Contents lists available at ScienceDirect

Pervasive and Mobile Computing

journal homepage: www.elsevier.com/locate/pmc

Fast track article

Secure video summarization framework for personalized wireless capsule endoscopy

Rafik Hamza[a], Khan Muhammad[b,c], Zhihan Lv[d,*], Faiza Titouna[a]

[a] *LAMIE Laboratory, Department of Computer Science, University of Batna 2, Algeria*
[b] *Intelligent Media Laboratory, Department of Software, College of Software Convergence, Sejong University, Seoul, Republic of Korea*
[c] *Digital Image Processing Laboratory, Department of Computer Science, Islamia College Peshawar, Pakistan*
[d] *School of Data Science and Software Engineering, Qingdao University, China*

ARTICLE INFO

Article history:
Available online xxxx

Keywords:
Information security
Medical image analysis
Wireless capsule endoscopy
Image encryption
Personalized healthcare systems
Video summarization

ABSTRACT

Wireless capsule endoscopy (WCE) has several benefits over traditional endoscopy such as its portability and ease of usage, particularly for remote internet of things (IoT)-assisted healthcare services. During the WCE procedure, a significant amount of redundant video data is generated, the transmission of which to healthcare centers and gastroenterologists securely for analysis is challenging as well as wastage of several resources including energy, memory, computation, and bandwidth. In addition to this, it is inherently difficult and time consuming for gastroenterologists to analyze this huge volume of gastrointestinal video data for desired contents. To surmount these issues, we propose a secure video summarization framework for outdoor patients going through WCE procedure. In the proposed system, keyframes are extracted using a light-weighted video summarization scheme, making it more suitable for WCE. Next, a cryptosystem is presented for security of extracted keyframes based on 2D Zaslavsky chaotic map. Experimental results validate the performance of the proposed cryptosystem in terms of robustness and high-level security compared to other recent image encryption schemes during dissemination of important keyframes to healthcare centers and gastroenterologists for personalized WCE.

1. Introduction

Digital images play an important role in different areas of interest such as commercial, military, and medical applications. The security of this specific data has become a major concern in recent years for which researchers have presented numerous techniques [1,2]. Cryptography is one of the solutions for information security and is considered as one essential aspect for secure communication over the public network *Internet*. The security of cryptographic techniques is mainly dependent on secret keys as dictated by Kirchhoff's principle [3,4]. These keys are of paramount importance in cryptographic applications such as image encryption [5,6] and secret stego key sharing [7–9]. Since, the cryptosystem is dependent only on the secret keys, therefore, it should be nearly impossible to retrieve the information without the exact secret keys. One of the well-known methods to generate secure cryptographic keys is to use the chaotic systems [10,11].

[*] Corresponding author.
E-mail addresses: r.hamza@univ-batna2.dz (R. Hamza), khan.muhammad@ieee.org (K. Muhammad), lvzhihan@gmail.com (Z. Lv), ftitouna@yahoo.fr (F. Titouna).

http://dx.doi.org/10.1016/j.pmcj.2017.03.011
1574-1192/© 2017 Elsevier B.V. All rights reserved.

The chaotic maps are nonlinear systems, which have been widely used in cryptographic systems. Chaotic maps can generate random numbers, therefore, they are considered as a solution to produce keystream. In the area of image encryption, there are two major classes of chaotic systems known as one-dimension (1D) and multi-dimension chaotic systems (M-D) [12]. The 1D chaotic systems such as the logistic map [11], are easier to implement than M-D ones, but are considered as non-secure [13]. Most of the 1D chaotic maps have multiple issues including the limited space key and the limited range of the chaotic behaviors. Hence, it is preferred to use M-D chaotic maps [13]. However, the chaotic maps still have certain defects regardless of their dimension, especially when such systems are defined on real numbers and their corresponding cryptosystems are defined on finite numbers [14]. Considering such weaknesses, many encryption systems have been cracked recently due to their weak secret keys [15] and poor security level [16,17]. Moreover, digital images have various inherent properties such as the large dimension data, low entropy, and high correlation between adjacent pixels. These properties make the algorithms not suitable for image encryption [13,18]. They also increase the thread of cryptanalysis and confirm the need of new solutions with confirmation about the security level.

Nowadays, IoT environments are highly visible in human life through which a variety of IoT applications such as life logging physical activity information [19], physical activity monitoring and assessment [20], and IoT personalized healthcare systems are possible [21], making human life easier and more efficient. However, these evolutionary processes need to pay attention to the security issues to ensure the authentication and privacy of data [22]. Moreover, most of the IoT components are characterized by low capabilities in terms of both energy and computing resources and thus they cannot implement complex security algorithms [22].

Recently, the problem of secure dissemination of secret information over the Internet is growing fast. Ensuring the confidentiality and privacy of medical images is becoming one of the challenging problem as they contain sensitive data with distinguishing visual representations of the interior of a human body [23,24]. One of the popular methods to record images of the digestive tract is wireless capsule endoscopy (WCE). During WCE procedure, the patient swallows a pill-sized capsule, which captures the images of gastrointestinal (GI) track while passing through it. The captured images are recorded in an image recording unit (IRU), which is fitted in a belt worn by patient [25]. The capsule is expelled from the body naturally after 72 h, however, the frames captured in the initial 8 h are important for visualization of GI track [26]. During this eight hours period, a large sequence of images (around 50 000) are generated, out of which only a limited number of frames are important for diagnosis by gasteroentrologists. The collected video data contains a significant amount of redundant and non-informative frames due to capsule's explosion to turbid fluids and food particles [27]. In this regard, it becomes inherently difficult and time consuming for gasteroentrologists to find the desired contents from this huge amount of collected video data. Thus, it is important to exploit a mechanism for automatic extraction of diagnostically important frames from the collected enormous amount of video data. Video summarization (VS) techniques [28,29] can be used to solve this problem, where the informative frames can be extracted automatically and can be sent to the remote patient monitoring centers and gasteroentrologists. As the overall diagnosis is mainly based on the extracted keyframes, it is necessary to send these frames securely as they can be exposed to various attacks such as spoofing or injection attacks [30]. Hence, the problem of security and authentication arises for which we have devised a new framework.

