IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

SPECIAL SECTION ON RECENT ADVANCES IN COMPUTATIONAL INTELLIGENCE PARADIGMS FOR SECURITY AND PRIVACY FOR FOG AND MOBILE EDGE COMPUTING

Received August 21, 2017, accepted October 3, 2017, date of publication November 29, 2017, date of current version November 8, 2018.

*Digital Object Identifier 10.1109/ACCESS.2017.2762405*

# Hash Based Encryption for Keyframes of Diagnostic Hysteroscopy

**RAFIK HAMZA[1], KHAN MUHAMMAD[2,3], (Student Member, IEEE), ARUNKUMAR N[4], AND GUSTAVO RAMÍREZ-GONZÁLEZ[5]**

[1]LAMIE Laboratory, Department of Computer Science, University of Batna 2, Batna 05078, Algeria
[2]Intelligent Media Laboratory, College of Software Convergence and Technology, Sejong University, Seoul 143-747, South Korea
[3]Digital Image Processing Laboratory, Department of Computer Science, Islamia College, Peshawar 25000, Pakistan
[4]School of Electrical and Electronics Engineering, SASTRA University, Thanjavur 613401, India
[5]Department of Telematics, University de Cauca, Popayan 143-747, Colombia

Corresponding author: Gustavo Ramírez-González (gramirez@unicauca.edu.co)

**ABSTRACT** In this paper, we address the problem of confidentiality of keyframes, which are extracted from diagnostic hysteroscopy data using video summarization. We propose an image color coding method aimed at increasing the security of keyframes extracted from diagnostic hysteroscopy videos. In this regard, we use a 2-D logistic map to generate the cryptographic keys sequences, which relies on mixing and cascading the orbits of the chaotic map in order to generate the stream keys for the encryption algorithm. The encrypted images produced by our proposed algorithm exhibit randomness behavior, providing a high-level of security for the keyframes against various attacks. The experimental results and security analysis from different perspectives verify the superior security and high efficiency of our proposed encryption scheme compared to other state-of-the-art image encryption algorithms. Furthermore, the proposed method can be combined with mobile-cloud environments and can be generalized to ensure the security of cloud contents as well as important data during transmission.

**INDEX TERMS** Image encryption, 2D chaotic map, diagnostic hysteroscopy, cloud content security.

## I. INTRODUCTION

Recently, captured medical data has become increasingly widespread due to advancements in technology such as wireless capsule endoscopy (WCE) [1]. Generally, medical data is collected from patients and transmitted to healthcare centers to enable doctors to make appropriate decisions and help them communicate more effectively. This data is very sensitive and vulnerable to many menace with security issues over the Internet. As a result, confidentiality of medical data has become an increasingly major concern over the last decade as hackers have gained considerable influence. Thus, it is extremely necessary to ensure the security and privacy of this data during transmission. In this regard, encryption can present a solution that can secure the privacy of this specific data [1], [2].

The most important and popular issue with cloud service is data privacy [3]. Hence, encrypting data and sending it to the cloud can ensure data security and user privacy [4]. Herein, medical images could have some scientific and industrial applications, making it more important using the cloud system. This led researchers to produce numerous image encryption methods with various techniques such as chaos [5], DNA [6], and so on. This is mainly due to the fact that encryption is the main mechanism to ensure privacy for digital images during transmission. Yet some works lack an equilibrium between good results with a satisfactory level of security while keeping computational complexity at a reasonable level. This is a challenging issue especially with the transmission of medical images for real-time applications.

Predominantly, users attempt to outsource their data to a heterogeneous environment for storage and processing especially in the cloud system [7]. Cloud storage should preserve the privacy of data holders by proposing encryption schemes. In this regard, researchers attempted to provide some solutions to ensure data confidentiality [8], [9]. For instance, Yan *et al.* [4] proposed an effective approach to verify data ownership between big data in the cloud and check for duplicate storage. Commonly, nonlinear systems have been employed in digital image encryption [10], [11]. In fact, chaotic maps are used ordinarily in generating the encryption keys for the cipher structure [12], or for key generation from wireless channels [13]. Hamza *et al.* [14]

presented a good use of the Zaslavsky chaotic map without any use of finite computations. The authors in [14] employed the mentioned chaotic map in their symmetric image cipher which ensures digital images security. Subsequently, Hamza *et al.* [15] proposed a secure framework for the extraction of diagnostically informative frames from the wireless capsule endoscopy video data for outdoor patients undergoing the WCE procedure. To this end, they have combined a video summarization technique [16] with an image encryption scheme [14] to ensure the security of keyframes during their transmission to healthcare centers. However, the main issue of [14] and [15] is the selection of the secret keys which is created with real numbers, often with number-strings fifteen digits long. Indeed, this is the case with many chaotic-encryption schemes where the selected secret key is always a set of real numbers. This might not be applicable for direct implementation with cloud-based applications.

In this paper, we propose a fast RGB image encryption method for the extracted keyframes from diagnostic hysteroscopy. Here, we have changed the cryptographic keys generator in our recent works [14], [15]. Furthermore, we have adjusted the cipher structure to increase the convenience for real-time transactions in terms of time and security measures. The secret keys could be formed of anything digital, such as a picture file or text file, pdf file, or just a traditional password. Security analyses show that the proposed cryptosystem can ensure the confidentiality of the extracted keyframes with reasonable computational complexity. Further, the results from the security analysis and tests demonstrate that the proposed algorithm can withstand various attacks. In addition, the proposed image encryption method can be more generally employed for various types of digital images. Furthermore, the implementation of our proposed cryptosystem is easy considering the number of steps and rounds of encryption required.

The rest of the paper is organized as follows: Section 2 highlights the key embodiments of the proposed work. Security analysis and experimental results are given in Section 3, followed by the conclusion and future work plans in Section 4.

## II. THE PROPOSED CRYPTOSYSTEM

Our cryptosystem consists of three main steps: an initial setup for keys generation, encryption of keyframes, and the decryption process to get the actual keyframes. The details of these three steps are provided in the sub-sequent sub-sections.

### A. SETUP PROCESSES

A hash function (HF) is a diversion that reduces an input of arbitrary length to a fixed length which is called the hash value. In our work, the secret key is setup using the SHA-256 hash function. The initial source is hashed to ensure maximum sensibility, and the output value of the hash function is setup to produce the initial values for the chaotic system to generate the cryptographic keys for the proposed image encryption algorithm.

Recently, many studies have proved that the key space of an encryption scheme should be larger than $2^{128}$ to resist the exhaustive attacks [14]. In this work, regardless of the length of the input for the hash function, we have the secret keyspace as 32 bytes (256 bits) which is employed to generate the initial values of the chaotic map. The generation processes of the initial states for the 2D-logistic map are shown in Algorithm 1. In our previous works [14], [15], we have used Zaslavsky chaotic map to generate appropriate encryption keys for the cipher algorithm. However, in the current work, we intend to change the chaotic map to another more secure and less complicated map (compared to the number of operations needed for initialization of the Zaslavsky chaotic map) while keeping the steps needed to generate the invertible matrices K and L under the finite field arithmetic.

