message padding method that is simple to invert. which, G: $\{0,1\}k0\rightarrow$ $\{0,1\}n+k1$ and H: $\{0,1\}n+k1\rightarrow$ $\{0,1\}k0$., which should satisfy that $2-k0$ and $2-k1$are negligible quantities. For message recognition, a string of zeros is added as redundant data. The transformation process is shown in Fig. 2.

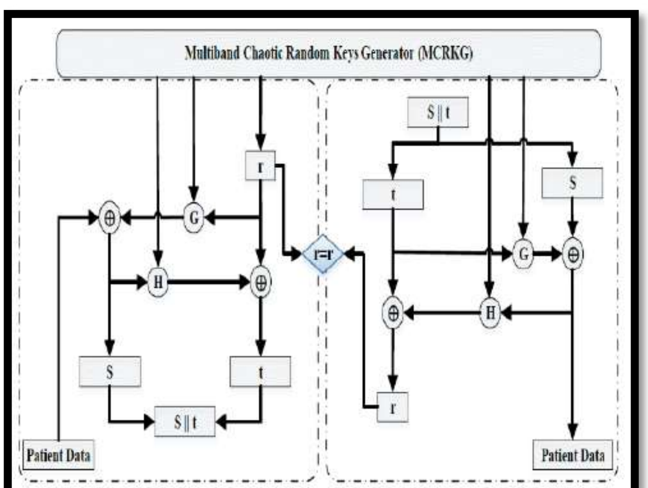


Figure 2: Block diagram Of the Multiband Chaotic Authenticated Encrypted Patient Data. The notation "||" represent the concatenation of two strings.

Doi : https://doi.org/10.54216/FPA.090201
Received: May 10, 2022 Accepted: October 22, 2022

Table1: Parameter values of the Biomedical Proposed System

	Parameter	Value
Sender	Size of biomedical image	512 x 512 pixel
	Size of Logo image	9 x 12 pixel
	Size of patient data	861 bits
MBRCKG	First Key hash length G_{k1}	10000 bits
	Second Key Hash Length H_{k2}	10000 bits
	Arnold parameter length (a)	8 bits
	Arnold parameter length (b)	8 bits
	Initial condition x_0	0.2893456
OFDM System	Modulation Technique	QPSK
	Modulation level	2
	symbol rate	250000
Channel	Noise environment	AWGN
Receiver	Channel estimation	Perfect

4. OFDM Biomedical Image Transmission

A biomedical encrypted and watermarked image is first staged in an OFDM baseband modulation system, then it is encoded and turned into complex data using digital modulation techniques [15-18]. The serial to parallel converter is then used, which is necessary for the inverse fast Fourier transform to function (IFFT). Using a parallel to serial converter, the resulting data is once more transformed into serial data. Before the data is transmitted into the AWGN channel, a cyclic prefix and guard interval are added to it in order to reinforce it in multipath fading environments and make sure that it has no ISI and ICI effect. Cyclic prefix is eliminated from the received signal on the receiver side before FFT, demodulation, and channel decoding are carried out as shown in Fig (3).

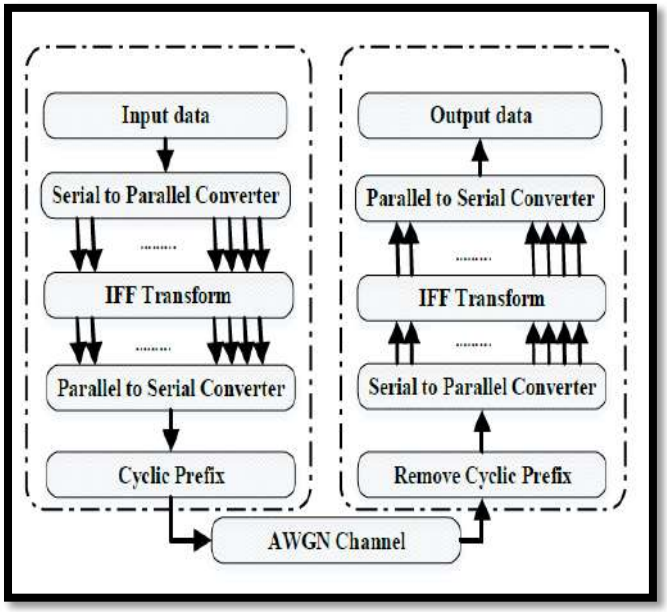


Figure 3: The Block diagram Of the OFDMA Transmission

Doi : https://doi.org/10.54216/FPA.090201
Received: May 10, 2022 Accepted: October 22, 2022

5. Results

This section provides a brand-new image encoding that takes use of the chaotic 4D memristor element behaviour. Traditional chaotic systems including logistic maps, Lorentz, and Chua circuits have recently become the subject of inquiry by several scientists. Recent research on the memristor element demonstrated that the element's chaotic behaviour can increase the resolution of chaotic calculations. Tables and Figures display the main block diagram of the proposed 4D MCIE as well as its top-secret specifications.