In this work, we propose an efficient and secure video summarization framework for overcoming the drawbacks of existing systems. Our main contributions are summarized as follows:

1. An efficient and privacy-preserving video summarization framework is proposed for extraction of diagnostically important frames from WCE videos and its secure dissemination to gastroenterologists and remote healthcare centers.
2. The proposed video summarization method uses the concept of integral image in features computation, increasing its suitability in real-time applications such as WCE.
3. A robust Zaslavsky chaotic map (ZCM) based image encryption scheme is proposed for security of keyframes. The proposed method can guarantee the secrecy of the keyframes with larger key space and can provide excellent confusion and diffusion properties with high level security. Moreover, it can be used for authentication of keyframes, preventing the possibility of injecting false keyframes.
4. The proposed framework can facilitate healthcare centers in ensuring the privacy of patients, reducing the energy, processing and communication cost, helping gastroenterologists to quickly browse for desired contents and fast analysis, leading to improved diagnosis with personalization.

The remaining of this paper is organized as follows. The proposed system is explained in Section 2. Experimental results and discussion are presented in Section 3. The comparison tests are given in Section 4, followed by conclusion in Section 5.

2. The proposed framework

Medical data has become very interesting especially in remote health monitoring applications due to rapid advancement in smart sensor technologies. The current sensor technology is facilitating remote patient monitoring centers to produce different bio-signals and images from the outdoor patients' body and monitor them remotely [31,32]. For example, during gait analysis, wearable sensors are used to measure numerous gait parameters including step length, cadence, swing-

Please cite this article in press as: R. Hamza, et al., Secure video summarization framework for personalized wireless capsule endoscopy, Pervasive and Mobile Computing (2017), http://dx.doi.org/10.1016/j.pmcj.2017.03.011

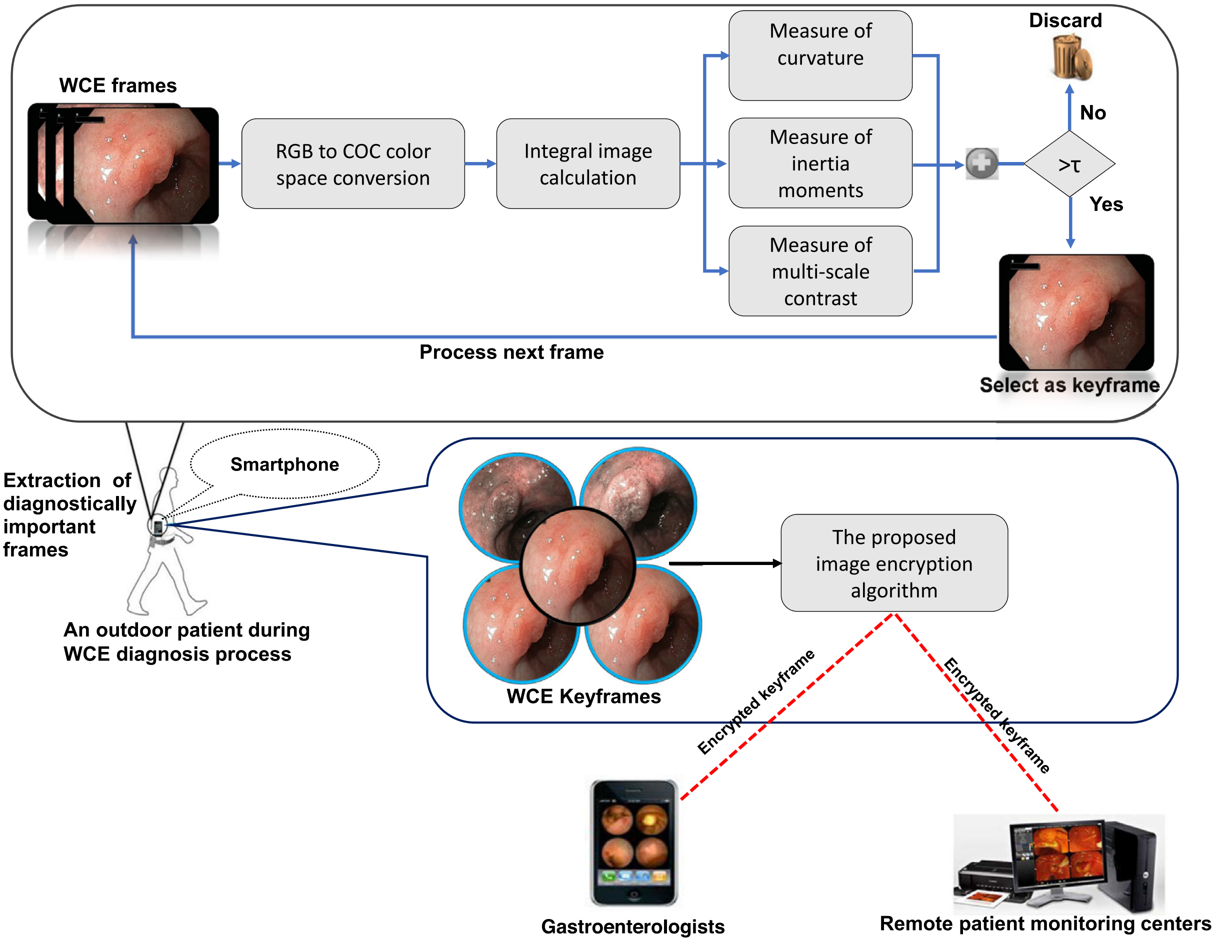
WCE frames
RGB to COC color space conversion
Integral image calculation
Measure of curvature
Measure of inertia moments
Measure of multi-scale contrast
Discard
No
>τ
Yes
Select as keyframe
Process next frame
Extraction of diagnostically important frames
Smartphone
An outdoor patient during WCE diagnosis process
WCE Keyframes
The proposed image encryption algorithm
Encrypted keyframe
Encrypted keyframe
Gastroenterologists
Remote patient monitoring centers

