A privacy-preserving cryptosystem for IoT E-healthcare

(Article begins on next page)

03 May 2024

A privacy-preserving cryptosystem for IoT E-healthcare

[1]Rafik Hamza, [2,3]Zheng Yan*, [4]Khan Muhammad, [5]Paolo Bellavista, [6]Faiza Titouna

[1] Sonatrach, Direction Centrale Recherche et Développement, Avenue 1 Novembre, 35000, Boumerdes, Algeria
[2]School of Cyber Engineering, Xidian University, China
[3]Department of Communications and Networking, Aalto University, Finland
[4]Intelligent Media Laboratory, Digital Contents Research Institute, Sejong University, Seoul, Republic of Korea
[5]Department of Computer Science and Engineering, University of Bologna, Italy
[6]Department of Computer Science, University of Batna 2, Algeria

---

Abstract

Privacy preservation has become a prerequisite for modern applications in the cloud, social media, Internet of things (IoT), and E- healthcare systems. In general, health and medical data contain images and medical information about the patients and such personal data should be kept confidential in order to maintain the patients' privacy. Due to limitations in digital data properties, traditional encryption schemes over textual and structural one-dimension data cannot be applied directly to e-health data. In addition, when personal data are sent over the open channels, patients may lose privacy of data contents. Hence, a secure lightweight keyframe extraction method is highly required to ensure timely, correct, and privacy-preserving e-health services. Besides this, it is inherently difficult to achieve a satisfied level of security in a cost-effective way while considering the constraints of real-time e-health applications. In this paper, we propose a privacy preserving chaos-based encryption cryptosystem for patients' privacy protection. The proposed cryptosystem can protect patient's images from a compromised broker. In particular, we propose a fast

---

*Corresponding Author: Zheng Yan (zheng.yan@aalto.fi)

probabilistic cryptosystem to secure medical keyframes that are extracted from wireless capsule endoscopy procedure using a prioritization method. The encrypted images produced by our cryptosystem exhibits randomness behavior, which guarantee computational efficiency as well as a highest level of security for the keyframes against various attacks. Furthermore, it processes the medical data without leaking any information, thus preserving patient's privacy by allowing only authorized users for decryption. The experimental results and security analysis from different perspectives verify the excellent performance of our encryption cryptosystem compared to other recent encryption schemes.

1 Introduction

Digital images security has become extremely significant in the last decade, especially with the rapid advancements in communication networks and multimedia applications [15]. In this pursuit, several encryption approaches have been used to guarantee data confidentiality and enhance the security of digital images. During the paradigm of image encryption, the sender selects a secret key and encrypts the data using a specific encryption cryptosystem such as homomorphic encryption [10] and attribute-based encryption [11]. The authorized users should be able to decode the encrypted data using the secret keys of a decryption algorithm. The security heavily relies on keeping the secret key confidential from attackers, and not the encryption machine as illustrated by Kirchhoff's principle [28]. Encryption is the main mechanism to ensure the security of digital images during transmission. Hence, researchers have attempted to present various image encryption methods in two last decades [19, 38]. However, getting a satisfied level of security while keeping the computational complexity reasonable is still a challenging issue especially with transmission of medical images for real-time applications.

The collection medical data paradigm raises serious privacy concerns mainly

because of the high sensitivity of these data. There is a need to protect the medical data confidential and process its large amount against unauthorized parties. In this pursuit, privacy and security for medical images can be guaranteed by engaging encryption to ensure confidentiality and authentication [17]. Many studies have pointed out that a good encryption cryptosystem should be extremely sensitive to any adjustment in the secret keys and should have low computational complexity [16, 42, 44]. Over the past two decades, the traditional encryption techniques like AES, DES, and IDEA have been widely used, however, these techniques are designed principally for textual and structural one-dimension data, but not suitable for digital images [27]. This kind of data has various unique properties such as distinguished with huge data capacity, strong correlation among pixels, and having two dimensions. Thus, digital images require different encryption approaches than textual data [51]. Furthermore, traditional data encryptions have huge computational complexity, limiting their applicability in modern applications and image transmission in real-time [4, 24, 32]. Thus, it is really challenging to satisfy the demands of an image encryption in terms of high security to resist the existing attacks and minimize the computational complexity.

The evolution of technology and the Internet shows numerous interesting applications especially due to the recent digital advances in E-health, IoT, and communication technologies. Wireless capsule endoscopy (WCE) is an imaging system that allows presenting the interior view of patient's intestine through a capsule-shaped tiny camera. During each WCE process, the expert doctors at the healthcare centers can receive diagnostic frames from the WCE video to take a real-time decision. The device facilitates doctors with a visualization of the gastrointestinal tract and sends the medical images wirelessly [45]. Patient at the start of the diagnostic process swallows WCE capsule, and then the endoscopic images captured by the camera are stored in image recording unit (IRU). In general, the expelling time for the capsule is 72 hours but the frames of first 8 hours are more important for analysis and abnormality findings. The doctors need a set of frames that are diagnostically important though the capsule cap-

3

tures a large number of frames. For instance, the WCE device captures 50,000 frames in the interval of the first eight hours only [20]. Manual extraction of this set of frames is tedious and time consuming. To avoid this, video summarization methods can be used [33]. Furthermore, for real-time medical applications, a secure lightweight keyframe extraction method is required to ensure timely, correct, and privacy-preserving diagnosis of patients.

In this paper, we propose a secure and fast probabilistic image encryption cryptosystem to guarantee the privacy of the extracted keyframes during WCE. The proposed encryption cryptosystem preserves the privacy of the patient's information. The proposed cryptosystem is applied to keyframes instantly after extracting them using a video summarization method from WCE video data. The summarization cryptosystem utilizes integral-image based features making it very appropriate for real-time processing of WCE. The proposed chaos-based cryptosystem is performed by a symmetric block encryption cryptosystem based on one round of confusion and diffusion operations. Moreover, we propose a new Pseudo Random Number Generator (PRNG) based on Zaslavsky chaotic map and 2D logistic map. To the best of our knowledge, this work is one of the first PRNG algorithms based on Zaslavsky system. The encryption cryptosystem is made probabilistic by using an additional randomization mechanism. This means that if we encrypt the same data twice using the same secret keys, the generated pair encrypted data will be different from each other. This probabilistic behavior makes our cryptosystem more suitable for real-time applications and creates hurdles for attackers in decryption. Performance evaluations show that the proposed PRNG has outstanding properties such as a wider key space, the unpredictability for the generated sequences, and dominating state-of-art method [35]. Furthermore, simulation tests and security analysis demonstrated the ability of the proposed cryptosystem to withstand different attacks. In addition, the proposed cryptosystem has a large key space that makes exhaustive attacks infeasible. The probabilistic behavior, secret key, and plain-image sensitivity make the proposed cryptosystem resistant to statistical and differential attacks (e.g., the known-plaintext attacks) as well as the chosen cipher-text

4

attacks. Overall, the proposed system reduces the energy, communication bandwidth, specialist analysis time and searching efforts as well as ensure the security of keyframes during its dissemination to healthcare centers. Thus, we can ensure that the cryptosystem is fast, secure, and robust against all known attacks.

To sum up, the main contributions in this work are summarized as follows:

1. We propose an efficient probabilistic cryptosystem to guarantee the medical keyframe confidentiality and protect the privacy of patients.

2. A new chaos-based PRNG is proposed that relies on mixing and cascading the orbits of two 2D chaotic maps.

3. The proposed cryptosystem is experimentally tested from different perspectives, showing excellent performance compared to recent image encryption schemes [6, 7, 19, 47, 52, 55, 57, 58]. In particular, it can provide a high-level security in a cost-effective way compared to existing methods.

4. The proposed cryptosystem guarantees secure and privacy-preserving transmission of diagnostically relevant keyframes to medical specialists and tailors a modern application of WCE with reduced energy, communication bandwidth, specialist analysis time as well as searching efforts.

The remaining of this article is organized as follows. We describe and discuss the related works in Section 2. In Section 3, we present the structure of PRNG algorithm based on Zaslavsky chaotic map and 2D logistic map, and describe the proposed cryptosystem to encrypt/decrypt the medical keyframes. Section 4, we present the experimental results and security analysis. In Section 5, we conclude this work and present some future directions for further research.

2   Related Work

In this section, we present the relevant literature of recent years. First, we present details of related works and highlight their key limitations regarding medical data privacy and security. At the end of this section, we briefly introduce our solution for tackling this issue.

Medical data become a valuable commodity and therefore patients' data privacy should be protected. Consequently, some cryptography techniques are presented to guarantee the video and digital images security such as compression methods [34], authentication methods [49], hybrid steganography and cryptosystem methods [1-3, 13], and encryption methods [9, 40]. The latest research on encryption methods have been suggested to ensure users' data privacy. For instance, Wei et al. [48] presented an encryption cryptosystem to conceal unintended human faces for multimedia social networks by proving access to only authorized users to blur certain regions. Encryption techniques rely on using mathematics and different transformation techniques such as Latin square, chaotic maps, neural networks, and DNA technique encryption. The performance of these ciphers is well-recognized especially the chaotic maps encryption, which have several applications in modern cryptography [39].