**Algorithm 1** Initialization of Secret Keys

```
Input: Sec
$x = \sum_{i=1}^{16} \mathrm{Sec} / \sum_{i=1}^{32} \mathrm{Sec}$, $y = \sum_{i=17}^{32} \mathrm{Sec} / \sum_{i=1}^{32} \mathrm{Sec}$
  if Sec(1) < 32
      r = 1.11 + abs(x-round(x,2)) + abs(y-round(y,2))
  Elseif Sec(1) >= 32 And Sec(1) < 64
      r = 1.12 + abs(x-round(x,2)) + abs(y-round(y,2))
  Elseif Sec(1) >= 64 And Sec(1) < 96;
      r = 1.13 + abs(x-round(x,2)) + abs(y-round(y,2))
  Elseif Sec(1) >= 96 And Sec(1) < 128
      r = 1.14 + abs(x-round(x,2)) + abs(y-round(y,2))
  Elseif Sec(1) >= 128 And Sec(1) < 160
      r = 1.15 + abs(x-round(x,2)) + abs(y-round(y,2))
  Elseif Sec(1) >= 160 And Sec(1) < 192
      r = 1.16 + abs(x-round(x,2)) + abs(y-round(y,2))
  Elseif Sec(1) >= 192
      r = 1.17 + abs(x-round(x,2)) + abs(y-round(y,2))
  End
Output: $x, y, r$.
```

The 2D logistic map is a discrete dynamic system with chaotic behavior of the evolution of orbits and attractors [17]. It has more complex behavior than one dimensional chaotic behavior. This non-invertible two-dimensional map is denoted using Equation (1) as follows:

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

Herein, the parameter of the system is denoted by 'r', the 2D logistic system is chaotic if "r" is within the interval [1.1-1.19] [11], [17]. Similar to many chaotic maps, this map also depends on the initial conditions $(x_0, y_0)$ and the parameter "r" to determine its trajectory. The generated sequences from this map should be completely chaotic, where the Lyapunov spectrum is 3.68, and for large set of the initial values according to previous research [17], which shows another reason for changing the chaotic map used in our previous works [14], [15]. From this discussion, we can

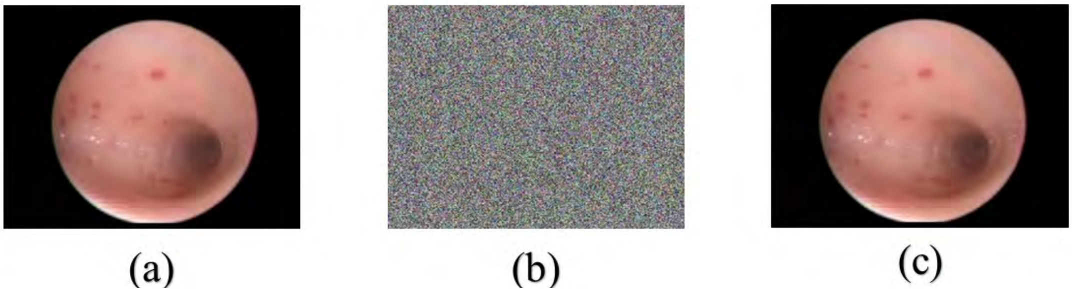


**FIGURE 1.** Visual test of original keyframe and its corresponding encrypted and decrypted keyframes.

say that the output sequences of the 2D logistic system are completely chaotic, unpredictable, and secure to employ in the PRNG.

**Algorithm 2** The Pseudo Keys

```
Input: File source, and $K_{in}$.
1: Sec $\leftarrow$ $HF$ ($Source$)
2 : $[\text{x,y,r}] \leftarrow$ Algorithm 1 ($Sec$)
3 : $Ve \leftarrow Logistic\_map\_2D(x, y, r)$
4: S1 $\leftarrow Ve(10 : h + 9)$
5: S2 $\leftarrow Ve(10 : w \times e + 9)$
6: $S3 \leftarrow reshape\ (Ve\ (10 : 1024 + 9),\ 32,\ 32)$
7: $[\neg, V] \leftarrow Sort(\text{S1}), [\neg, V'] \leftarrow Sort(\text{S2}), [\neg, R] \leftarrow Sort(S3)$.
8: $\alpha = |\sum S1 + \sum S2 + \sum S3| \text{mod } 256$
9: $IF\ \ \alpha = 0\ then$
$\alpha = |\sum S1 + \sum S2 + \sum S3| \text{mod } 255$
End
10: $K \leftarrow \alpha \cdot K_{in}, L \leftarrow K^{-1}$
Output: $V, V', R, \alpha, L, K$.
```

Algorithm 2 shows the steps for generating the encryption keys for our proposed encryption scheme based on source data (denoted as a secret key for the proposed algorithm) and an initial [32, 32] matrix that must be invertible in the finite field. In this pursuit, we use the same matrix $K_{in}$ as used in our previous work [14]. In the beginning, we set up the initial values $(x_0, y_0, r)$ for the chaotic map using Algorithm 1. Then, we generate the random sequences *S1, S2,* and *S3* using the 2D-logistic map by employing Equation 1 as shown in Algorithm 2. The chaotic sequences *S1* and *S2* should have the same representation format as the pixels in plain-keyframe *P* so that these generated sequences could be employed to perform permutation in the subsequent processes. Since the confusion and diffusion operations are manipulated with each block [32, 32], the encryption algorithm can be applied to the digital keyframe of any representation size format with [N*32, M*32], where M and N are integer numbers (Example: [640, 720]). The encrypted keyframe has the same size format of the original keyframe as like as the decrypted keyframe.

### B. ENCRYPTION PROCESS

In this step, the system reads the keyframe as an RGB image, and the obtained matrices are reshaped to one matrix. After that, some random bits are produced using true random number generator. The generated bits sequence should be added (using Bitwise-XOR operation) with the entire keyframe pixels. Note here that the produced bits noise should have the same image size. The tests and analysis demonstrated that adding random bits to the original keyframes can enhance the security level of cipher-keyframes especially against differential attacks. Fig. 1 shows the original keyframe, the encrypted keyframe using our proposed image encryption, and finally the decrypted keyframe. As shown, adding random bits will not affect the visual presentation of the keyframes after decryption of the ciphered keyframe.

The randomized propriety in our proposed framework can ensure that with or without any adjustment of the keyframe pixels, the ciphered keyframes will be completely different for each encryption process. Moreover, any adjustment in the initial values (input) shall completely change the ciphered keyframe too. Thus, the ciphered data will be completely different even with using the same data and same secret keys.