Fig. 1. Framework of the proposed system.

stance radio, stride length, and stride width, which are useful for diagnosis of several diseases such as Parkinson's disease, Huntington, and stroke [33]. Another interesting application of medical sensors is WCE, where a capsule swollen by patient visualizes the entire GI track by capturing its images for several hours, producing a large amount of video data which is stored in IRU. Using smart phones, this video data can be transferred remotely to healthcare centers but it requires more transmission cost, bandwidth, and energy and wastes the time of gastroenterologists in searching for diagnostically desired frames. In addition, ensuring the security of large amount of data is also comparatively challenging. Our proposed framework resolves these issues by using video summarization technology combined with image encryption. Our proposed system is two-fold: (1) extracting keyframes using video summarization and (2) encrypting the extracted keyframes using a robust image encryption scheme [5]. Fig. 1 highlights the proposed framework for secure dissemination of keyframes to remote health monitoring centers during WCE. The technical detail of the framework is provided in the sub-sequent sections.

2.1. Summarization of video data captured by wireless capsule during WCE

In this sub-section, the process of summarization of WCE video data is presented. During WCE, a large amount of redundant and non-informative video data is generated due to explosion of wireless capsule to food substances while passing through GI track [26]. Considering the limited resources of smart phones and long duration of WCE process, it is usually assumed that sending all the WCE data to healthcare centers and gastroenterologists is impractical [27,34]. Therefore, it is important to devise a mechanism, which can allow only the informative frames for transmission and discard the redundant and non-informative frames. This goal can be achieved using video summarization methods. Keeping in view the constraints of WCE, we have used our recent video summarization scheme [35] for extraction of diagnostically important frames. Our recent VS method is computationally inexpensive, which is the main motivational reason for using it in the proposed

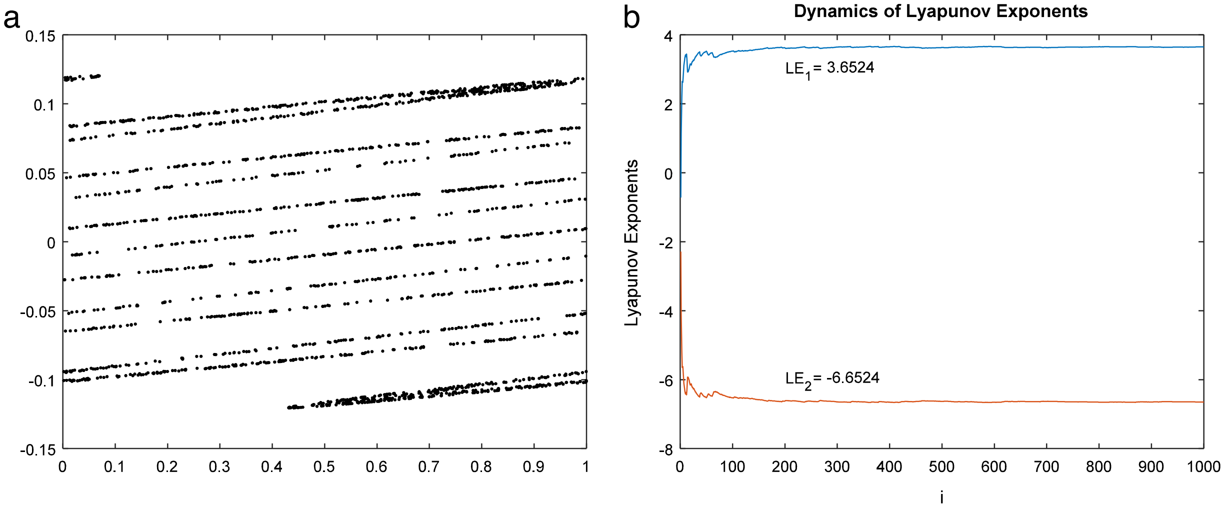

Fig. 2. (a) The Zaslavsky attractor. (b) The dynamics of Lyapunov exponents of 2D Zaslavsky chaotic map.

framework. The reason is the utilization of integral image, which is a light-weight process with time complexity of 2WH (H: height, W: width of the frame), making this method more suitable for real-time processing of WCE video data.

Suppose the sequence of WCE frames coming from wireless capsule is F_t with $t = 1, 2, 3, \ldots, N_T$ where N_T indicates the total number of frames. The target is to eliminate the redundant frames and classify the remaining WCE frames into informative and non-informative, thereby sending the informative frames to healthcare centers and discarding the non-informative. To this end, each frame is converted from RGB to COC color model based on which the integral image is computed. Next, three features including moments of inertia, multi-scale contrast, and curvature map are computed. The saliency scores of these features are then normalized in the range 0–1. The normalized values of individual saliencies are then fused to form an aggregated attention curve based on which the keyframes can be extracted. For detailed information about our recent VS method, the readers are referred to [35]. Overall, this scheme provides several advantages such as reduction in the transmission cost, storage, and battery and saving the analysis time of gastroenterologists by avoiding large amount of redundant and non-informative frames.