The literature presents nonlinear dynamics in two ways: discrete systems such as logistic map and continue systems such as hyper-chaotic system [18]. These systems have been widely used in cryptography mainly due to their capability of generating random number sequences with excellent stochastic behaviour. In addition, the initial values of the chaotic maps are extremely sensitive to any adjustment. Based on this, the cryptographers used these initial values as secret keys in chaos-cryptosystems. In this regard, one of the most known cryptographic applications is chaotic-based pseudo random number generator (PRNG) algorithm. The PRNG used widely to produce stream keys for chaotic-encryption schemes. For instance, Hu et al. [21] presented a cryptographic PRNG based on a high-dimensional chaotic map using the combination of three coordinates of the chaotic orbits suitable for image encryption among other cryptographic applications. Yet, the recent studies show some issues with PRNGs even with high-dimensional chaotic map [37], and specifically with lower dimensional chaotic systems. Although it is impossible to predict the generated sequences from high-dimensional chaotic systems, yet, they have certain shortcomings including complex performance and high computational complexity [22]. Also, one-dimensional chaotic systems have small space keys and more

6

vulnerable to degradation problem in the case of finite computing precision [26], which effects the length cyclic of the generated sequences. The chaotic systems can be used to produce a sequence of real numbers with randomness properties. Nevertheless, the generated sequences from chaotic maps do not fit the computations with the pixels of digital images directly without using a finite precision. Also, those generators are not suitable for direct employing and less suitable for applications with real-time requirements such as encryption of representative frames during the real-time process of WCE [29].

Recently, we proposed an encryption cryptosystem [19] for security of digital images based on Zaslavsky chaotic map with four iteration of permutation-diffusion processes. The generated chaotic signals were used directly for permutation stage, and without any finite precision computation. In this step, a diffusion$(K \cdot B \cdot L)_{2^8}$process was applied for each [32×32] block "B" using an invertible matrix over finite field. The results showed satisfactory security performances and the cryptosystem demonstrated capability of withstanding against various attacks. Although the previous image cryptosystem is suitable for all kind of images. Yet, the proposal was not designed directly for color images and for such special kind of medical images (keyframes), there exists diversity in the nature of digital images and even more with its use, requiring different constraints. WCE is an excellent example, where the medical images are captured using a wireless capsule with the help of a tiny camera. Once the summarization method selects keyframes, the healthcare center can receive the informative data (keyframes) to keep tracking the patients and ongoing treatment. An example of such informative and non-informative frames are given in Fig. 1. In this regard, the secure transmission of such frames is very crucial due to heavy dependency of the target treatment on it. Therefore, considering the special characteristics of these keyframes and constraints of WCE procedure, we employed a light-weight video summarization technique [33] using integral-image for calculating various features and classification into informative and non-informative. Subsequently, a probabilistic image encryption cryptosystem is used to encrypt the keyframes and preserve the patients' privacy. Indeed,
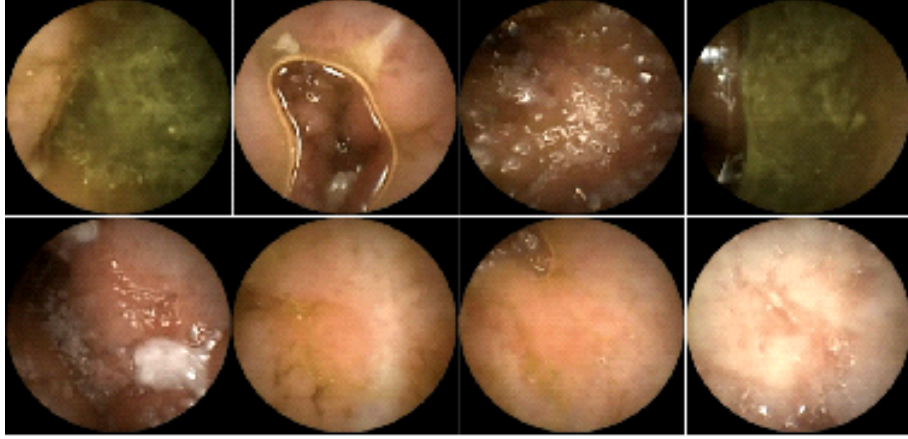
Figure 1: Illustration of non-keyframes and keyframes from wireless capsule endoscopy procedure. The images in the first row are non-informative while the images in the 2nd row are informative.

the privacy of patients becomes fully protected thanks to the encrypted information, where only authorized users can decrypt the medical data, making our cryptosystem more suitable for privacy perseveration during WCE for e-health.

3   Proposed Cryptosystem

In this section, we illustrate the keys generation algorithm based on two 2-D chaotic system, followed by encryption/decryption algorithms for the extracted keyframes from WCE data. The proposed cryptosystem provides privacy preservation of the concerned medical data with access to only authorized people. This ensures that the authorized users will have access to the extracted keyframes, while the unauthorized users will obtain random images.

3.1   PRNG based on Chaotic Maps

In this sub-section, we present details of the encryption keys algorithm for the proposed cryptosystem.

3.1.1 2D-Zaslavsky Chaotic Map

The Zaslavsky chaotic map is a nonlinear discrete system with two chaotic orbits. This map is introduced by George M. Zaslavsky in 1978 and has been implemented in several applications [19]. The formula of Zaslavsky chaotic map is denoted using Equation (1) below:

$$
\begin{cases}
x_{i+1} = x_i + v\,(1 + uy_i) + \varepsilon vu\,(\cos{(2\pi x_i)}) \bmod 1 \\
\quad y_{i+1} = e^{-\tau}(y_i + \varepsilon \cos{(2\pi x_i)}) \\
\quad\quad Where, \quad u = \frac{1-e^{-\tau}}{\tau}
\end{cases}
\tag{1}
$$

The Lyapunov spectrum of the 2D-Zaslavsky chaotic map is computed 1.55 [19]. This demonstrates that the generated chaotic sequence has good random statistical characteristic. As a result, the output signal of this system is very chaotic and unpredictable and thus we incorporated it in the proposed cryptosystem.

3.1.2 2D-Logistic Map

The 2D logistic map is a discrete dynamic system with a chaotic behavior of the evolution of orbits and attractors [52]. It has extra complex random behavior than the 1-D logistic map [52]. This noninvertible two-dimensional map is denoted using Equation (2) below:

$$
\begin{cases}
x_{i+1} = r(3y_i + 1)x_i(1 - x_i) \\
y_{i+1} = r(3x_{i+1} + 1)y_i(1 - y_i)
\end{cases}
\tag{2}
$$

Herein, 'r' is the parameter of the system [52], where 2D-Logistic system is chaotic if the value of "r" is within [1.1-1.19]. In this equation, (x_i, y_i) is a point of the loop. This card depends on the initial conditions (x_0, y_0) and the parameter "r" to determine its trajectory. The Lyapunov of the 2D logistic chaotic system is positive and computed to be around 3.68 [52], proving that the output signal of the system is chaotic and unpredictable. Moreover, it has been used widely with encryption images [52]. Both 2D-logistic map and ZCM are highly sensitive to their initial values and are more chaotic than other chaotic systems like Hénon chaotic map [52]. As discussed, these characteristics are

9

convenient for a cryptosystem especially to produce the encryption keys that match the requirements of digital images e.g. keyframes of WCE.

3.1.3 PRNG Algorithm

In this part, we employ two chaotic maps to design the proposed PRNG. The behaviors of these maps are deterministic under the iteration with the same conjugate. The proposed encryption cryptosystem uses the sequences generated by PRNG to encrypt the pixels of the plain image. To avoid the degradation problem caused by using finite precision computation, we cascade and mixes the samples of these chaotic maps. According to a previous research [25], using multi-chaotic maps and cascading the orbits should be enough to avoid the problem of degradation.

Algorithm 1 describes the processing steps of the proposed PRNG, while Algorithm 2 shows the steps of generating these stream keys based on Algorithm 1 for the proposed cryptosystem. We discard the first teen numbers of the generated sequence so that we can get rid of initial values effect on the generated sequence. The generated keys are the index sorts to carry out the permutation process of the proposed cryptosystem, and the $[32 \times 32]$ invertible matrix $(K_{initial})$ over the finite field of Gf (2^8). In addition, Alpha should not return zero and it will link all the initial values, which will enhance the key sensitivity of the proposed cryptosystem. The PRNG is employed to generate the encryption keys for the medical keyframes from WCE.

Algorithm 1. Pseudo Random Numbers Generator

Input: $x_{l(0)}$, $y_{l(0)}$, $v, \varepsilon, \tau, x_{z(0)}$, $y_{z(0)}, r, m$.

1: $[x_l, \ y_l] \leftarrow [x_{l(0)}, \ y_{l(0)}]$

2: $[x_z, \ y_z] \leftarrow [x_{z(0)}, \ y_{z(0)}]$

3: **For** i = 1 to ceil(m/4)

$[x_l, \ y_l] \leftarrow \text{Logistic}(x_l, y_l, r)$

$[x_z, \ y_z] \leftarrow \text{ZCM}(x_z, \ y_z, v, \varepsilon, \tau)$

$Vec(4 \times i) \quad = round(abs(10^{14} \times x_z \times x_l \times y_l)) \, mod \, 256.$

$Vec(4 \times i + 1) = round(abs(10^{14} \times x_l \times x_z \times y_z)) \, mod \, 256.$

$Vec(4 \times i + 2) = round(abs(10^{14} \times y_z \times x_l \times y_l)) \, mod \, 256.$

$Vec(4 \times i + 3) = round(abs(10^{14} \times y_l \times x_z \times y_z)) \, mod \, 256.$

End

Output: Vec

3.2 Encryption Algorithm

This part describes the details of our image encryption scheme, which adopts permutation–diffusion architecture using the chaos-based PRNG. All the initial values of the 2D logistic map and ZCM are considered as secret keys in this algorithm with main steps described as follows:

Step 0: Read plain image I, followed by applying Algorithm 1 and Algorithm 2 using the secret keys.