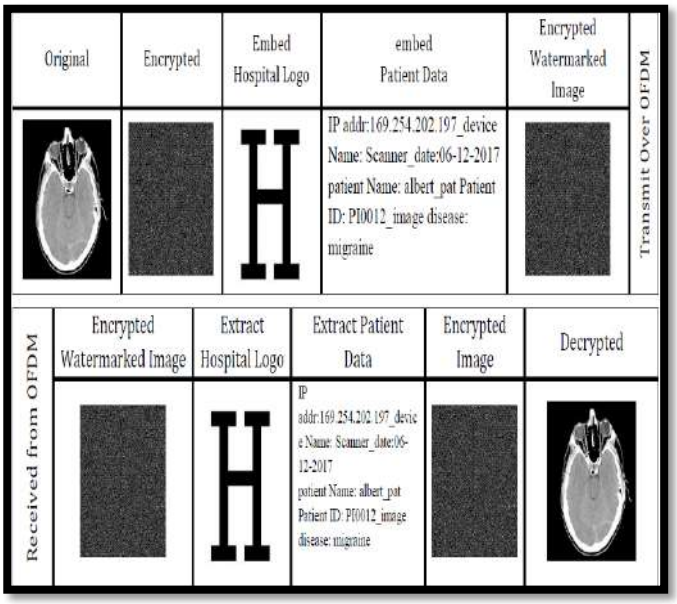


Figure.4: Simulation results of the proposed PAE biomedical image Tx, Rx at 7 dB

Table 2: Hospital Logo extracted from biomedical

No attacks	Parameters	Encrypted biomedical image	Hospital Logo	Patient Data	Decrypted Biomedical Image
System Test	Image			IP addr:169.254.202.197_device Name: Scanner_date:06-12-2017patient Name: albert_pat Patient ID: PI0012_image disease: migraine	
	BER / Error	--	0	0	0
	NCC	0.43158	1	1	1
	PSNR	5.88901	Inf	--	Inf
	UACI	33.34%			
	PNCR	99.89%			

Doi : https://doi.org/10.54216/FPA.090201
Received: May 10, 2022 Accepted: October 22, 2022

Table 3: Patient Data extracted from biomedical Image

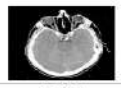
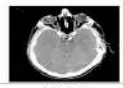
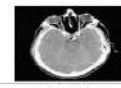
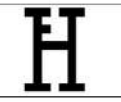
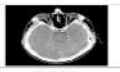
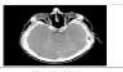
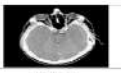
Attacks	Parameter	Intensity 0.002	Intensity 0.003	Intensity 0.004
Gaussian Noise	Patient Data	IPaddr:169.254.202.197_device Name: Scanner_date:06-12-2017patient Name: albert_pat Patient ID: PI0012_image disease: migraine	IPaddr:169.254.22.197_levice Name:Scanner_date206,12-2017patientNaM%albert_pat PatientID:PI0012_image diconicomigranno	IPaddr:169.254.202.197_devi % Name:Scanner_date:06 12)2013 patienu NaMe:albert^pat PtientAD:PI002 image dIrease:migraIoE
	Error	0	5	12
	Hospital Logo			
	PSNR Extracted Logo	65.454	62.444	62.444
	NCC	1	0.9737	0.9726
	BER	0	4	4
	Decrypted Image			
	PSNR	44.4541	43.4776	43.4871
Salt & Paper Noise	Patient Data	IPaddr:169.254.202.197_device Name: Scanner_date:06-12-2017patient Name: albert_pat Patient ID: PI0012_image disease: migraine	IPaddr:169.254.202.197^devi ce Naie:Scanner_date:06-12- 2017 patient NaMe:albert_pat PatientID:PI0012_image disease:migraine	IPaddr:1&9.254.202.197_devic e Ncme:Scanner_date:06-12-2017 patient NaMe:albert_pat PatientID:PI0012_image disease:migraine
	Error	0	2	3
	Hospital Logo			
	PSNR	Inf	65.454	68.465
Speckle Noise	Patient Data	IPaddr:169.254.202.197_device Name: Scanner_date:06-12-2017patient Name: albert_pat Patient ID: PI0012_image disease: migraine	IPaddr:169.254.202.197_device Name: Scanner_date:06-12-2017patient Name: albert_pat Patient ID: PI0012_image disease: migraine	IPaddr:169.254.202.197_device Name: Scanner_date:06-12-2017patient Name: albert_pat Patient ID: PI0012_image disease: migraine
	Error	0	0	0
	Hospital Logo			
	PSNR	60.465	Inf	Inf
	NCC	0.9930	1	1
	BER	1	0	0
	Decrypted Image			
	PSNR	52.5661	51.6122	40.3231