2.2. ZCM-based image encryption algorithm

In this sub-section, we describe our image encryption algorithm [5], for ciphering the keyframes in detail. The proposed cryptosystem is divided into two steps: initialization and processing steps. In the first step, the algorithm for generating the encryption keys for the cryptosystem process is described. In the second part, the proposed encryption/decryption algorithms are explained, which are based on permutation–diffusion processes, achieving a high level of security. All the initial values of the ZCM are taken as secret keys in our encryption method. The upcoming sub-sections explain the key generation procedure, followed by encryption/decryption of keyframes.

2.2.1. The pseudo-key encryption/decryption generator

The proposed image encryption algorithm uses the pseudo random of ZCM because it generates very random numbers sequence. The chaotic behavior of a dynamical system is measured using Lyapunov exponents (LE) such that a dynamical system with a positive LE is considered as chaotic [36]. Fig. 2(a) shows the attractive frame for ZCM. Fig. 2(b) shows the values of LE for the ZCM using the secret key: $(x_0, y_0, \upsilon, \varepsilon, \tau) = (0.8, 0.9, 7, 6, 5)$. The Lyapunov spectrum of this chaotic system is computed to be around 1.55 [5]. Therefore, the generated sequence directly from the ZCM is very chaotic and high compared to other 2D chaotic maps such as Hénon chaotic map, which has LE $= 1.24$ [37]. Kolmogorov entropy (KE) provides a quantitative explication of randomness of a signal. Since, ZCM has one positive LE, the KE should be positive too [36], indicating that our pseudo random generator is unpredictable.

The proposed image encryption uses directly the sequences generated by the chaotic map, avoiding the problem of degradation caused by finite precision computation. Algorithm 1 shows the steps to produce the generated keys for the proposed cryptosystem. These generated keys denote the encryption keys whereas the initial keys of the ZCM are the secret keys for the proposed cryptosystem scheme. The generated encryption keys represent the index sorts, which help to execute the permutation steps within the cryptosystem.

Please cite this article in press as: R. Hamza, et al., Secure video summarization framework for personalized wireless capsule endoscopy, Pervasive and Mobile Computing (2017), http://dx.doi.org/10.1016/j.pmcj.2017.03.011

Algorithm 1. The generation of Keys for ZCM-WCE.

```
**Input**: $x_0, y_0, v, \varepsilon, \tau, K_{in}, I(Keyframe)$.
1: $[h, w, e] \leftarrow size\ (I)$
2: $u = \frac{1-e^{-\tau}}{\tau}$
3: For  $i = 1$ to $(\max(h, w \times e) + 1034)$
        $Ve\,(2i) = \mathbf{x}_{\mathrm{i}} + v\ (1 + uy_i) + \varepsilon vu\ (\cos(2\pi x_i))\ \mathrm{mod}\ 1$
        $Ve\,(2i+1) = e^{-\tau}(y_i + \varepsilon \cos\ (2\pi x_i))$
   End
4: $V_{in} \leftarrow Ve(10{:}h + 9)$
5: $V'_{in} \leftarrow Ve(10{:}w \times e + 9)$
6: $R_{in} \leftarrow reshape\ (Ve\ (10{:}1024 + 9), 32, 32)$
7: $[\neg, V] \leftarrow Sort(V_{in})$
8: $\left[\neg, V'\right] \leftarrow Sort(V'_{in})$
9: $[\neg, R] \leftarrow Sort(R_{in})$
10: $\alpha = |\sum \mathrm{V}'_{\mathrm{in}} + \sum \mathrm{V}_{\mathrm{in}} + \sum \mathrm{R}_{\mathrm{in}}|\ \mathrm{mod}\ 256$
11: IF $\alpha = 0$ then
        $\alpha = |\sum \mathrm{V}'_{\mathrm{in}} + \sum \mathrm{V}_{\mathrm{in}} + \sum \mathrm{R}_{\mathrm{in}}|\ \mathrm{mod}\ 255$
   End
12: $K \leftarrow \alpha \cdot K_{in}$
13: $L \leftarrow K^{-1}$
**Output:** $V, V', R, \alpha, L, K$.
```

Algorithm 1 illustrates the steps for generating the main keys of our scheme. For the first step in Algorithm 1, we get height and width of the keyframe, followed by generating the chaotic sequence *Ve* directly from ZCM. To avoid the effect of initial values, we discarded the first ten numbers of the generated sequence "*Ve*". As shown in Algorithm 1, our method uses the ZCM directly to produce the appropriate encryption keys of the proposed cryptosystem. Therefore, these encryption keys are random and unpredictable in their nature as they have been generated directly from chaotic system. The function "Sort" is used for sorting the elements of an input vector and each column in R_{in}. It means that the matrix R contains indexes for sorting the elements of each column in R_{in} while V and V' are two vectors, representing the index sorts of V_{in} and V'_{in}. Finally, we compute $\alpha,\ L,\ K$ over the finite field using the chaotic sequences R, V_{in} and V'_{in}, where α is an integer number so that $\alpha \in \{1, 2, \dots, 255\}$. The initial matrix K_{in} is $[32 \times 32]$ invertible matrix over Gf (2^8), which is more suitable to be applied with the proposed image encryption scheme.

2.2.2. The cryptosystem algorithm

The proposed algorithm uses a permutation–diffusion processing to dismantle and distribute pixels of the keyframe. The arithmetic matrix multiplication over Galois Fields GF (2^8) is applied for each sub-block B of the data matrix image, where B is denoted by a $[32,\ 32]$ block of the data matrix. An irreducible polynomial $x^8 + x^4 + x^3 + x^2 + 1$ is selected to generate the elements of GF (2^8) for our proposed scheme. The reason to choose this irreducible polynomial is that it is the first polynomial of the degree 8 listed in our recent work [5], where we have listed 16 primitive polynomials (all primitive polynomials are also irreducible), each with well-tested security. In fact, there exists 30 irreducible polynomials with degree 8, which can serve as the irreducible polynomial to be used [38,39].