Step 1: Apply the initial processing as follows.

The extracted keyframes from WCE data have been captured with black zones in footnotes. We aim to employ this property in the proposed encryption, and without affecting the quality of the visual medical images. First, we apply disruption footnotes for each color channel of the extracted keyframe. These steps are described in Algorithm 3, where the matrices (R, G, and B) have been adjusted by embedding random bits to the footnotes pixels of each matrix.

Algorithm 2. The generation of encryption Keys

Input:$x_{l(0)},\ y_{l(0)}, v, \varepsilon, \tau, x_{z(0)},\ y_{z(0)}, r,\ K_{initial},\ I(Plain\,image)$.

1: $[h, w, e] \leftarrow size\ (I)$

2: m=max(max $(10 + h, 10 + w \times e), 1034)$

3: Vec $\leftarrow PRNG(x_{l(0)},\ y_{l(0)}, v, \varepsilon, \tau, x_{z(0)},\ y_{z(0)}, r, m)$

4: $[\sim, V] \leftarrow$ sort(Vec(11 : h + 10))

5: $[\sim, V'] \leftarrow$ sort(Vec(11 : e $\times w + 10$))

6: $K \leftarrow$ reshape(Vec(11 : 1034), 32, 3 2)

7: $\alpha = \sum Vec \mod 256$

8: $if\ \alpha = 0\ then$

$\alpha = \sum Vec \mod 255$

$End\,if$

9: $K \leftarrow (K_{initial})_{2^8}$

10: $R \leftarrow \alpha \times K$

11: $L \leftarrow (R^{-1})_{2^8}$

Output: V, V', α, R, L

Here in Algorithm 3, noise addition is a two-step process: generating truly random numbers and combining them with the pixels of keyframes using bitwise-XOR operation. We set the adjustment in the algorithm by the first and the last 21 column from the input keyframe matrix. To get the pixel values of the black-zone in footnotes of keyframes, we hold two pixels (the first and the last pixel), containing the original values of the block-zone. This ensures that the process will not cause any damage to the important regions of the keyframe for medical diagnostic. Fig. 2 shows a keyframe and the obtained matrix from this step.
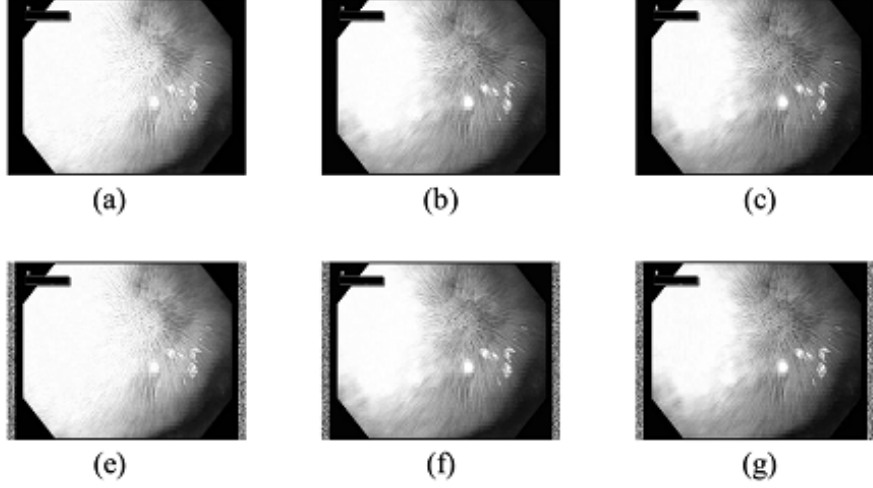
12

Figure 2: Noise numbers effect on footnotes in each color channel of the keyframe. (a) Channel R in keyframe. (b) Channel G in keyframe. (c) Channel B in keyframe. (e) Effect of Algorithm 3 for channel R. (f) Effect of Algorithm 3 for channel G. (g) Effect of Algorithm 3 for channel B.

Algorithm 3. Disruption footnotes

Input: $I_{R,G,B}$ ($Plain\,image$).

1: $C_{R,G,B} \leftarrow Noise(I_{R,G,B})$

2: $C_{R,G,B}(1,1) = I_{R,G,B}(1,1)$;

3: $C_{R,G,B}(end, end) = I_{R,G,B}(end, end)$;

4: $C_1 \leftarrow [C_R\, C_G\, C_B]$

Output: C_1

Step 2: Shift all pixels of the obtained matrix C using the index sort V, V'. The pixels along "w" are shifted using the key V. The pixels along "w" are shifted using the key V'. The obtained matrix is denoted by C_2.

Step 3: Shift each sub-block of the obtained matrix C_2 using the index sort in columns of the matrix R. The obtained matrix is denoted by C_3.

Step 4: The matrix multiplication over finite field GF (2^8) is applied on each

block [32×32] of C_3 as follows.

$$C_4 \leftarrow (L \cdot B_{C_4})_{2^8} \tag{3}$$

Herein, B_{C_2} represents [32×32] bock from C_2 matrix. The obtained matrix is denoted by C_4.

Step 5: Repeat Step 2 of permutation by the vectors V, and V'. C_5 is the obtained matrix.

Step 6: Repeat Step 3 of permutation using the matrix R. The obtained matrix is denoted by C_6

Step 7: Apply the following Equation (4) and obtain the matrix denoted by C_7.

$$C_7 \leftarrow (B_{C_6} \cdot K)_{2^8} \tag{4}$$

Step 8: Repeat Step 2. The obtained matrix is denoted by C_8.

Step 9: Reshape C_8 matrix into three matrices $C_R C_G C_B$ corresponding to the RGB matrix. The obtained matrix "C" is the encrypted image for plain image I.

The resultant encrypted keyframe seems to be a random image and cannot be distinguished from random sources. Thus, it is hard to obtain any information regarding patients without the exact values of secret keys, ensuring the patients' privacy.

3.3   Decryption Algorithm

In this sub-section, we illustrate the steps of decryption algorithm to reconstruct the keyframes at receiving end. Due to the use of the randomization process, the cryptosystem can be defined as a lossless cryptosystem. Nevertheless, the decryption can reconstruct the keyframe from the encrypted image without losing its visual appearance. The following steps explain the decryption processing for the proposed algorithm.

Step 0: Read the decrypted image, and get its size *[h, w]*. Next, apply Algorithm 1 and 2.

14

Step 1: Reshape the image matrices (corresponding to RGB matrices) into a single matrix with size [h, 3×w]. The obtained matrix is denoted by D_1.

Step 2: Apply an operation inverse of step 2 in the encryption algorithm, which means that the keyframe pixels should be recovered successfully using the sorted indices. The obtained matrix is denoted by D_2

Step 3: The matrix multiplication using Galois Fields GF (2^8) is applied on each block [32×32] of the obtained matrix as follows.

$$D_3 \leftarrow (B_{D_2} \cdot L)_{2^8} \tag{5}$$

Herein, B_{D_2} represents [32×32] bock from D_3 matrix. The obtained matrix is denoted by D_3.

Step 4: Apply an operation inverse of Step 3 in the encryption algorithm using the index sort in column of R. The obtained matrix is denoted by D_4.

Step 5: Repeat Step 2 in the decryption algorithm. The obtained matrix is denoted by D_5.

Step 6: Apply the following Equation (6), the obtained matrix is denoted by D_6.

$$D_5 \leftarrow (K \cdot B_{D_2})_{2^8} \tag{6}$$

Step 7: Repeat Step 4 in decryption algorithm. The obtained matrix is denoted by D_7.

Step 8: Repeat Step 2 in decryption algorithm. The obtained matrix is denoted by D_8.

Step 9: Apply final processing as described in Algorithm 4 to get the decrypted image "D".

Algorithm 4. Recover footnotes blocks

Input: D_8 .