Table4: Gaussian filter Extracted logo hospital

Attacks	Parameter	Value Gaussian [3 3] (0.5)	Value Gaussian [5 5] (0.5)
Gaussian Filter	Extracted patient data	IPcdDr:169.254.202.197_deviae Name:Scanner_date:06-12-2017 patient NaMe:albert_pat PatientID:QI0012_image disease:migraine	IPcdDr:169.254.202.197_deviae Name:Scanner_date:06-12-2017 patient NaMe:albert_pat PatientID:QI0012_image disease:migraine
	Error	4	4
	Extracted logo hospital		
	PSNR	Inf	Inf
	BER	0	0
	NCC	1	1

Doi : https://doi.org/10.54216/FPA.090201
Received: May 10, 2022 Accepted: October 22, 2022

Table5: Gaussian filter Extracted logo hospital

Attacks	Parameter	Filter	
		Gaussian [3 3] (0.5)	Gaussian [5 5] (0.5)
Gaussian Filter	Extracted patient data	IPcdDr:169.254.202.197_deviae Name:Scanner_date:06-12-2017 patient NaMe:albert_pat PatientID:QI0012_image disease:migraine	IPcdDr:169.254.202.197_deviae Name:Scanner_date:06-12-2017 patient NaMe:albert_pat PatientID:QI0012_image disease:migraine
	Error	4	4
	Extracted logo hospital		
	PSNR	Inf	Inf
	BER	0	0
	NCC	1	1

Table6: Computed parameters of extracted hospital logo vs. channel SNR

SNR	Parameters			Extracted logo hospital	Extracted patient data	Error
	PSNR	BER	NCC			
1	55.912	18	0.880		IY itfr!6I9n: 7 p =LVA"]9EaygCB#1.~%_\ Tm#4-S'~8M!7"<idHA2wBiky:AbexU^eaB^u^w. A:Ri0jiGCGUtec++@UD-|igvlq>h	225
2	57.325	13	0.914		IP addr:169.254.2 2.197_levice Name:Scanner_date206,12-#4-S'~8M!7"<idHA2wBiky:AbexU^eaB^u^w. A:Ri0jiGCGUtec++@UD-|igvlq>h	125
3	63.693	3	0.980		IPadEr:169.:5$.202<196EDrice"ame:Scdnner_late:p6l122015 patent NqM%:cl^ert^patPiThendIH:PY012Wim^g disEasE:-igralne	46
4	65.454	2	0.987		IP adds:169n254. 0:.197_$evice(Name:Scanner_date:06-12-2017 patient Na e:Albert_pat PatientID:PI0012_image tIsease:migrahne	12
5	Inf	0	1.00		IP addr:169.254.202.197_device Name:Scanner_date:06-12-2017 patient NaMe:albert_pat PatigntID:PI0012_image disease:migraine	1
6	Inf	0	1.00		IP addr:1&9.254.202.197_device Ncme:Scanner_date:06-12-2017 patient NaMe:albert_pat PatientID:PI0012_image disease:migraine	0
7	Inf	0	1.00		IP addr:1&9.254.202.197_device Ncme:Scanner_date:06-12-2017 patient NaMe:albert_pat PatientID:PI0012_image disease:migraine	0

Doi : https://doi.org/10.54216/FPA.090201
Received: May 10, 2022 Accepted: October 22, 2022

6. Conclusion

In this search, a unique provable authenticated encrypted scheme for biomedical image based on multiband random chaotic key generator for the health care biomedical system, which can be used in *5G* communication system is introduced. The proposed provable authenticated scheme is based on symmetric authenticated encryption data; in addition, the encryption technique used in this paper is based on Multiband Random Chaotic Key Generator (*MBRCKG*). The proposed provable Authenticated Chaotic Encrypted Biomedical Image (*ACE-BI*) is used in (*OFDM*) communication system. This paper is based on (*DWT*) and (*DCT*) to hide both of hospital watermark and patient data in biomedical image. Statistical analysis, channel analysis has been studied for its *OFDM* effects on the extracted hospital logo and patient data with different statistical and *OFDM* parameters. The simulation studies show the proposed *ACE-BI* algorithm is robust against communication signal processing. In addition, the proposed algorithm is able to reduce encryption time to one quarter because we used partial encryption based in one level *DWT* scheme.