Algorithm 2. Encryption Algorithm.

```
**Input**: $x_0, y_0, v, \varepsilon, \tau, K_{in}, I(Keyframe)$.
0: Read the plain frame, and apply Algorithm 1
1: Transform the frame matrices into one matrix with [h, 3×w]
2: $I_2 \leftarrow$ Permutation using the matrix $V$, and $V'$
3: $I_3 \leftarrow I_2 \oplus \alpha$
4: $I_4 \leftarrow$ Permutation using the matrix R
5: $I_5 \leftarrow L \cdot B_{I_4} \cdot K$
6: $I_6 \leftarrow$ Permutation using the matrix $V$, and $V'$
7: Repeat the previous steps 4–6 four rounds, sequentially
8: $C \leftarrow$ Reshape the obtained matrix intro three matrices with size [h, w]
**Output**: C: Encrypted keyframe.
```

Algorithm 2 shows the steps of encryption for the extracted keyframe from WCE video data using our recent video summarization scheme. Firstly, we pack the matrices of the keyframe, which represent the corresponding RGB color (three matrices), into one matrix with size $[h, e \times w]$, followed by dismantling and distribution of pixels for the obtained data

Please cite this article in press as: R. Hamza, et al., Secure video summarization framework for personalized wireless capsule endoscopy, Pervasive and Mobile Computing (2017), http://dx.doi.org/10.1016/j.pmcj.2017.03.011

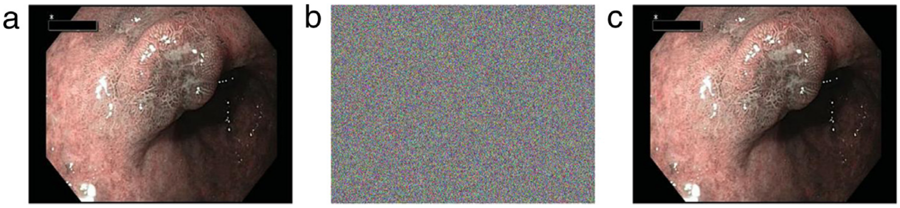

Fig. 3. (a) A sample of keyframe extracted using our recent video summarization scheme. (b) The encrypted keyframe using our proposed scheme. (c) The corresponding decrypted keyframe.

matrix. The symbol $\oplus$ indicates the bitwise XOR operator. The term "permutation" in Algorithm 2 means that each pixel is permuted using the given element sort. We use the matrix R as indexes for shifting each block B. Similarly, we use the indexes vector V and V' to shift each column and row of the image. We use the arithmetic matrix multiplication for each B block using the matrices $K,\ L$, where L is the invertible matrix of K such that $L \cdot K = Id_{32}$ and Id_{32} is an [32, 32] identical matrix. The symbol '·' in Algorithm 2 is the operator of the multiplication over Galois Fields GF (2^8).

```
Algorithm 3. Decryption algorithm.
Input: $x_0, y_0, \upsilon, \varepsilon, \tau, K_{in}, I(Encrypted\_Keyframe)$.
0: Read the encrypted frame, and apply Algorithm 1
1: Transform the frame matrices to one matrix with [h, 3 × w]
2: $C_2 \leftarrow$ Permutation inverse using the matrix V, and V′
3: $C_3 \leftarrow K \cdot B \cdot L$
4: $C_4 \leftarrow$ Permutation inverse using the matrix R
5: $C_5 \leftarrow$ Repeat the previous steps 2–4 four rounds, sequentially
6: $C_6 \leftarrow C_5 \oplus \alpha$
7: $C_7 \leftarrow$ Permutation inverse using the matrix V, and V′
8: $D \leftarrow$ Reshape the obtained matrix intro three matrices with size [h, w]
Output: D: the decrypted keyframe.
```

Algorithm 3 shows the decryption steps for our proposed scheme. The inverse steps for the encryption processes can recover the original pixels completely only by using the exact secret keys. Since the sorted indexes are unique, the original pixels can be recovered successfully from the permutation steps. Fig. 3 shows the keyframe extracted by the proposed scheme along with the corresponding encrypted keyframe and decrypted keyframe. Fig. 4 summarizes the overall process of the proposed framework by combining the video summarization module with encryption module during WCE.

3. Experimental results and discussion

In this section, the proposed system is evaluated through different experiments from security and statistical analysis point of view. First, we evaluated the proposed method through histogram analysis, key space, and sensibility analysis. Next, we analyzed the performance of the secret key and showed its resistance to common security attacks. Next, we exposed our proposed method to different attacks such as chosen/known attacks, and resisting differential attack, followed by its analysis using different tests such as randomness tests, and test of correlation analysis for two adjacent pixels in a ciphered keyframe. Finally, we showed the advantages of our proposed image encryption scheme by comparing its performance results with several recent state-of-the-art image encryption methods [10,37,40,41]. Due to special nature of WCE images, we directly used their source codes for the frames extracted by our recent VS method for comparison of results using the same platform and configurations, making the comparative analysis more fair and unbiased. A set of test keyframes and non-keyframes from a sample WCE video along with frame number are shown in Figs. 5 and 6.

During experiments, the initial values and controlling parameters of ZCM were selected as secret keys in our proposed scheme. For instance, we used the following values in our experimental tests as default values: $(x_0, y_0, \upsilon, \varepsilon, \tau) = (0.8, 0.9, 7, 6, 5)$.

3.1. Histogram analysis

The histogram of a frame illustrates the distribution of its gray levels. Fig. 7 shows the uniform probability distribution of ciphered keyframe without any statistical similarity, while the original keyframe appears significantly different from the ciphered keyframe. The histogram of encrypted frame is obviously uniform and the visual view is impossible to redirect to the original one as shown in Fig. 7. Consequently, our proposed scheme does not provide any information for attackers to be used in statistical attacks, which makes it more suitable for securing transmission of keyframes during WCE.