1: $[D_R \, D_G \, D_B] \leftarrow D_8$

2: $Ones \leftarrow matrix \; of \; ones \; [h, \, 21]$

3: $D_{R,G,B}(1:h, \; 1:21) \leftarrow Ones \times D_{R,G,B}(1, \, 1)$

4: $D_{R,G,B}(1:h, \; end-20:-1:end) \leftarrow Ones \times D_{R,G,B}(end, \, end)$

Output: $D_{R,G,B}$

---

4 Security Analysis and Discussion

In this section, we carried out different tests to evaluate the efficiency and effectiveness of the proposed cryptosystem. The experiments and measurements include resistance against statistical attacks, secret key attacks, and differential attacks. First, the histogram analysis is provided demonstrating that the encrypted image pixels are in uniform distribution as well as completely different from the histograms of the plain images. Next, information entropy is computed; verifying the resistance against entropy attacks and demonstrates that the encrypted image acts like a random source. The correlation coefficient proves that the proposed cryptosystem eliminates successively the correlation between adjacent pixels of the plain image. The differential attacks are measured using number of pixels change rate (NPCR) and unified average changing intensity (UACI) tests. Secret keys analysis determines the resistance capability of our cryptosystem against exhaustive attacks. The probabilistic analysis performed in this section proves that the cryptosystem produces completely different encrypted keyframes using the same keyframe and the same secret keys. Furthermore, the sensitivity analysis confirms without any debt that the keyframe restoration cannot be accomplished without the exact numerical values of the secret keys. This means that any amendment to the secret keys will lead to a completely different encrypted image. In addition, image quality analysis
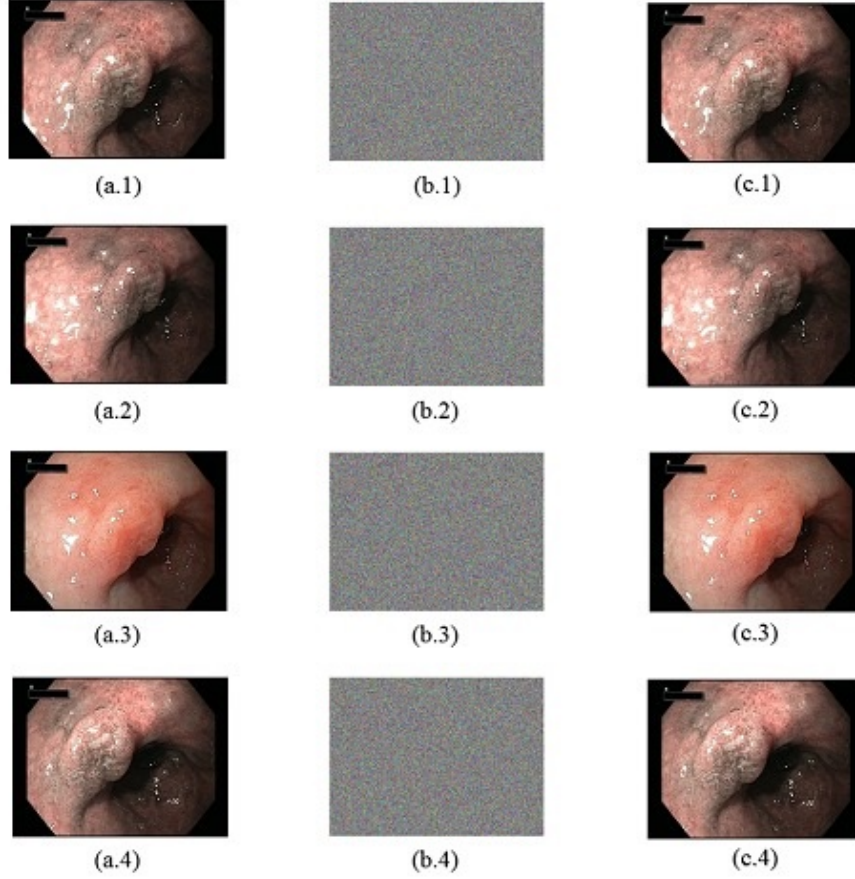
16

Figure 3: Visual encryption tests. (a) Original frames. (b) Encrypted frames. (c) Decrypted frames.

confirms that the decrypted image has good quality. Anti-clipping analysis tests the robustness of cryptosystem in cases of losing some pixels of certain blocks. Finally, the comparison analysis shows the superiority of our cryptosystem over other recent state-of-art cryptosystems. These detailed security analysis and tests are performed using Matlab R2015a in Windows 10 environment, with i7 processor 2.4 GHz and 12 GB of RAM.
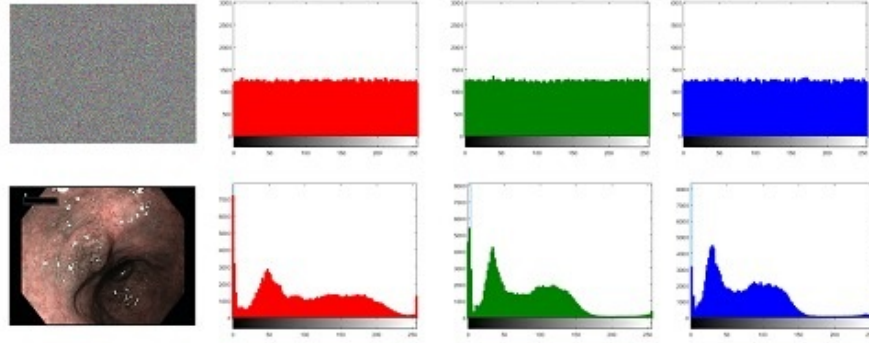
Figure 4: The histogram test of the encrypted image and the decrypted image in the three Red, Green, and Blue components.

4.1 Histogram Analysis

In this test, we analyze the distribution of numerical data of the keyframe and its corresponding encrypted image. The histogram represents the image pixels distribution through plotting the number of pixels at each color intensity level [51]. This test intends to verify that the pixel values of the encrypted image has a uniform distribution and completely different histogram in comparison with the original distribution of the pixel values. Fig. 3 shows the plain images, their encrypted versions, and decrypted images, respectively. Fig. 4 shows the keyframes histograms and encrypted images in three components of RGB, respectively. The histograms of the encrypted images in three components are uniform and very different from the keyframes image histograms.

4.2 Information Entropy Analysis

In this test, we present entropy analysis of the encrypted images to investigate its randomness. Shannon's entropy [43] proposes a method for measuring the randomness of the encrypted image. The mathematical equation of Shannon's entropy test is defined as follows:

$$E(C) = -\sum_{i=1}^{n} P(c_i) \log_2 P(c_i) \tag{7}$$

18

Herein, $P(c_i)$ describes the probability of $c_i \in C$, while C is an ensemble of symbols and "n" is the number of all symbols. According to Shannon, the encrypted image pixels should show a uniform distribution. The ideal numerical score of local Shannon entropy test is eight. The results of this test are given in Table 1, and the comparative analysis with other recent methods [55] are shown in Table 2. In particular, Table 1 shows the results of local Shannon entropy for a keyframe and the corresponding encrypted image in the three channels (RGB). As shown, all the numerical scores of the encrypted data are very close to 8, validating the efficiency of the proposed work compared to other recent works [55]. The results demonstrate that the proposed image cryptosystem can transform the medical keyframe to a random image.

Table 1: The local Shannon entropy tests.

Component	Keyframe	Ciphered
R	7.2657	7.9995
G	7.0346	7.9994
B	6.9276	7.9994

Table 2: The local Shannon entropy comparison tests.

Algorithm	Proposed	Yao et al. [55]	Wei et al. [47]
Image size	[640,480,3]	[512,512,3]	[256,256,3]
Entropy(Red)	7.9995	7.9993	7.9971
Entropy(Green)	7.9994	7.9993	7.9969
Entropy(Blue)	7.9994	7.9992	7.9962

4.3 Correlation Coefficient Analysis

In this test, correlation coefficient test proves the ability of the proposed cryptosystem in eliminating the correlation between adjacent pixels of a keyframe. Correlation indicates the strength and direction of a linear relationship between two random variables [46]. Based on this, we examine the connection between two adjacent pixels of the encrypted and the original keyframe. Due to large

number of the medical keyframe pixels, we choose randomly 2048 pairs of adjacent pixels for testing the correlation of two adjacent pixels from vertical, horizontal, and diagonal directions, respectively. Equation (8) calculates the correlation of two adjacent pixels.

$$CC_{xy} = \frac{cov(x,y)}{\sqrt{D(x) \times D(y)}} \tag{8}$$

$$cov(x,y) = \frac{1}{n}\sum_{i=1}^{n}(x_i - E(x))(y_i - E(y)) \tag{9}$$

$$D(x) = \frac{1}{n}\sum_{i=1}^{n}(x_i - E(x))^2 \tag{10}$$

$$E(x) = \frac{1}{n}\sum_{i=1}^{n}x_i \tag{11}$$

Table 3 shows the results of this test with a selected keyframe and its corresponding encrypted image in red, blue, and green components. The ideal value for this test with an encrypted image should be found CC=0 [36]. The original keyframe shows strong correlation between adjacent pixels in each direction (CC∼=1). The ideal numerical score of correlation coefficients test for an encrypted image should be is zero, indicating that there is no correlation between adjacent pixels. In addition, we illustrate the correlation distribution of the keyframe and its corresponding encrypted images using Fig. 5. The dots in encrypted image are scattered over the entire plot while the dots in the plain image are restricted to a particular area within the plot figure. Therefore, the encryption cryptosystem can efficiently eliminate the correlation between adjacent pixels of the medical keyframe.

Table 3: The correlation coefficient analysis.