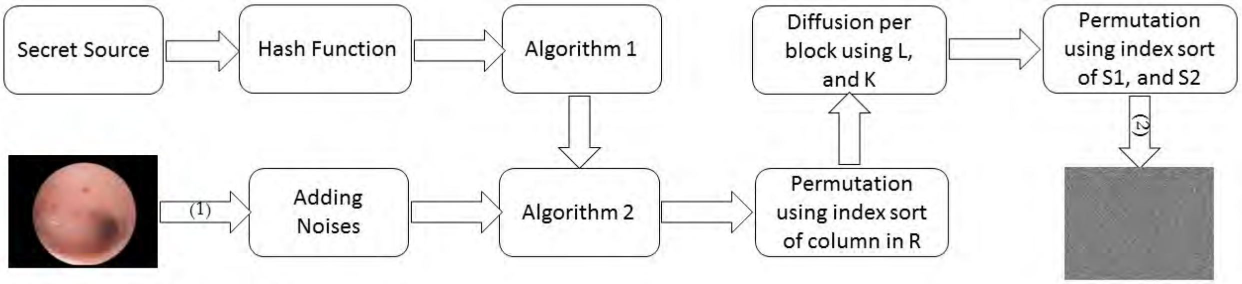
The flowchart of the image encryption scheme is shown in Fig. 2. Basically, the plain-keyframe *P* is transformed from a clear RGB image into a random-like RGB image using only a one-round confusion-permutation process as given in [14].

In the first part, algorithm 1 is used to manufacture the initial values and parameters of the 2D-logistic map based on setup processes of the hash function SHA-256.

In the second part, we apply the permutation-diffusion procedures as follows. First, we shift the obtained matrix for each sub-block [32, 32] using the index sort in columns of the matrix R (refer to step 7 in Algorithm 1). Next, we employ the arithmetic matrix multiplication over finite space GF (256) for each sub-block [32 × 32], denoted as "B" of the obtained matrix as follows.

$$Ciphered\_Step\_Keyframe \leftarrow (L \cdot B.K)_{2^8} \qquad (2)$$

Here, *B* represents a [32 × 32] block from the obtained matrix, where L is the invertible matrix of K over


Secret Source
Hash Function
Algorithm 1
Diffusion per block using L, and K
Permutation using index sort of S1, and S2
(1)
Adding Noises
Algorithm 2
Permutation using index sort of column in R
(2)

(1): Reshape RGB matrices into one matric
(2): Reconstructed the RGB matrices

**FIGURE 2.** Proposed image encryption framework.

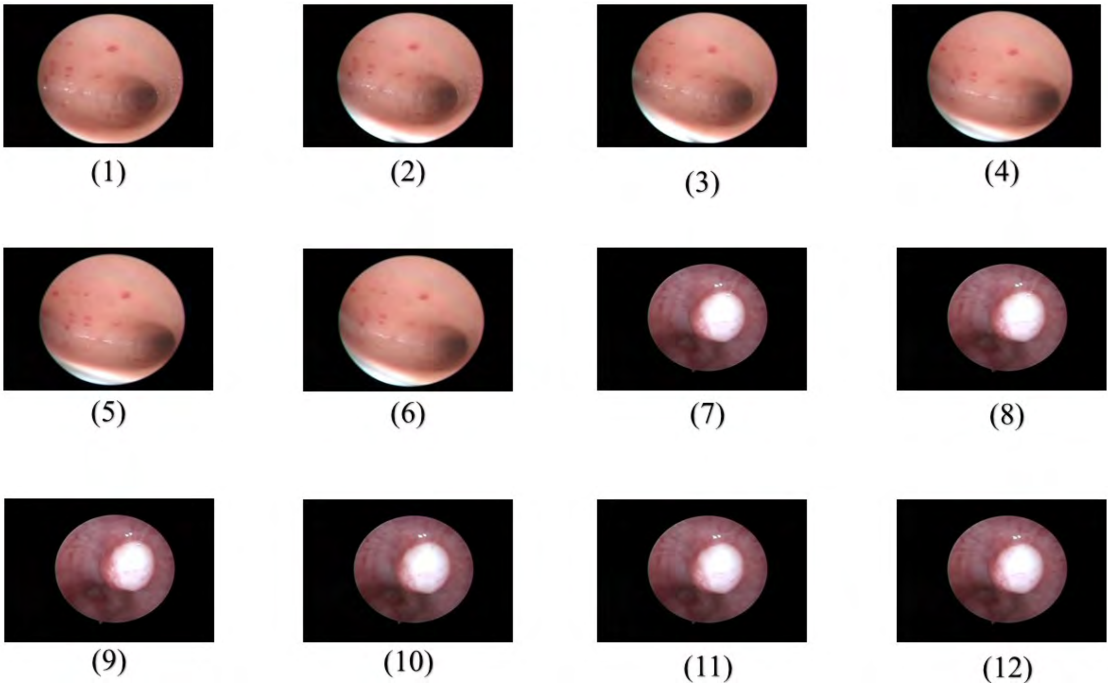


**FIGURE 3.** Illustration of the extracted frames from diagnostic hysteroscopy videos.

the finite field. Next, we shift all pixels using the index sort of the chaotic sequences $S_1$ and $S_2$. Finally, the encrypted keyframe is obtained after reshaping the obtained matrix from the last step into three matrices (RGB image).

### C. DECRYPTION PROCESS

The inverse steps for the encryption processes can recover the visual presentation of the keyframe using an RGB image. It should be noted that the decrypted image can only be recovered by using the secret source/keys. Essentially, each operation in our coding algorithm is reversible. For the arithmetic matrix multiplication over finite space step, we have $L$ as the invertible matrix of $K$, which means that $L \cdot K = Id_{32}$ and $Id_{32}$ is an [32, 32] identical matrix. The reverse operation for Eq. (3) can therefore be reproduced as follows:

$$Decrypted\_Step\_Keyframe \leftarrow (K \cdot B \cdot L)_{2^8} \tag{3}$$

The visual results of applying the encryption-decryption algorithm are shown in Fig. 4 and Fig. 5.