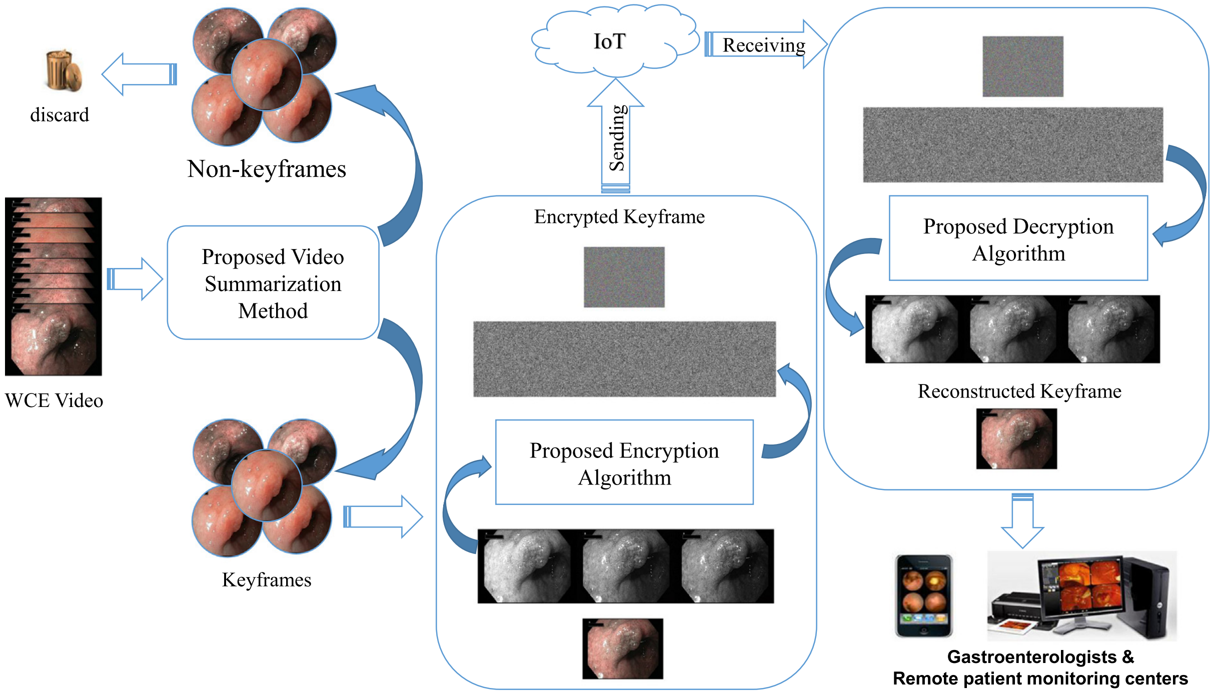
discard
Non-keyframes
WCE Video
Proposed Video Summarization Method
Keyframes
IoT
Sending
Receiving
Encrypted Keyframe
Proposed Encryption Algorithm
Proposed Decryption Algorithm
Reconstructed Keyframe
Gastroenterologists &
Remote patient monitoring centers

Fig. 4. Overall procedure of the proposed framework, illustrating the extraction of keyframes and flow of the proposed encryption/decryption algorithms for secure WCE in remote healthcare.

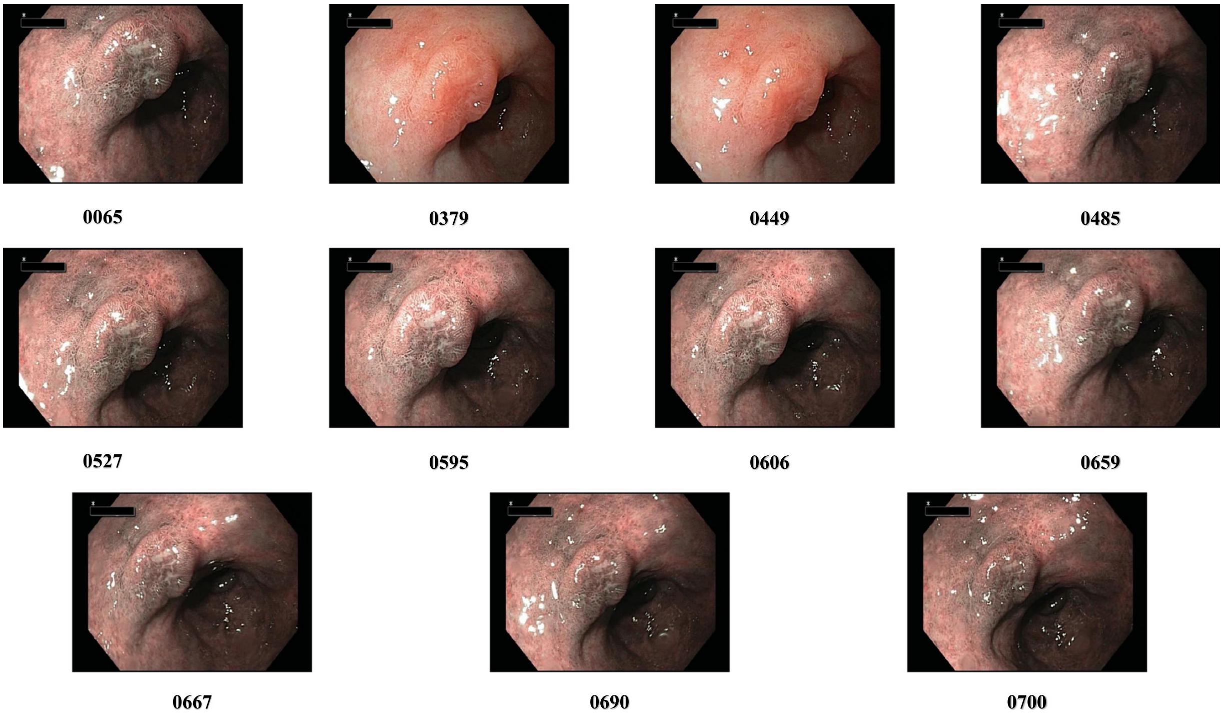

Fig. 5. The selected test keyframes with frame numbers from our proposed scheme.