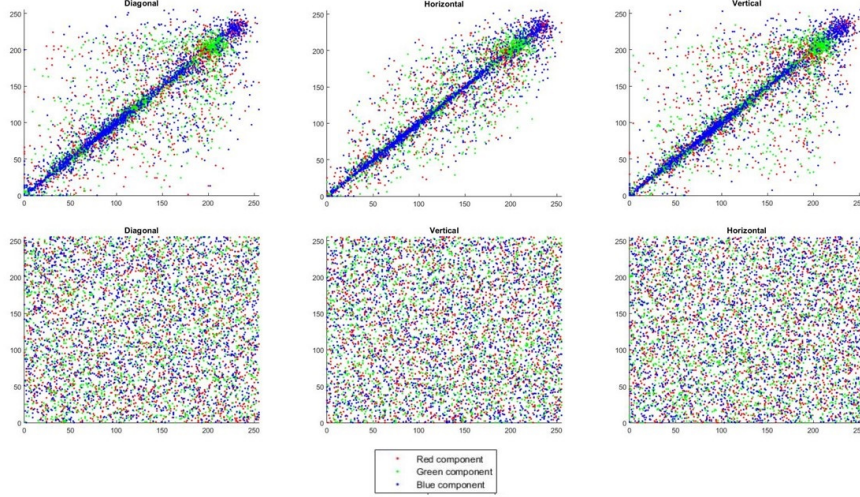| Component	Keyframe			Ciphered		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
R	0.9937	0.9901	0.9854	0.0012	-0.0027	0.0002
G	0.9909	0.9834	0.9877	-0.0007	0.0021	-0.0010
B	0.9931	0.9824	0.9901	0.0015	-0.0010	0.0007

Figure 5: Correlation of two adjacent pixels in horizontal, vertical, and diagonal in the three spectral components (R, G, and B) before and after encryption.

4.4   NPCR and UACI Analysis

In this test, we measure the ability of the proposed cryptosystem to withstand against the differential attack via NPCR and UACI tests [56]. NPCR refers to the number of pixels change rate when one pixel of the plain image is changed, while UACI refers to the average intensity of change between the keyframe image and encrypted image. The ideal score of NPCR and UACI tests for an encryption algorithm should be near to 99.61 % and 33.44%, respectively [12]. Differential attack investigates the relation between the input processes and the corresponding outputs [41]. Accordingly, we calculate NPCR and UACI numerical scores between two encrypted images C*1* and C*2*. In this step, images J and I, which differ only in one bit, are used to produce the encrypted images C1 and C2. Then, we use Equation 12 and Equation 13 to compute the results of NPCR and UACI.

$$NPCR(C_1, C_2) = \sum_{i,,j} \frac{S(i,j)}{D} \times 100 \ \% \tag{12}$$

$$UACI(C_1, C_2) = \sum_{i,,j} \frac{C_1(i,j) - C_2(i,j)}{255 \times D} \times 100\ \% \tag{13}$$

"D" denotes the number of pixels whereas "S" is expressed by Equation 14 as follows:

$$S(i,j) = \begin{cases} 0, & IF\ C_1(i,j) = C_2(i,j) \\ 1, & Elsewise. \end{cases} \tag{14}$$

In this test, a single bit of a pixel from the original keyframe "I" is changed, resulting in new keyframe denoted by "J". We encrypted these keyframes using the same secret keys, and we obtained two encrypted images C_1 and C_2 corresponding to the keyframes "I" and "J". Next, we passed both C_1 and C_2 from NPCR and UACI tests using each RGB channel. Table 4 lists the results of a few sample images. The proposed cryptosystem proves that each encryption process is completely different from each other (randomized encrypted images). Fig. 6 shows the NPCR and UACI results for two encrypted images. In particular, we encrypted the same plain images using the same secret key and employed the above tests of NPCR and UACI for the pair encrypted images. Table 4 shows the theoretical score for these tests presented by Wu et al. [53]. After the third line in Table 4, we showed the average result of repeating this test 100 times. The obtained results are satisfactory and the cryptosystem performances successfully passed these tests and meet all theoretical expectations. Furthermore, we compared the performances of the proposed image encryption with recent encryption schemes in Table 5, demonstrating its effectiveness.

Table 4: Results of NPCR and UACI test.

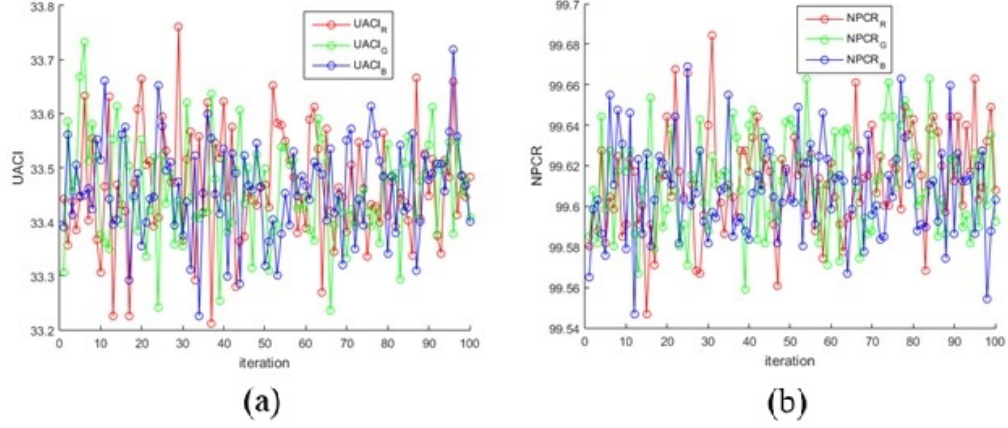|	0.05-level	0.01-level	0.001-level
Expected value NPCR	>99.5693%	>99.5527%	>99.5341%
Expected value UACI	33.2824-33.6447%	33.2255-33.7016%	33.1594-33.7677%
$\text{NPCR}_{(R,G,B)}(99.6098)$	Pass	Pass	Pass
$\text{UACI}_{(R,G,B)}(33.4658)$	Pass	Pass	Pass

[1]

Figure 6: Evaluation of our encryption cryptosystem using NPCR and UACI test for 100 iterations.

Table 5: NPCR and UACI comparison results for each channel of RGB.

Keyframe	Our Algorithm		Wei et al. [47]		Zhou et al. [57]	
Image size	[640×480×3]		[640×480×3]		[512×512×3]	
	NPCR	UACI	NPCR	UACI	NPCR	UACI
R	99.6068	99.6068	99.5864	33.4847	99.62	33.39
G	99.6149	99.6149	99.2172	33.4639	99.61	33.42
B	99.6172	99.6172	98.8479	33.2689	99.59	33.40

4.5 PRNG Analysis

In this section, we present different analysis and tests for evaluation of the PRNG algorithm. To test the secret keys sensitivity for the cryptosystem, we change slightly one value of the PRNG initial values to see if the cryptosystem will produce a different sequence from the original one. The difference between two sequences P1 and P2 produced by the proposed PRNG is shown in Fig. 7a. These sequences have been produced using two secret keys S1 and S2, where
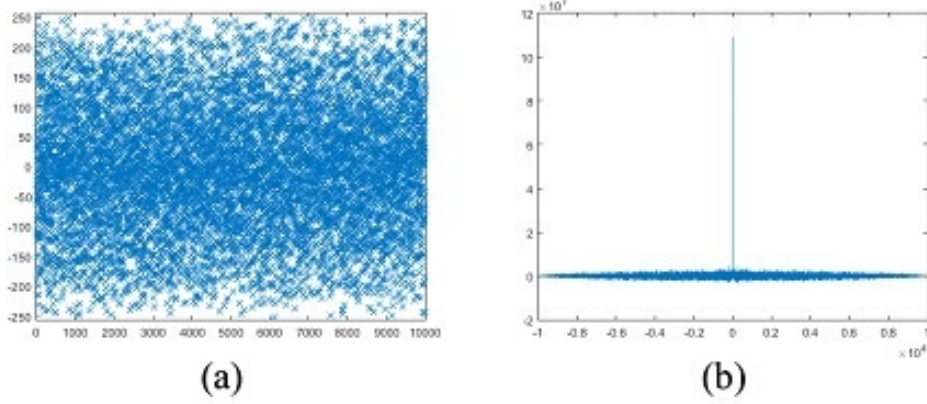
23

Figure 7: The deference plot (P1-P2), (b) Auto-correlation of the difference of these sequences.

S1: [0.2; 0.8; 7; 6; 5; 0.1; 0.9; 1.18] and S2: [0.2+10^{-14}; 0.8; 7; 6; 5; 0.1; 0.9; 1.18]. In addition, Fig. 7b shows the auto-correlation analysis of these generated sequences. The experimental result shows that the difference ratio between P1 and P2 is approximated to *99%*. This means that changing secret keys even with extremely small value (e.g., $+10^{-14}$) will produce a completely different new number sequence. Thus, we can only conclude that the PRNG is extremely sensitive to the chosen initial keys, and the generated sequences are completely independent from each other.