## III. SECURITY ANALYSIS AND RESULTS

In this section, the proposed system is evaluated from various perspectives such as its resistance to common security attacks and the time execution of the cryptosystem. The performance results of the proposed image encryption have been compared with several recent state-of-the-art image

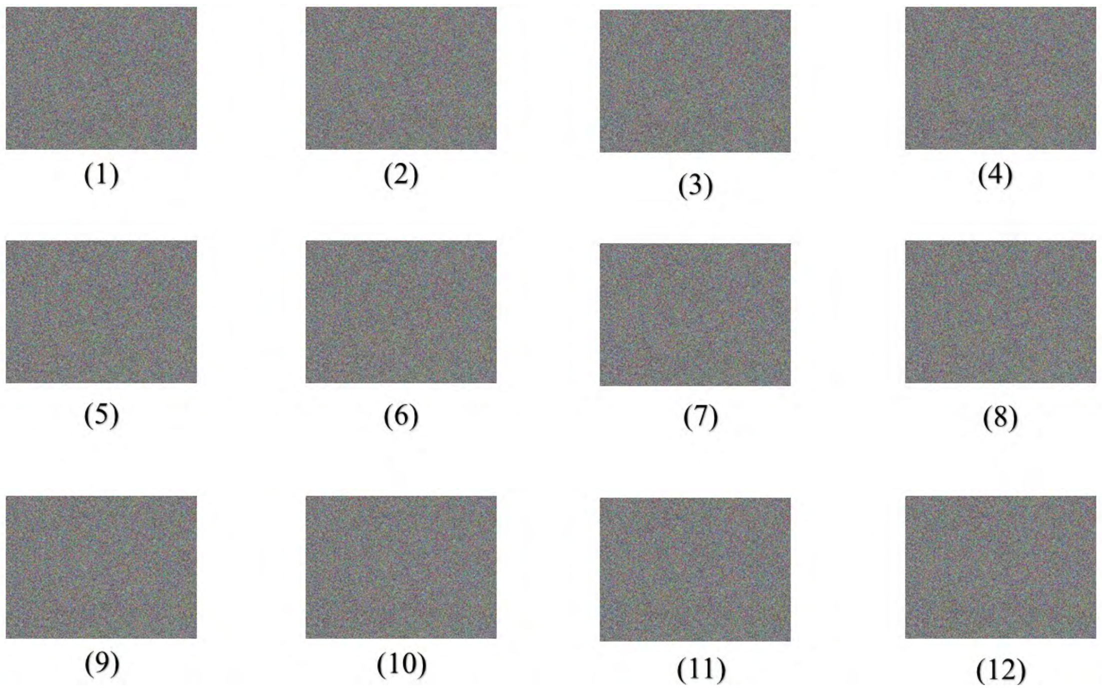


**FIGURE 4.** Encrypted keyframes corresponding to keyframes with numbering identical to Fig. 3.

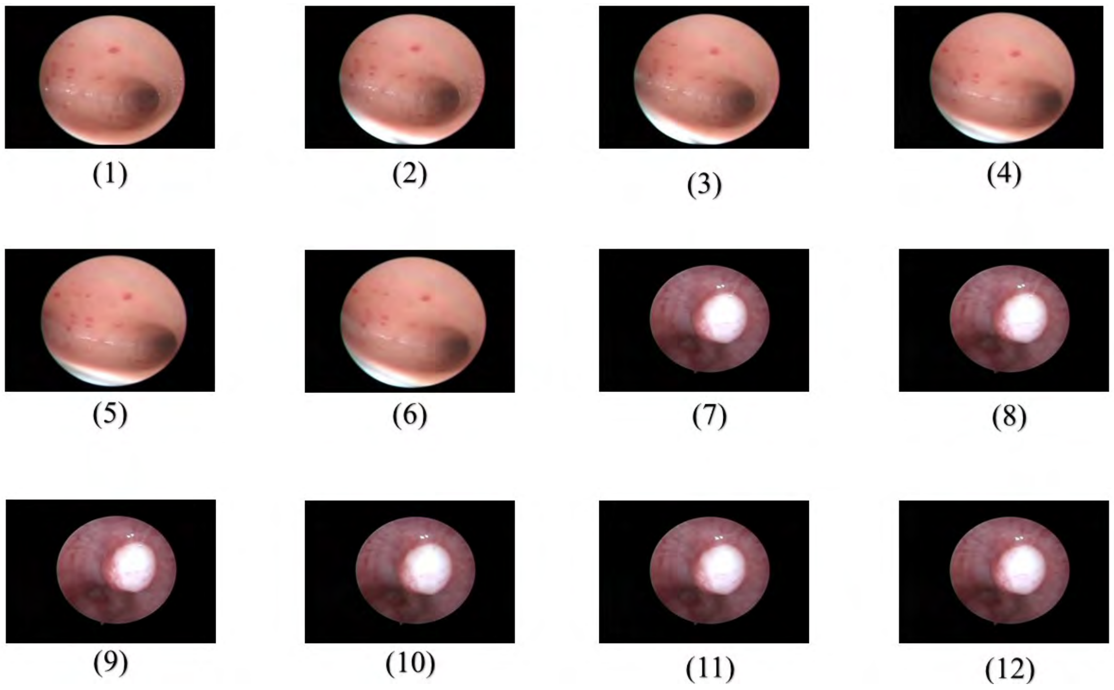


**FIGURE 5.** Decrypted keyframes corresponding to the encrypted keyframes.

encryption methods. A set of examples for the extracted frames from diagnostic hysteroscopy are given in Fig. 3. Keyframe selection is done using our recent work [18], where the selected keyframe is sent to a healthcare center to keep track of the patient and ongoing treatment. In this work, we propose a technique to ensure the transmission of these keyframes, which in turn ensures the confidentiality of this sensitive data.

### A. VISUAL TESTS

The encrypted keyframe should not show any information regarding the original keyframe. In fact, the ciphered

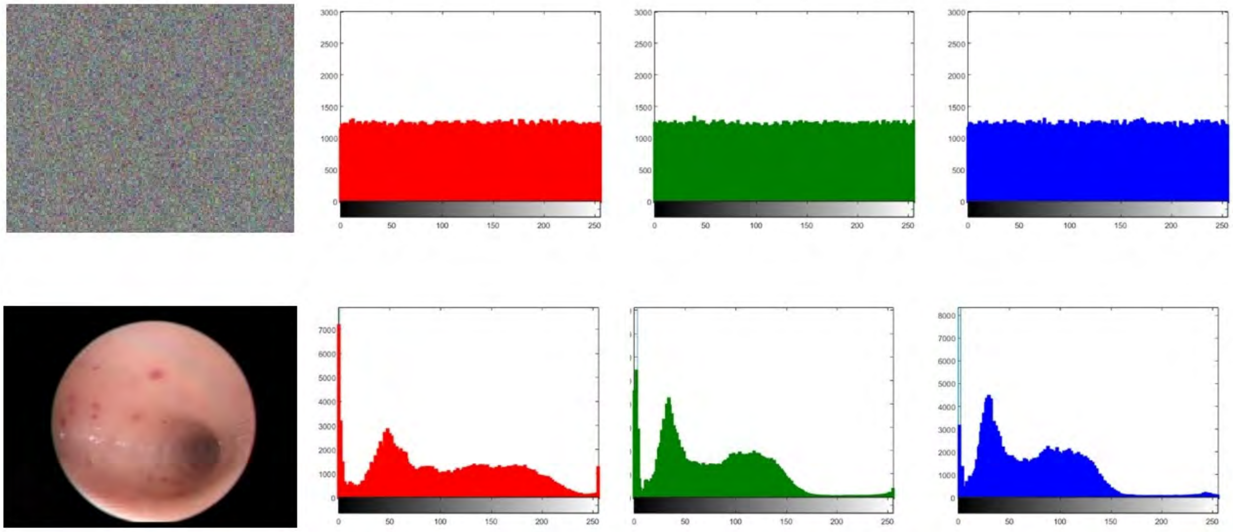


**FIGURE 6.** Histograms of the original keyframe and its corresponding encrypted keyframe in each RGB channel.

keyframe should be similar to random pixels like a true random source. Fig. 3 shows the original keyframes denoted as 1 to 12, while the corresponding encrypted versions are listed with the same number as shown in Fig. 4. Finally, the decrypted keyframes are given in Fig. 5. The visual analysis with various keyframes confirm that there is no information regarding the original keyframes from the encrypted keyframes, except of course the size of the keyframe.