3.2. Differential attack

Differential attack refers to investigating the difference in inputs and its corresponding effects on outputs [41]. Basically, an attacker investigates how a small change in any frame can affect the ciphered image so that he/she can proceed with

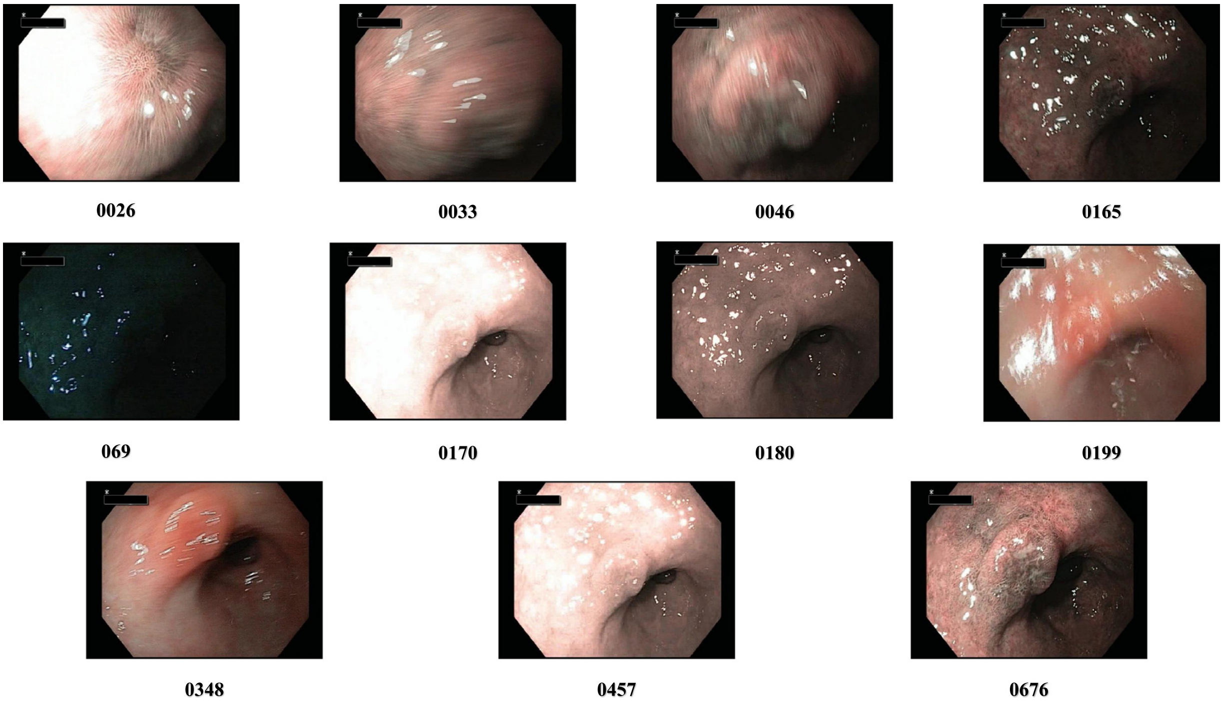

Fig. 6. Sample non-keyframes with frame number for a sample video for the proposed scheme.

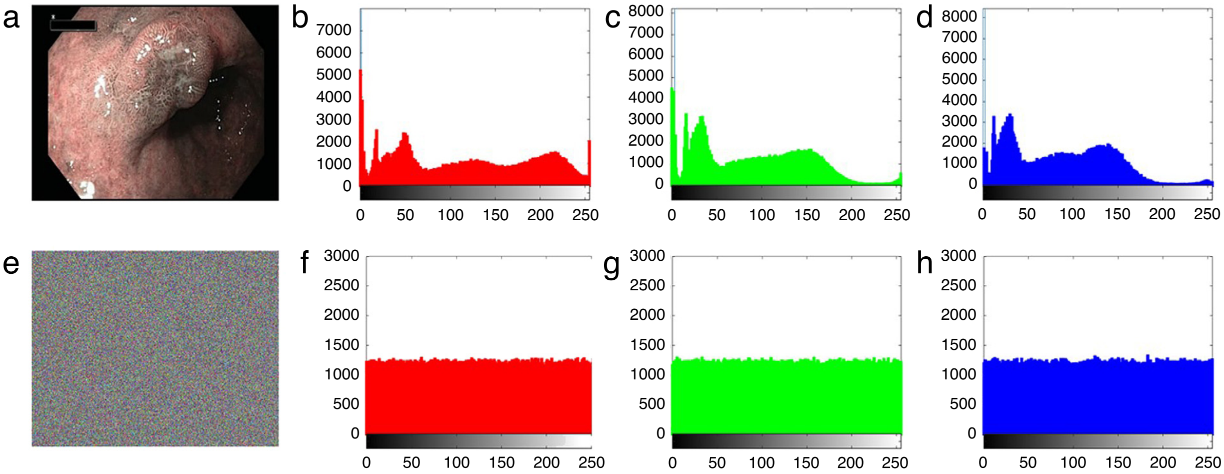

Fig. 7. (a) Keyframe 0065, (e) the encrypted keyframe, histogram of the original keyframe in (b) red, (c) green, and (d) blue components. Histogram of the encrypted keyframe in the (f) red, (g) green, and (h) blue components. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

his/her attacks. The ability to resist the differential attack can reveal the security level of any image encryption technique. This resistance of the differential attack can be measured using the number of pixel changing rate (NPCR) test [42] and unified average changed intensity (UACI) test [42], which are computed using Eqs. (1) and (2) as follows:

$$NPCR(C_1, C_2) = \sum_{i,j} \frac{S(i,j)}{D} \times 100\% \tag{1}$$

$$UACI(C_1, C_2) = \sum_{i,j} \frac{C_1(i,j) - C_2(i,j)}{255 \times D} \times 100\%. \tag{2}$$

Table 1
NPCR and UACI tests results for each channel of RGB frame.