Furthermore, we tested the generated sequences from the proposed PRNG using NPRC and UACI tests. These tests are used for the encrypted images to measure the resistance against the differential attacks. In this test, we produce the first sequence using the secret key S1. Next, we produce 100 PRNG sequences (denoted by S3) using 100 secret keys differ only by tiny change and only in one of the initial value of S1. Fig. 8 shows the results of 100 analysis of NPCR and UACI tests of the generated sequences using S1 and S3. The average result is 99.6089% and 33.4259% for NPCR and UACI tests, respectively. The proposed PRNG overrides other recent PRNGs in the same test such as in Murillo-Escobar et al. [35] (NPCR = 99.5774%, UACI =33.3014%).
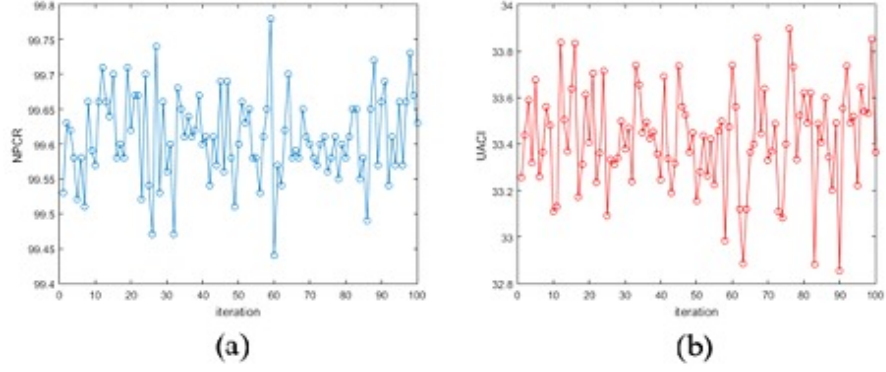
24

Figure 8: (a) NPCR and (b) UACI tests of two sequences using S1 and S3.

Table 6: NIST tests results.

Name of Test		P_{value}	Passed
1. Monobit Frequency		0.7886	**YES**
2. block Frequency		0. 6546	**YES**
3. Runs test		0. 2882	**YES**
4. Test of Longest run of ones in a block		0. 9682	**YES**
5. Test of Binary matrix rank		0. 6982	**YES**
6. Test of Discrete Fourier transform.		0.8688	**YES**
7. Test of Non-overlapping template matching with B=10101101.		0.9364	**YES**
8. Test of Overlapping template matching		0. 4703	**YES**
9. Test of Maurer's universal statistical		0. 5367	**YES**
10. Test of Linear complexity		0. 0549	**YES**
11. Test of Serial 1	Test of Serial 2	0.8961; 0.7669	**YES; YES**
12. Test of approximate entropy		0.3554	**YES**
13. Test of cumulative sums		0.9269	**YES**
14. Test of Random excursions with x = -4		0.6265	**YES**
15. Test of Random excursions variants with x = -9		0.3001	**YES**

Besides this, the generated sequences should have good statistical characteristics to resist different statistical attacks. For proving the randomness of the

PRNG, we employed NIST suite test (SP 800-22). This test is producing an output P_{value}. The values of P_{value} must be larger than 0.01 to successfully pass the test [41]. Table 6 lists results of the statistical methods of this test. It can be seen that the generated sequences successfully passed all these tests. The results demonstrate that the generated encryption keys based on the proposed PRNG have excellent randomness properties and can resist statistical attacks.

4.6   Sensitivity Analysis

As mentioned in Section 3, the PRNG algorithm relies on mixing two chaotic systems. The chaotic maps are famous by their sensitivity to their initial values. Based on this, all these initial values of ZCM and 2D logistic map are selected as secret keys of the proposed cryptosystem. To validate current state regarding the sensitivity in both directions (encryption and decryption), we encrypt two images using two secret keys differ by a single slight change $+10^{-14}$. Finally, we use the difference test to evaluate the pair encrypted images. In the same manner, we decrypt the original encrypted image using two secret keys, differ only by a single slight change $+10^{-14}$ and we present the difference to evaluate the pair decrypted images. The secret key sensitivity analysis for encryption and decryption are shown in Fig. 9 and Fig. 10, respectively.

In particular, we used three secret keys in this test: S2 and S3 are two secret keys that differ only by one bit difference with S1, where S1: [0.2; 0.8; 7; 6; 5; 0.1; 0.9; 1.18], S2: [0.2+10^{-14}; 0.8; 7; 6; 5; 0.1; 0.9; 1.18], and S3: [0.2; 0.8+10^{-14}; 7; 6; 5; 0.1; 0.9; 1.18]. The obtained encrypted images are different due to the key sensitivity property of our scheme, and the decryption is not possible without the correct secret key.

4.7   Key Space Analysis

The key space of a strong encryption cryptosystem should not be less than 2^{100} [19]. In this test, we affirmed that all the initial values of 2D logistic map and ZCM are chosen as secret keys for the cryptosystem. In addition, we decided to choose to test with precision 10^{-14}, though there are some recent evident that
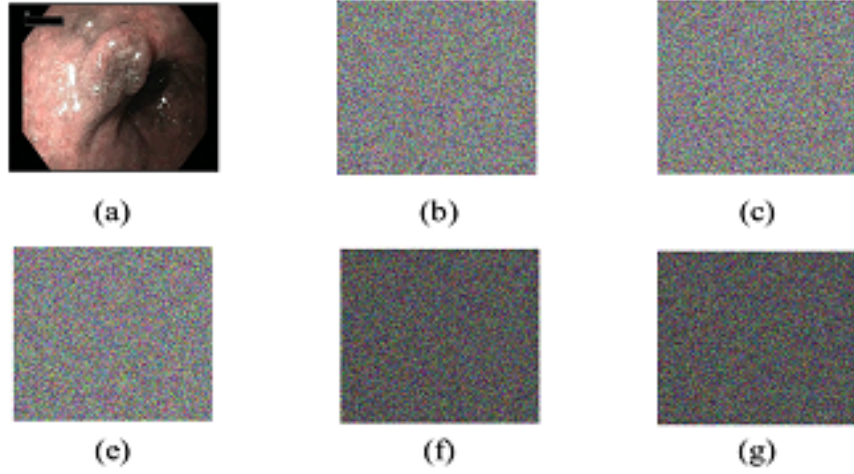
26

Figure 9: Secret key sensitivity analysis. (a) Original keyframe. (b) Encrypted keyframe-using S1. (c) Encrypted keyframe-using S2. (d) Encrypted keyframe-using S3. (e) The difference image (C1–C2). (f) The difference image (C1–C3).
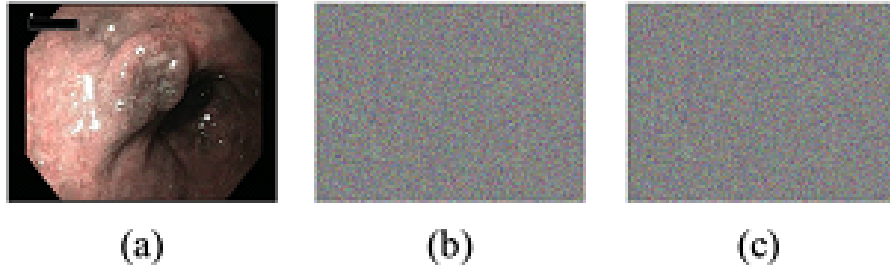

Figure 10: Key sensitivity analysis at the decryption stage. (a) Decrypted image using the correct secret key S1. (b) Decrypted image using the secret key S2. (c) Decrypted image using the secret key S3.

the computational precision of the 64-bit double-precision numbers could be around 10^{-15} [5]. Thus, the space keys in our proposed chaos-based PRNG can be computed with more than $10^{814} \sim = 2^{372}$. Therefore, the proposed encryption cryptosystem can guarantee the resistance against the exhaustive attacks.

4.8 Image Quality Analysis

In this test, we investigate the performance of the proposed cryptosystem using several image quality analysis and metrics. The measurements include mean square error (MSE), peak signal to noise ratio (PSNR), structural similarity index metric (SSIM), and NCC [50]. The decrypted image should have a good quality, which means PSNR value should be high (> 30 dB) [8]. The equations of the three metrics (PSNR, MSE, SSIM, and NCC) are given in Equations 15-18 as follows:

$$MSE = \frac{1}{MN} \sum_{x=1}^{M} \sum_{y=1}^{N} (I_{xy} - E_{xy})^2 \tag{15}$$

$$PSNR = \frac{10 \log_{10} (255)^2}{\sqrt{MSE}} \tag{16}$$

$$NCC = \frac{\sum_{x=1}^{M} \sum_{y=1}^{N} (E_{xy} \times I_{xy})}{\sum_{x=1}^{M} \sum_{y=1}^{N} (E_{xy})^2} \tag{17}$$

$$SSIM = \frac{(2\mu_x\mu_y + c_1) \times (2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1) \times (\sigma_x^2 + \sigma_y^2 + c_2)} \tag{18}$$

In these equations, the keyframe is denoted as "I", the encrypted image is denoted as "J", and x and y are loop counters. The image dimension are presented using M and N (height and width). For better performance, the PSNR score should be at least greater than 30 dB and the MSE should be as minimum as possible. For SSIM and NCC, the scores should be closer to one [30, 31]. Table 7 shows that the decrypted image has good quality and good features compared to other methods [14, 23]. Herein, we use the reported image quality results of the decrypted images with a color image from [51]. The comparative results

with [14, 23] are shown in Table 8, confirming the better performance of our scheme.

Table 7: Decrypted keyframe quality tests

Image	NCC	SSIM	MSE	PSNR
Keyframe Fig. 2 (a1)	1	0.9991	0.0110	67.7270
Keyframe Fig. 2 (a2)	1	0.9981	0.0213	64.8506
Keyframe Fig. 2 (a3)	1	0.9995	0.0065	70.0143
Keyframe Fig. 2 (a4)	1	0.9998	0.0028	73.5965

Table 8: Comparison of decrypted keyframe's quality with other schemes.