### B. HISTOGRAM TEST

A histogram of an image can be plotted by showing the number of pixels for each tonal value. This description of the distribution of the pixels which could be used to judge the entire tonal distribution. The histogram of an RGB image can be described by its pixel distribution, where it could be plotted by the number of pixels at each color intensity level [19]. In this regard, the histogram of the encrypted image should obey the uniform distribution of pixel values (uniform histogram), which ensures the capability of the cryptosystem to withstand statistical attacks such as a frequency analysis attack. Fig. 6 shows histograms in each RGB channel of a keyframe and its corresponding encrypted keyframe histograms. In the proposed framework, the results of histograms in Fig. 6 demonstrated that the ciphered data have uniform histogram distribution. Indeed, these results confirm our claim that the proposed image encryption can withstand statistical attacks.

### C. PROBABILISTIC ENCRYPTION

The proposed image encryption employed a randomized step to ensure that the cryptosystem is semantically secure. This means that adversary will not be able to collect useful information, even partial information about the original keyframe based on the encrypted keyframe. So, attackers will not be able to obtain any useful information that would allow them to build their cryptanalysis model against the proposed cryptosystem. Indeed, this feature can guarantee high-security level against adversaries attacks.

In this part, we demonstrate that the proposed cryptosystem has probabilistic features. In this regard, we use NPCR and UACI tests to analyse the probabilistic properties of the ciphered images generated from our proposed encryption algorithm. The theoretical value for NPCR is 99.60%, while the theoretical value for NPCR is 33.47% [17]. Also, the mentioned tests can determine the ability of a cryptosystem to resist the differential attacks [41].

NPCR and UACI can be computed as follows:

$$NPCR(C_1, C_2) = \sum_{i,j} \frac{S(i,j)}{D} \times 100\ \% \tag{4}$$

$$UACI(C_1, C_2) = \sum_{i,j} \frac{C_1(i,j) - C_2(i,j)}{255 \times D} \times 100\ \% \tag{5}$$

Where, "$D$" is the number of pixels, and we computed "$S$" using Eq. 6.

$$S(i,j) = \begin{cases} 0, & if\ C_1(i,j) = C_2(i,j) \\ 1, & Elsewise. \end{cases} \tag{6}$$

Herein, we compute the NPCR and UACI scores between two ciphered images C1 and C2. The ciphered images are produced based on our proposed image encryption scheme from the same image I and the same secret source.

The results for this test with different keyframes are listed in Table 1. Our proposed scheme resisted successfully the differential attacks and exceeded all theoretical values for

**TABLE 1.** NPCR and UACI tests results for each RGB channel.

| | Frame 1 | | Frame 5 | | Frame 9 | | Frame 12 | |
|---|---|---|---|---|---|---|---|---|
| | NPCR | UACI | NPCR | UACI | NPCR | UACI | NPCR | UACI |
| R | 99.6881 | 33.3848 | 99.6070 | 33.4251 | 99.6165 | 33.3546 | 99.5987 | 33.5580 |
| G | 99.6288 | 33.4851 | 99.5808 | 33.4013 | 99.6094 | 33.3943 | 99.5739 | 33.3754 |
| B | 99.5819 | 33.4459 | 99.6307 | 33.5713 | 99.6046 | 33.4404 | 99.6106 | 33.3106 |

**TABLE 2.** Comparison of results for the NPCR and UACI tests.

| | Our | [5] | [20] | [21] | [22] | [23] |
|---|---|---|---|---|---|---|
| NPCR | 99.6125 | 99.6177 | 99.2172 | 99.60 | 99.6200 | $> 99$ |
| UACI | 33.4451 | 33.6694 | 33.4058 | 33.40 | 33.5100 | $\cong 33.43$ |

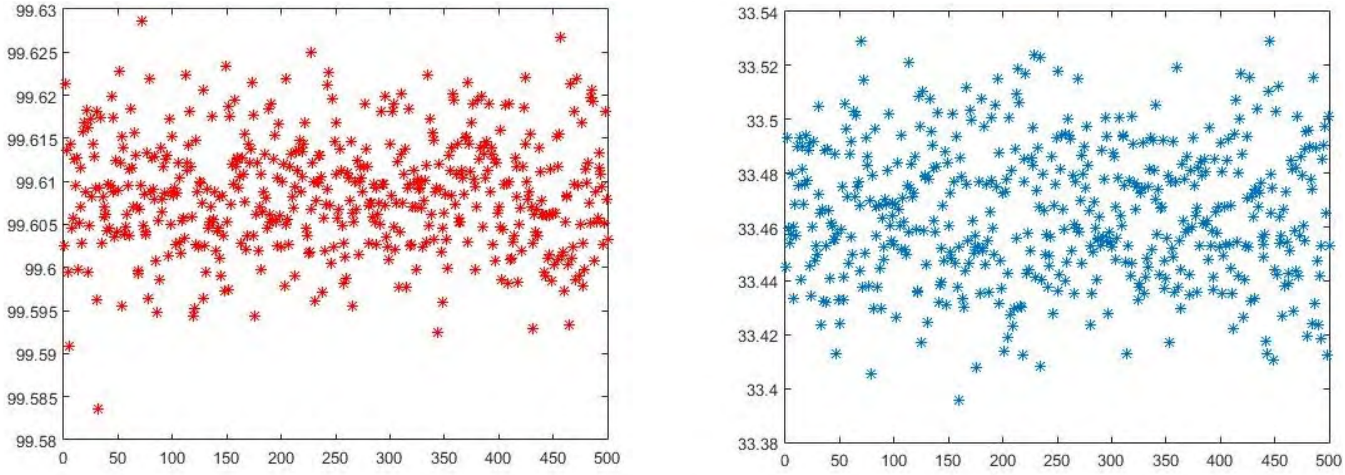


**FIGURE 7.** NPCR and UACI results for 500 repeat tests to evaluate the ability of our algorithm to withstand differential attacks.

NPCR and UACI [17]. In fact, the results demonstrate that the pair of encrypted keyframes are completely different from each other although we used the same data with the same secret key. So, it is clear that each encryption will produce a completely different encrypted data. To add more credibility to our work, we repeated this test with the same steps 500 times for the same keyframe. Fig. 7 shows the results of this test for a keyframe of size [640, 480, 3].