References

[1] amali, M., Samavi, S., Karimi, N., Soroushmehr, S. M. R., Ward, K., & Najarian, K. (2016). Robust watermarking in non- ROI of medical images based on DCT-DWT. 2016 38th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC). doi:10.1109/embc.2016.7590920
[2] Yu, Y., Lei, M., Xiaoming Liu, Zhiguo Qu, & Cheng Wang. (2016). Novel zero-watermarking scheme based on DWT-DCT. China Communications, 13(7), 122–126. doi:10.1109/cc.2016.7559084.
[3] Arya, R. K., Singh, S., & Saharan, R. (2015). A secure non-blind block based digital image watermarking technique using DWT and DCT. 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI). doi:10.1109/icacci.2015.7275917
[4] Al-Mansoori, S., & Kunhu, A. (2014). Hybrid DWT-DCT-Hash function based digital image watermarking for copyright protection and content authentication of DubaiSat-2 images. High-Performance Computing in Remote Sensing IV. doi:10.1117/12.2067254
[5] Mehto, A., & Mehra, N. (2016). Adaptive Lossless Medical Image Watermarking Algorithm Based on DCT & DWT. Procedia Computer Science, 78, 88–94. doi:10.1016/j.procs.2016.02.015.
[6] Zhang, Z., Wang, C., & Zhou, X. (2016). Image watermarking scheme based on Arnold transform and DWT-DCT-SVD. 2016 IEEE 13th International Conference on Signal Processing (ICSP). doi:10.1109/icsp.2016.7877942
[7] Benoraira, A., Benmahammed, K., & Boucenna, N. (2015). Blind image watermarking technique based on differential embedding in DWT and DCT domains. EURASIP Journal on Advances in Signal Processing, 2015(1). doi:10.1186/s13634- 015-0239-5
[8] Srilakshmi, P., Himabindu, C., & Suvarna. (2017). A novel approach of watermarking for multiple images with DWT- DCT. 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI). doi:10.1109/icpcsi.2017.8391971
[9] Zhu, H., Zhao, C., Zhang, X., & Yang, L. (2014). An image encryption scheme using generalized Arnold map and affine cipher. Optik - International Journal for Light and Electron Optics, 125(22), 6672–6677. doi:10.1016/j.ijleo.2014.06.149
[10] Abbas, N. A. (2016). Image encryption based on Independent Component Analysis and Arnold's Cat Map. Egyptian Informatics Journal, 17(1), 139–146. doi:10.1016/j.eij.2015.10.001
[11] Vaish, A., & Kumar, M. (2017). Color image encryption using MSVD, DWT and Arnold transform in fractional Fourier domain. Optik, 145, 273–283. doi:10.1016/j.ijleo.2017.07.041
[12] Zhu, H., Zhao, C., Zhang, X., & Yang, L. (2014). An image encryption scheme using generalized Arnold map and affine cipher. Optik - International Journal for Light and Electron Optics, 125(22), 6672–6677. doi:10.1016/j.ijleo.2014.06.149
[13] M. Bellare, P. Rogaway . "Optimal Asymmetric Encryption" Published in EUROCRYPT 9 May 1994 Computer Science, Mathematics. DOI:10.1007/BFb0053428.
[14] Bellare, M. and Rogaway, P. (1993) Random Oracles Are Practical: A Paradigm for Designing Efficient Protocols. In: Proceedings of the 1st ACM Conference on Computer and Communications Security, ACM Press, Fairfax, 62-73. https://doi.org/10.1145/168588.168596.
[15] Hichan Moon, & Cox, D. C. (n.d.). Efficient power allocation for coded OFDM systems. IEEE 60th Vehicular Technology Conference, 2004. VTC2004-Fall. 2004. doi:10.1109/vetecf.2004.1404904
[16] Arora, S., Chandna, V. K., & Thomas, M. S. (2012). Performance Analysis of 16-QAM using OFDM for Transmission of Data over Power Lines. Energy Procedia, 14, 1723–1729. doi:10.1016/j.egypro.2011.12.1158.

Doi : https://doi.org/10.54216/FPA.090201
Received: May 10, 2022 Accepted: October 22, 2022

[17] Wang, Z., Chen, F., Qiu, W., Chen, S., & Ren, D. (2018). A two layer chaotic encryption scheme of secure image transmission for DCT precoded OFDM-VLC transmission. Optics Communications, 410, 94–101. doi:10.1016/j.optcom.2017.09.095
[18] Abdelaleem, O., Khedr, M., Sharkas, M., & Almaghrabi, A. (2007). Robust Wireless Image Communications Using Combined SPIHT/OFDM Technique. 2007 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing. doi:10.1109/pacrim.2007.4313178.

Doi : https://doi.org/10.54216/FPA.090201
Received: May 10, 2022 Accepted: October 22, 2022