	Our Algorithm	[14]		[23]	
Image	Fig. 2 (a4)	Baboon	Lena	Baboon	Lena
MSE	0.0028	8.1486	11.5899	0.4037	0.6041
PSNR	73.5965	39.02	37.49	52.07	50.32

Furthermore, we tested the ability of resisting data lost attacks on the encrypted images. The encrypted keyframes could lose some of their pixels during transmission, especially with real-time processing. Therefore, a cryptosystem should not be affected by losing some encryption pixels for reconstructing the original image from the encrypted image. The goal is to make sure that the reconstruction from the modified encrypted image should be possible with certain quality of the keyframe. Fig. 11 shows the result of pixels loss attack with different ratios of the lost (Fig. 11a: 0.0833%, Fig. 11.b: 0.3333%, Fig. 11.c: 1.3333%). As shown, the proposed algorithm can resist losing 1.3333% of its pixels during the transmission, and the reconstructed image will visually appear the same enough.

4.9 Time and Performance Analysis

To analyze the performance of our encryption scheme, we analyzed the time consumed to encrypt different keyframes and compared its running time with the time needed by the other schemes [6, 19, 55]. The proposed cryptosystem takes
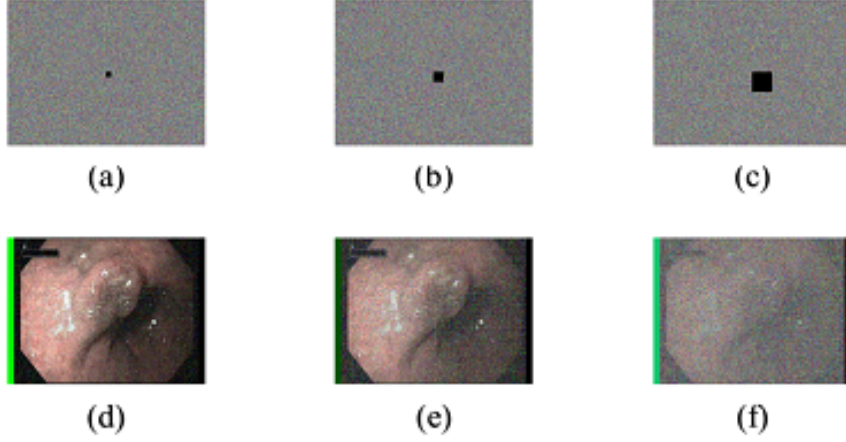
Figure 11: Data lost attack. (a) Cutting a square of [16, 16] pixel from each RGB channels of the encrypted image. (b) Cutting a square of [32, 32] pixel from each RGB channels of the encrypted image. (f) Cutting a square of [64, 64] pixel from each RGB channels of the encrypted image. (d) The decrypted image for (a) image. (e) The decrypted image for (b) image. (f) The decrypted image for (c) image.

around 0.95 seconds to complete the whole encryption or decryption processes for a keyframe of size $[640{\times}480{\times}3]$ pixels. For performance evaluation and comparison analysis, we considered some studies where the encryption time for their methods for digital images is reported [6, 7, 19, 52, 55, 58] as shown in Table 9. The results confirm the high speed of the proposed cryptosystem compared to other methods.

Table 9: Encryption speed (KB/Sec) comparison

Algorithm	Encryption
The proposed scheme	970
Belazi et al. [6]	167
Belazi et al. [7]	4.17
Hamza et al. [19]	205
Wu et al. [52]	5.12
Yao et al. [55]	437.75
Zhou et al. [58]	22.5

4.10   Comparison with Existing Works

The comparison test is a valuable test in order to demonstrate the overall efficiency of the proposed cryptosystem compared to other state-of-art cryptosystems especially to ensure a high-grade suitability for real-time applications. We carried out several comparison tests as shown in previous sub-sections. The results demonstrated that our cryptosystem has excellent performance compared to the existing works [6, 14, 19, 23, 35, 47, 55, 57]. In this part of work, we expand the comparison tests based on several experimental analysis to highlight the superiority of our cryptosystem compared to other state-of-the-art encryption schemes. Table 10 shows that the proposed cryptosystem is as effective as others are in various analysis terms. However, the encryption speed of our cryptosystem is better than the other algorithms in Table 9 and Table 10. Furthermore, the proposal in this work has larger space key, demonstrating the capability of the proposed cryptosystem to resist against well-known attacks effectively as shown in Table 10. Another motivational and major benefit of using our cryptosystem is the ability of real implementations by an integrated circuit such as a field-programmable gate array (FPGA), especially throughput Finite Field multipliers [54]. Considering this superiority, the proposed cryptosystem can guarantee the privacy and security of patients during WCE work.

Table 10: Comparison analysis based on several analysis metrics.

Method	Image Size	Key space	SpeedAnalysis	NPCR & UACI Analysis		SensitivityAnalysis
Proposed	[640,480,3]	2^{372}	0.95/0.96 s	99.609	33.465	Yes
[7]	[1024,1024,1]	2^{624}	2.51/2.51 s	99.617	33.669	Yes
[19]	[256,256,1]	2^{711}	0.32/0.31	99.61	33.50	Yes
[47]	[256,256,3]	2^{233}	-	99.217	33.405	Yes
[52]	[640,480,3]	2^{256}	179.8/180.0 s	99.619	33.477	Yes
[58]	[640,480,3]	2^{256}	40.96/41.08 s	99.606	44.486	Yes

5   Conclusion and Future Work

In this paper, we proposed a secure and fast image cryptosystem to protect the privacy of patients. The proposed cryptosystem ensures the privacy and security of medical data during its dissemination to healthcare centers. This cryptosystem contains a new PRNG algorithm, which adopts two chaotic maps. The proposed PRNG relies on mixing and cascading the orbits of two of the 2D chaotic maps and produce the encryption keys for the cryptosystem algorithm. The proposed cryptosystem employed a block symmetric encryption algorithm based on one round of confusion and diffusion operations. In addition, the proposed cryptosystem employed the border of keyframes to embed noise (random) numbers without affecting the visual quality of decrypted image. The performance of our cryptosystem is excellent and can effectively resist various attacks including differential, statistical, and exhaustive attacks for finding secret keys. Through extensive experimental results and security analysis, we found that the proposed cryptosystem is fast and more secure compared to state-of-the-art schemes. The proposed cryptosystem keeps the confidentiality of the medical information of keyframes. This maintains the privacy of the patients and manages to reduce the energy, communication bandwidth, specialist analysis time, and searching efforts during the WCE procedure. In the future, we aim to explore access control mechanisms for WCE and homomorphic encryption schemes to

further improve the efficiency of our cryptosystem and open new directions to this field of research.

6 Acknowledgement

7 References

[1] A. Gutub, N. Al-Juaid, E. Khan, Counting-based secret sharing technique for multimedia applications, Multimedia Tools and Applications (2017) 1–29.

[2] N. A Al-Juaid, A. A Gutub, E. A Khan, Enhancing pc data security via combining rsa cryptography and video based steganography, Journal of Information Security and Cybercrimes Research 1 (2018) 8–18.

[3] N. Alassaf, B. Alkazemi, A. Gutub, Applicable light-weight cryptography to secure medical data in iot systems, Journal of Research in Engineering and Applied Scie nces (JREAS) 2, No. 2.

[4] N. A. Al-Otaibi, A. A. Gutub, 2-leyer security system for hiding sensitive text data on personal computers, Lecture Notes on Information Theory 2 (2) (2014) 151–157.

[5] N. A. Al-Otaibi, A. A. Gutub, Flexible stego-system for hiding text in images of personal computers based on user security priority, in: Proceedings of 2014 International Conference on Advanced Engineering Technologies (AET-2014), 2014, pp. 250–256.

[6] D. H. Bailey, High-precision floating-point arithmetic in scientific computation, Computing in science & engineering 7 (3) (2005) 54–61.

[7] A. Belazi, A. A. A. El-Latif, S. Belghith, A novel image encryption scheme based on substitution-permutation network and chaos, Signal Processing 128 (2016) 155–170.

[8] A. Belazi, M. Khan, A. A. A. El-Latif, S. Belghith, Efficient cryptosystem approaches: S-boxes and permutationsubstitution-based encryption, Nonlinear Dynamics (2016) 1–25.

[9] L. Chih-Yang, C.-C. Chang, W. Yu-Zheng, Reversible steganographic method with high payload for jpeg images, IEICE transactions on information and systems 91 (3) (2008) 836–845.

[10] Den Zhuo Wei; Zheng Yan; Swee Won Lo; Yongdong Wu; Yanjiang Yang; Robert H., Security of Scalable Video Coding: Encryption and Authentication, CRC Press, Taylor and Francis Group., 2018.

[11] W. Ding, Z. Yan, R. Deng, Privacy-preserving data processing with flexible access control, IEEE Transactions on Dependable and Secure Computing.`doi:10.1109/TDSC.2017.2786247`.

[12] W. Ding, Z. Yan, R. H. Deng, Encrypted data processing with homomorphic re-encryption, Information Sciences 409 (2017) 35–55.