Finally, to enrich our work in this paper, we compared the performances of our proposed algorithm with other recent encryption algorithms as given in Table 2. It should be noted that we use the average result for the three plans (RGB). All results confirm that our proposed image encryption has good performance compared with other recent schemes with strong ability to resist differential attacks.

### D. CORRELATION ANALYSIS

The correlation of two adjacent pixels has been used in many studies as part of the security analysis to prove that the correlation of pixels of an encrypted image is eliminated. In other words, the correlation coefficient of two adjacent pixels in a ciphered keyframe should be almost equal to zero [15], which indicates the ideal result for this test. Here, we test the correlation between two adjacent pixels in the original keyframe and its corresponding encrypted keyframe by randomly selecting 2048 pairs of two-adjacent pixels in diagonal, vertical, and horizontal directions from the original keyframe and its corresponding encrypted keyframe. Next, we compute the correlation coefficient of each pair using the following equations:

$$CC_{xy} = \frac{cov(x, y)}{\sqrt{D(x)} \times D(y)} \tag{7}$$

**TABLE 3.** Correlation coefficient of adjacent pixels tests.

| | Component | Keyframe | | | Ciphered | | |
|---|---|---|---|---|---|---|---|
| | | Horizontal | Vertical | Diagonal | Horizontal | Vertical | Diagonal |
| Keyframe 1 | R | 0. 9995 | 0. 9984 | 0. 9980 | 0.0035 | -0.004 | 5.034e-04 |
| | G | 0. 9994 | 0. 9971 | 0. 9967 | -0.0026 | 0.0044 | 0.0006 |
| | B | 0. 9993 | 0. 9968 | 0. 9963 | 0.0025 | -3.594e-04 | 0.0004 |
| Keyframe 5 | R | 0. 9995 | 0. 9990 | 0. 9987 | -0.0057 | -0.004 | -0.008 |
| | G | 0. 9993 | 0. 9983 | 0. 9981 | 0.003 | 0.003 | 0.004 |
| | B | 0. 9993 | 0. 9981 | 0. 9979 | 0.005 | -0.007 | 0.001 |
| Keyframe 9 | R | 0. 9996 | 0. 9989 | 0. 9986 | 0.0030 | 0.0075 | -0.0053 |
| | G | 0. 9994 | 0. 9980 | 0. 9978 | 0.0063 | -0.0024 | -0.0051 |
| | B | 0. 9993 | 0. 9978 | 0. 9976 | 0.0017 | -0.0023 | -0.0030 |
| Keyframe 12 | R | 0. 9997 | 0. 9991 | 0. 9988 | -0.0010 | 0.0022 | 0.0012 |
| | G | 0. 9995 | 0. 9984 | 0. 9981 | -0.0015 | 0.0016 | -0.0017 |
| | B | 0. 9995 | 0. 9982 | 0. 9979 | 0.0025 | 0.0004 | 0.0003 |

**TABLE 4.** Comparison of various key spaces for different algorithms.

| Algorithm | Our | [22] | [23] | [24] | [17] | [25] |
|---|---|---|---|---|---|---|
| Space Key | $2^{192}$ | $0.25 \times 10^{64}$ | $10^{56}$ | $2^{180}$ | $2^{256}$ | $2^{215}$ |

**TABLE 5.** Encryption and decryption test speed per second for each frame.

| Frame number | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | Moy |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Encryption | 0.75 | 0.83 | 0.85 | 0.80 | 0.81 | 0.75 | 0.78 | 0.75 | 0.87 | 0.79 | 0.79 |
| Decryption | 0.80 | 0.76 | 0.82 | 0.79 | 0.78 | 0.80 | 0.76 | 0.77 | 0.80 | 0.79 | 0.78 |

$$cov(x, y) = \frac{1}{n}\sum_{i=1}^{n}(x_i - E(x))(y_i - E(y)) \qquad (8)$$

$$D(x) = \frac{1}{n}\sum_{i=1}^{n}(x_i - E(x))^2 \qquad (9)$$

$$E(x) = \frac{1}{n}\sum_{i=1}^{n}x_i \qquad (10)$$

The distribution of two adjacent pixels in a keyframe and its corresponding encrypted keyframe in the blue, green, and red channels over horizontal, vertical, and diagonal directions are shown in Fig 8. The visual results show that the plots from the original keyframe varies a lot from the encrypted keyframe. The dots in the original keyframe tend to regroup in the diagonal line while the dots in the encrypted keyframe have good uniform probability distribution as shown in Fig. 8. The numerical results of this test are shown in Table 3, where the correlation coefficient of two adjacent pixels in the ciphered keyframe is almost zero. The results demonstrated that our proposed algorithm successfully eliminates the correlation of pixels, ensuring the ability of our proposed algorithm to withstand statistical attacks