[13] C. Fu, J.-j. Chen, H. Zou, W.-h. Meng, Y.-f. Zhan, Y.-w. Yu, A chaos-based digital image encryption scheme with an improved diffusion strategy, Optics Express 20 (3) (2012) 2363–2378.

[14] K. Gupta, S. Silakari, Novel approach for fast compressed hybrid color image cryptosystem, Advances in Engineering Software 49 (2012) 29–42.

[15] A. A.-A. Gutub, F. A.-A. Khan, Hybrid crypto hardware utilizing symmetric-key and public-key cryptosystems, in: Advanced Computer Science Applications and Technologies (ACSAT), 2012 International Conference on, IEEE, pp. 116–121.

[16] R. Hamza, A novel pseudo random sequence generator for image-cryptographic applications., Journal of Information Security and Applications 35 (2017) 119–127.

[17] R. Hamza, K. Muhammad, Z. Lv, F. Titouna, Secure video summarization framework for personalized wireless capsule endoscopy., Pervasive and Mobile Computing 41 (2017) 436–450.

[18] R. Hamza, K. Muhammad, A. Nachiappan, G. R. Gonzlez, Hash based encryption for keyframes of diagnostic hysteroscopy., IEEE Access PP (99) (2017) 1–1. doi:10.1109/ACCESS.2017.2762405.

[19] R. Hamza, F. Titouna, A novel sensitive image encryption algorithm based on the zaslavsky chaotic map., Information Security Journal: A Global Perspective (2016) 1–18.

[20] H. Hu, L. Liu, N. Ding, Pseudorandom sequence generator based on the chen chaotic system, Computer Physics Communications 184 (3) (2013) 765–768.

[21] Z. Hua, Y. Zhou, Image encryption using 2d logistic-adjusted-sine map, Information Sciences 339 (2016) 237–253.

[22] C. Huang, H. Nien, Multi chaotic systems based pixel shuffle for image encryption, Optics Communications 282 (11) (2009) 2123–2127.

[23] C. Jin, Z. Tu, A Novel Color Image Encryption Algorithm Using Chaotic Map and Improved RC4, Springer, 2016, pp. 3–14.

[24] S. Li, G. Chen, X. Mou, On the dynamical degradation of digital piecewise linear chaotic maps, International Journal of Bifurcation and Chaos 15 (10) (2005) 3119–3151.

[25] Y. Liu, Y. Luo, S. Song, L. Cao, J. Liu, J. Harkin, Counteracting dynamical degradation of digital chaotic chebyshev map via perturbation, International Journal of Bifurcation and Chaos 27 (03) (2017) 1750033.

[26] Y. Luo, L. Cao, S. Qiu, H. Lin, J. Harkin, J. Liu, A chaotic map-control-based and the plain image-related cryptosystem, Nonlinear Dynamics 83 (4) (2016) 2293–2310.

[27] K. Muhammad, J. Ahmad, N. U. Rehman, Z. Jan, M. Sajjad, Cisska-lsb: color image steganography using stego key-directed adaptive lsb substitution method, Multimedia Tools and Applications (2016) 1–30.

[28] K. Muhammad, J. Ahmad, M. Sajjad, S. W. Baik, Visual saliency models for summarization of diagnostic hysteroscopy videos in healthcare systems, SpringerPlus 5 (1) (2016) 1495.

[29] K. Muhammad, R. Hamza, J. Ahmad, J. Lloret, H. Wang, S. W. Baik, Secure surveillance framework for iot systems using probabilistic image encryption, IEEE Transactions on Industrial Informatics 14 (8) (2018) 3679–3689.

[30] K. Muhammad, M. Sajjad, S. W. Baik, Dual-level security based cyclic18 steganographic method and its application for secure transmission of keyframes during wireless capsule endoscopy, Journal of medical systems 40 (5) (2016) 1–16.

[31] Image steganography using uncorrelated color space and its application for security of visual contents in online social networks, Future Generation Computer Systems 86 (2018) 951 – 960.

[32] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, S. W. Baik, A novel magic lsb substitution method (m-lsb-sm) using multi-level encryption and achromatic component of an image, Multimedia Tools and Applications 75 (22) (2016) 14867–14893.

[33] A. Mulla, J. Baviskar, S. Wagh, N. Kudu, A. Baviskar, Probabilistic triangular shuffling approach in dwt based image compression scheme, in: Communication, Information & Computing Technology (ICCICT), 2015 International Conference on, IEEE, pp. 1–6.

[34] M. Murillo-Escobar, C. Cruz-Hernndez, L. Cardoza-Avendao, R. Mndez-Ramrez, A novel pseudorandom number generator based on pseudorandomly enhanced logistic map, Nonlinear Dynamics (2016) 1–19.

[35] B. Norouzi, S. Mirzakuchaki, S. M. Seyedzadeh, M. R. Mosavi, A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process, Multimedia tools and applications 71 (3) (2014) 1469–1497.

[36] F. zkaynak, S. Yavuz, Security problems for a pseudorandom sequence generator based on the chen chaotic system, Computer Physics Communications 184 (9) (2013) 2178–2181.

[37] S. Papadimitriou, T. Bountis, S. Mavroudi, A. Bezerianos, A probabilistic symmetric encryption scheme for very fast secure communication based on chaotic systems of difference equations, International Journal of Bifurcation and Chaos 11 (12) (2001) 3107–3115.

[38] N. K. Pareek, V. Patidar, K. K. Sud, Image encryption using chaotic logistic map, Image and Vision Computing 24 (9) (2006) 926–934.

[39] Ramakrishnan, Cryptographic and Information Security: Approaches for Images and Videos, CRC Press LLC, 2018.

[40] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, A statistical test suite for random and pseudorandom number generators for cryptographic applications, Report, DTIC Document (2001).

[41] K. R. Sekhar, T. R. Chandra, S. Pooja, S. Tapaswi, Light weight security protocol for communications in vehicular networks, Wireless Networks 22 (4) (2016) 1343–1353.

[42] C. E. Shannon, A mathematical theory of communication, ACM SIGMOBILE Mobile Computing and Communications Review 5 (1) (2001) 3–55.

[43] Y. Shin, J. Hur, Scalable and efficient approach for secure group communication using proxy cryptography, Wireless Networks 18 (4) (2012) 413–425.

[44] A. Wang, S. Banerjee, B. A. Barth, Y. M. Bhat, S. Chauhan, K. T. Gottlieb, V. Konda, J. T. Maple, F. Murad, P. R. Pfau, Wireless capsule endoscopy, Gastrointestinal endoscopy 78 (6) (2013) 805–815.

[45] X.-y. Wang, X.-m. Bao, A novel block cryptosystem based on the coupled chaotic map lattice, Nonlinear Dynamics 72 (4) (2013) 707–715.

[46] X. Wei, L. Guo, Q. Zhang, J. Zhang, S. Lian, A novel color image encryption algorithm based on dna sequence operation and hyper-chaotic system, Journal of Systems and Software 85 (2) (2012) 290–299.

[47] Z. Wei, Y. Wu, Y. Yang, Z. Yan, Q. Pei, Y. Xie, J. Weng, Autoprivacy: Automatic privacy protection and tagging suggestion for mobile social photo, Computers & Security.doi:https://doi.org/10.1016/j.cose.2017.12.002.

[48] Z. Wei, Z. Yan, Y. Wu, R. H. Deng, Trustworthy authentication on scalable surveillance video with background model support, ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM) 12 (4s) (2016) 64.

[49] H. Wu, H. Wang, H. Zhao, X. Yu, Multi-layer assignment steganography using graph-theoretic approach, Multimedia Tools and Applications 74 (18) (2015) 8171–8196.

[50] X. Wu, D. Wang, J. Kurths, H. Kan, A novel lossless color image encryption scheme using 2d dwt and 6d hyperchaotic system, Information Sciences 349 (2016) 137–153.

[51] Y. Wu, J. P. Noonan, S. Agaian, Npcr and uaci randomness tests for image encryption, Cyber journals: multidisciplinary journals in science and technology, Journal of Selected Areas in Telecommunications (JSAT) (2011) 31–38.

[52] Y. Wu, G. Yang, H. Jin, J. P. Noonan, Image encryption using the two-dimensional logistic chaotic map, Journal of Electronic Imaging 21 (1) (2012) 013014–1–013014–15.

[53] J. Xie, P. K. Meher, Z.-H. Mao, High-throughput finite field multipliers using redundant basis for fpga and asic implementations, IEEE Transactions on Circuits and Systems I: Regular Papers 62 (1) (2015) 110–119.

[54] W. Yao, F. Wu, X. Zhang, Z. Zheng, Z. Wang, W. Wang, W. Qiu, A fast color image encryption algorithm using 4-pixel feistel structure, PloS one 11 (11) (2016) e0165937.

[55] G. Zhang, Q. Liu, A novel image encryption method based on total shuffling scheme, Optics Communications 284 (12) (2011) 2775–2780.

[56] S. Zhou, Z. Wei, B. Wang, X. Zheng, C. Zhou, Q. Zhang, Encryption method based on a new secret key algorithm for color images, AEU - International Journal of Electronics and Communications 70 (1) (2016) 1–7.

[57] Y. Zhou, Z. Hua, C.-M. Pun, C. P. Chen, Cascade chaotic system with applications, IEEE transactions on cybernetics 45 (9) (2015) 2001–2012.