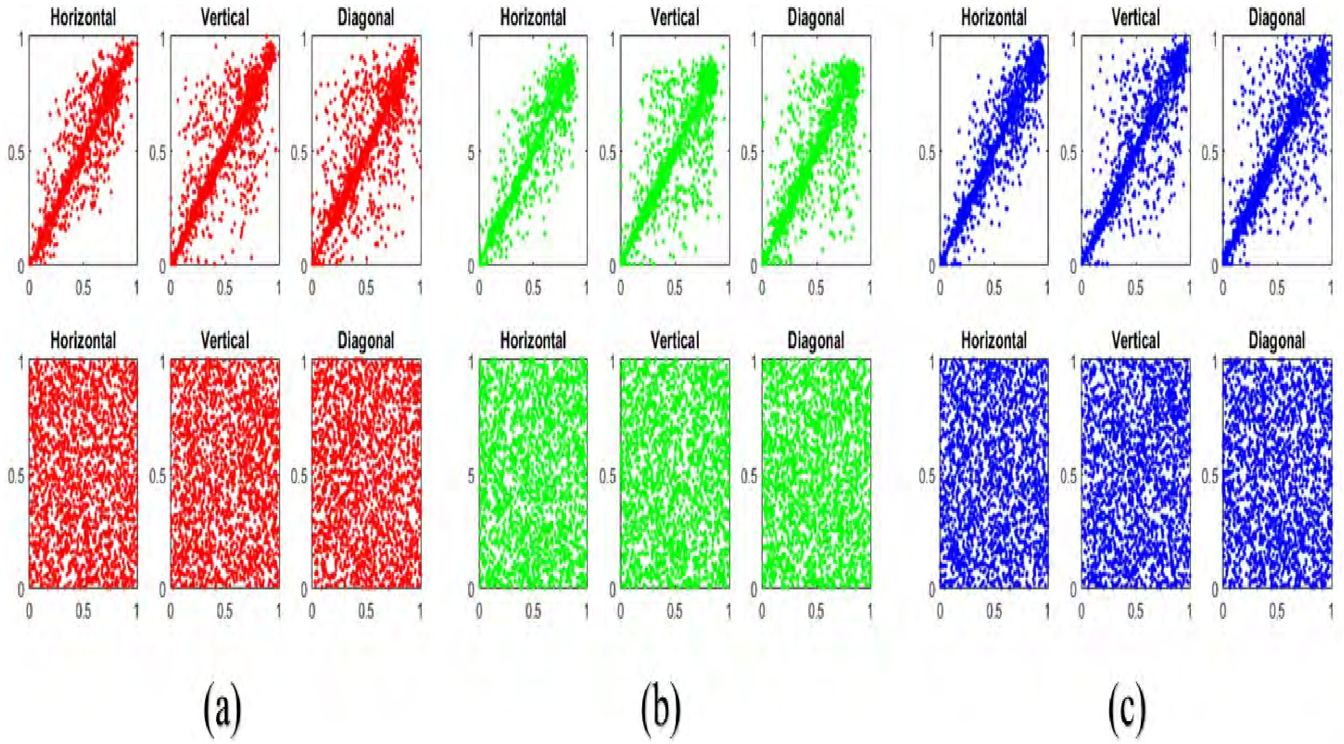


**FIGURE 8.** Correlation of two adjacent pixels in horizontal, vertical, and diagonal directions of a keyframe before and after encryption for each RGB spectral component.

### E. SECRET KEY ANALYSIS

A reliable ciphering algorithm should have large key space to resist exhaustive search attacks [14]. In our proposed algorithm, the secret key generated using Algorithm 2 (based on a hash function) ensures thorough sensibility and security for the initial secret source. The given initial source is hashed using SHA256 function and the output of the function is employed to generate the initial value and parameters of the chaotic system. In this situation, the attacker has two choices to execute attacks in an attempt to find the secret key. First, he shall try to find the hash output, and second, he shall try to find the initial values of the chaotic maps. The hash output ensures $2^{256}$ keys while the initial values of the 2D logistic map can ensure $2^{192}$ keys. Taking into account that our chaotic system has three inputs as secret keys (x,y,r) and these spaces can generate one chaotic key. It should be noted that we can generate three keys – S1, S2, and S3 – using three sources to fit the requirement of large space required by Algorithm 2. Therefore, in both previous scenarios, our proposed algorithm can ensure a large space of keys ($2^{192}$) that can resist all kinds of brute-force attacks and can provide a high level of security.

### F. SPEED ANALYSIS

In real-time processing, the algorithms should provide good speed performance along with ensuring maximum security. The proposed encryption algorithm can achieve good speed and can ensure a high level of security for the extracted keyframes. The speed performance of the proposed algorithm is shown in Table 5 using a different set of keyframes. Also, the results of different state-of-the-art image encryption schemes based on chaotic maps are shown in Table 6. The results prove that our algorithm has a good speed compared to other methods shown in Table 6.

**TABLE 6.** Encryption speed (Kb/sec) comparison.

| Algorithm | Encryption |
|---|---|
| The proposed algorithm | 1166 |
| Zhou et al. [26] | ≈390 |
| Belazi et al. [27] | ≈200 |
| Yao et al. [28] | ≈440 |
| Hamza et al.[14, 15] | ≈205 |

### G. COMPARISONS WITH OTHER SCHEMES

In this subsection, we compare our proposed algorithm with other state-of-the-art schemes across four aspects (key space, speed, resisting statistical attacks, and resisting differential attacks) as given in Table 7. These metrics are the main tests to compare the performance of any algorithm in terms of security and speed. Also, we consider this part of analysis in

**TABLE 7.** Comparison results.

|  | Size Image | Key space | Speed (ms) | Correlation | NPCR | UACI |
|---|---|---|---|---|---|---|
| Our | [640, 480,3] | $10^{90}$ | 790 | 0.0035 | 99.615 | 33.4658 |
| [5] | [1024,1024,1] | $2^{624}$ | 2513 | 0.0129 | 99.6177 | 33.6694 |
| [22] | [256,256,1] | $0.25 \times 10^{64}$ | 1320 | 0.0060 | 99.6200 | 33.5100 |
| [23] | [256,256,1] | $10^{56}$ | 547 | 0.0722 | $> 99$ | $\cong 33.43$ |

our work to show the merits of using our proposed algorithm compared with current other schemes and our previous works.

## IV. CONCLUSION

This paper addressed the problem of confidentiality of the keyframes extracted from diagnostic hysteroscopy videos. Our system is two-fold: extracting keyframes using video summarization and ciphering the extracted keyframes using the proposed image encryption method. The ciphered images can be then transmitted to healthcare centers and concerned users such as remote medical specialists. Our proposed image ciphering algorithm is based on 2D logistic chaotic map sequences for which we employed a 2D logistic map to produce chaotic sequences for the encryption scheme. The generated sequences rely on mixing and cascading the orbits of the chaotic map without any use of finite computations which ensure the randomness behavior of the encryption keys. The results collected from different sets of experiments and security analysis from different perspectives verify the superiority, security, and efficiency of our proposed encryption scheme compared to other image encryption algorithms.

## REFERENCES

[1] K. Muhammad, M. Sajjad, and S. W. Baik, "Dual-level security based cyclic18 steganographic method and its application for secure transmission of keyframes during wireless capsule endoscopy," *J. Med. Syst.*, vol. 40, no. 5, p. 114, 2016.

[2] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, and S. W. Baik, "A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image," *Multimedia Tools Appl.*, vol. 75, no. 22, pp. 14867–14893, 2016.

[3] M. Sajjad *et al.*, "Mobile-cloud assisted framework for selective encryption of medical images with steganography for resource-constrained devices," *Multimedia Tools Appl.*, vol. 76, no. 3, pp. 3519–3536, 2016.

[4] Z. Yan, W. Ding, X. Yu, H. Zhu, and R. H. Deng, "Deduplication on encrypted big data in cloud," *IEEE Trans. Big Data*, vol. 2, no. 2, pp. 138–150, Jun. 2016.

[5] A. Belazi, A. A. A. El-Latif, and S. Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos," *Signal Process.*, vol. 128, pp. 155–170, Nov. 2016.

[6] L. Zeng and R. Liu, "Cryptanalyzing a novel couple images encryption algorithm based on DNA subsequence operation and chaotic system," *Optik-Int. J. Light Electron Opt.*, vol. 126, pp. 5022–5025, Dec. 2015.

[7] W. Ding, Z. Yan, and R. H. Deng, "Encrypted data processing with Homomorphic re-encryption," *Inf. Sci.*, vol. 409, pp. 35–55, Oct. 2017.

[8] T. Jung, X. Li, Z. Wan, and M. Wan, "Control cloud data access privilege and anonymity with fully anonymous attribute-based encryption," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 1, pp. 190–199, Jan. 2014.

[9] W. Lu, A. L. Varna, and M. Wu, "Confidentiality-preserving image search: A comparative study between homomorphic encryption and distance-preserving randomization," *IEEE Access*, vol. 2, pp. 125–141, 2014.

[10] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," *Image Vis. Comput.*, vol. 24, no. 9, pp. 926–934, 2006.

[11] M. Machkour, A. Saaidi, and M. Benmaati, "A novel image encryption algorithm based on the two-dimensional logistic map and the latin square image cipher," *3D Res.*, vol. 6, p. 36, Dec. 2015.

[12] R. Hamza, "A novel pseudo random sequence generator for image-cryptographic applications," *J. Inf. Secur. Appl.*, vol. 35, pp. 119–127, Aug. 2017.

[13] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, pp. 614–626, 2016.

[14] R. Hamza and F. Titouna, "A novel sensitive image encryption algorithm based on the Zaslavsky chaotic map," *Inf. Secur. J., A Global Perspect.*, vol. 25, pp. 162–179, Dec. 2016.

[15] R. Hamza, K. Muhammad, Z. Lv, and F. Titouna, "Secure video summarization framework for personalized wireless capsule endoscopy," *Pervasive Mobile Comput.*, vol. 41, pp. 436–450, Oct. 2017.

[16] I. Mehmood, M. Sajjad, and S. W. Baik, "Video summarization based tele-endoscopy: A service to efficiently manage visual data generated during wireless capsule endoscopy procedure," *J. Med. Syst.*, vol. 38, p. 109, Sep. 2014.

[17] Y. Wu, G. Yang, H. Jin, and J. P. Noonan, "Image encryption using the two-dimensional logistic chaotic map," *J. Electron. Imag.*, vol. 21, no. 1, pp. 013014-1–013014-15, 2012.

[18] K. Muhammad, J. Ahmad, M. Sajjad, and S. W. Baik, "Visual saliency models for summarization of diagnostic hysteroscopy videos in healthcare systems," *SpringerPlus*, vol. 5, p. 1495, Dec. 2016.

[19] X. Wu, D. Wang, J. Kurths, and H. Kan, "A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system," *Inf. Sci.*, vol. 349, pp. 137–153, Jul. 2016.

[20] X. Wei, L. Guo, Q. Zhang, J. Zhang, and S. Lian, "A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system," *J. Syst. Softw.*, vol. 85, no. 2, pp. 290–299, 2012.

[21] S. Zhou, Z. Wei, B. Wang, X. Zheng, C. Zhou, and Q. Zhang, "Encryption method based on a new secret key algorithm for color images," *AEU-Int. J. Electron. Commun.*, vol. 70, pp. 1–7, Jan. 2016.

[22] L. Xu, Z. Li, J. Li, and W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps," *Opt. Lasers Eng.*, vol. 78, pp. 17–25, Mar. 2016.

[23] X. Huang, "Image encryption algorithm using chaotic Chebyshev generator," *Nonlinear Dyn.*, vol. 67, no. 4, pp. 2411–2417, 2012.

[24] A. Akhavan, A. Samsudin, and A. Akhshani, "A symmetric image encryption scheme based on combination of nonlinear chaotic maps," *J. Franklin Inst.*, vol. 348, pp. 1797–1813, Oct. 2011.

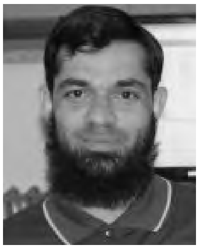
[25] Y. Zhou, L. Bao, and C. L. P. Chen, "Image encryption using a new parametric switching chaotic system," *Signal Process.*, vol. 93, no. 11, pp. 3039–3052, 2013.

[26] Y. Zhou, L. Bao, and C. P. Chen, "A new 1D chaotic system for image encryption," *Signal Process.*, vol. 97, no. 11, pp. 172–182, 2014.

[27] A. Belazi, M. Khan, A. A. A. El-Latif, and S. Belghith, "Efficient cryptosystem approaches: S-boxes and permutation-substitution-based encryption," *Nonlinear Dyn.*, vol. 87, no. 1, pp. 337–361, 2016.

[28] W. Yao *et al.*, "A fast color image encryption algorithm using 4-pixel feistel structure," *PloS ONE*, vol. 11, no. 11, p. e0165937, 2016.

**RAFIK HAMZA** received the M.Sc. and Ph.D. degrees in computer science from the University of Batna 2, in 2014 and 2017, respectively. He has authored several papers in peer-reviewed international journals, such as the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE ACCESS, and *Pervasive and Mobile Computing*. His research interests include information security, image and video processing, medical image analysis, chaos theory, and lightweight cryptography applications. He is serving as a reviewer for well reputed international journals, including IEEE ACCESS, *Multimedia Tools and Applications* (Springer), *Journal Cluster Computing*, *Computer Networks*, *Sustainable Computing*, the *Informatics and Systems Journal*, the *Future Generation Computer Systems Journal*, and the *Journal of Computational Science*.



**KHAN MUHAMMAD** (S'16) received the bachelor's degree in computer science from the Islamia College Peshawar, Pakistan, in 2014, with a focus on information security. He is currently pursuing the M.S. leading to Ph.D. degree in digital contents from Sejong University, Seoul, South Korea. He has been a Research Associate with the Intelligent Media Laboratory since 2015. He has authored over 24 papers in peer-reviewed international journals and conferences, such as *Future Generation Computer Systems*, the IEEE ACCESS, the *Journal of Medical Systems*, *Biomedical Signal Processing and Control*, *Multimedia Tools and Applications*, *Pervasive and Mobile Computing*, *SpringerPlus*, the *KSII Transactions on Internet and Information Systems*, the *Journal of Korean Institute of Next Generation Computing*, the *NED University Journal of Research*, the *Technical Journal*, the *Sindh University Research Journal*, the *Middle-East Journal of Scientific Research*, MITA 2015, PlatCon 2016, and FIT 2016. His research interests include image and video processing, information security, image and video steganography, video summarization, diagnostic hysteroscopy, wireless capsule endoscopy, computer vision, deep learning, and video surveillance.

**ARUNKUMAR N** received the B.E. degree in electronics and instrumentation engineering from Madurai Kamaraj University in 2003, the M.E. degree from the College of Engineering, Guindy, in 2005, and the Ph.D. degree from SASTRA University in 2012. His main research area includes biomedical signal processing, machine learning, and data mining. He has received various awards and has been in top hundred list in technical exams across his country. He has been invited as the conference chair for many international conferences at various places across the world.

**GUSTAVO RAMÍREZ-GONZÁLEZ** received the Ph.D. degree from the Universidad Carlos III de Madrid, Spain, in 2010. He has been a Titular Professor with the Department of Telematics, University of Cauca, Colombia, since 2005. His research interests include image and video processing, multimedia, cloud security, e-learning, and signal processing.