Frames	0065		0606		0667		0690	
Test	NPCR	UACI	NPCR	UACI	NPCR	UACI	NPCR	UACI
R	99.6126	33.4412	99.6247	33.4923	99.6139	33.4750	99.6090	33.4698
G	99.6117	33.4361	99.6245	33.3929	99.6234	33.4864	99.6051	33.4480
B	99.6071	33.4371	99.6058	33.4985	99.5964	33.4861	99.6276	33.5088

Table 2
NPCR and UACI tests results for a set of keyframes.

Frames	0065	0379	0449	0485	0527	0595	0606	0659	0667
NPCR	99.6104	99.6085	99.6172	99.6164	99.6161	99.6235	99.6112	99.6006	99.6194
UACI	33.4381	33.4575	33.4784	33.5177	33.4456	33.4614	33.4825	33.4551	33.4935

Table 3
NPCR and UACI tests results for a set of non-keyframes.

Frames	0026	0033	0046	0165	0169	0170	0180	0348	0457
NPCR	99.6124	99.6144	99.6213	99.6071	99.6150	99.6085	99.6169	99.6087	99.6110
UACI	33.4579	33.5009	33.4876	33.4839	33.4740	33.5009	33.4001	33.5004	33.4735

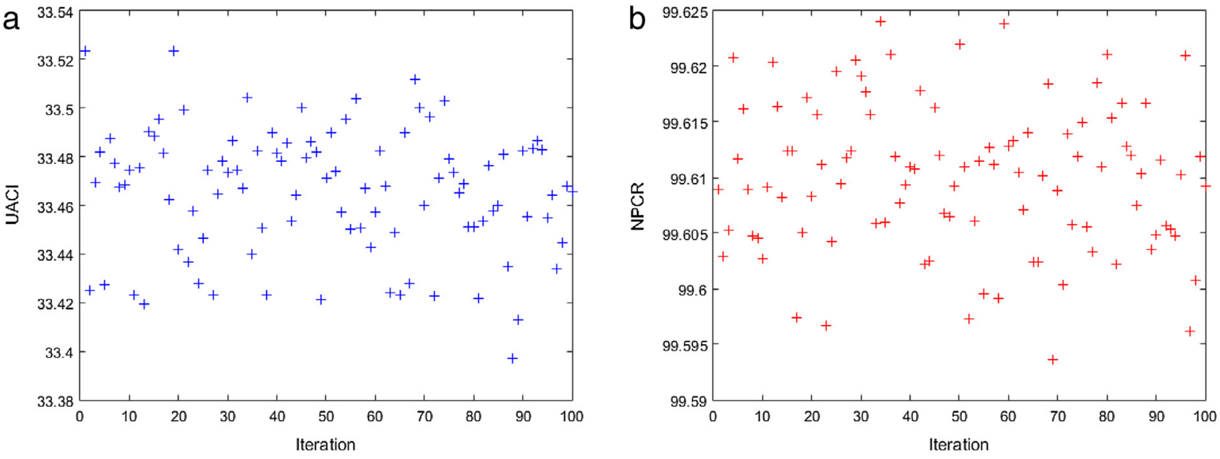

Fig. 8. (a) NPRC tests and (b) UACI tests for 100 modified plain-images only with one bit (randomly chosen).

Herein, "D" denotes the number of pixels and "S" is represented by Eq. (3).

$$S(i,j) = \begin{cases} 0, & \text{If } C_1(i,j) = C_2(i,j) \\ 1, & \text{Elsewise.} \end{cases} \tag{3}$$

In this test, we randomly change one bit of a pixel from a keyframe "I". The obtained keyframe is denoted by "J". We use the same secret key in our proposed scheme to encrypt both keyframes. C_1 and C_2 are the two ciphered keyframes corresponding to "I" and "J", respectively. Finally, we apply the tests of NPCR and UACI using both C_1 and C_2. The results of this analysis for a complete set of test keyframes and non-keyframes are listed in Tables 1–3. The obtained results show the high level security presented by our approach. The scores exceeded the ideal score for an encryption algorithm 99.61% and 33.44% for NPCR and UACI [43], respectively. Fig. 8 shows the NPCR and UACI tests repeated 100 times for one keyframe with randomly chosen one bit change. The results confirm that any minor change of the plain keyframe can change the corresponding ciphered keyframe completely. Therefore, the proposed image encryption demonstrated good ability to resist the differential attack and can provide high-level security to the keyframe extracted using VS during WCE.

3.3. Sensibility tests

The proposed algorithm is based on a chaotic map, which is known by its sensibility for any tiny change in the initial values and controlling parameters. Therefore, all these initial values and controlling parameters are selected as secret keys in our method. To confirm that our image encryption technique has a high security level, we change one initial value or parameter of the chaotic systems slightly to analyze the effect of the ciphered image.

Please cite this article in press as: R. Hamza, et al., Secure video summarization framework for personalized wireless capsule endoscopy, Pervasive and Mobile Computing (2017), http://dx.doi.org/10.1016/j.pmcj.2017.03.011

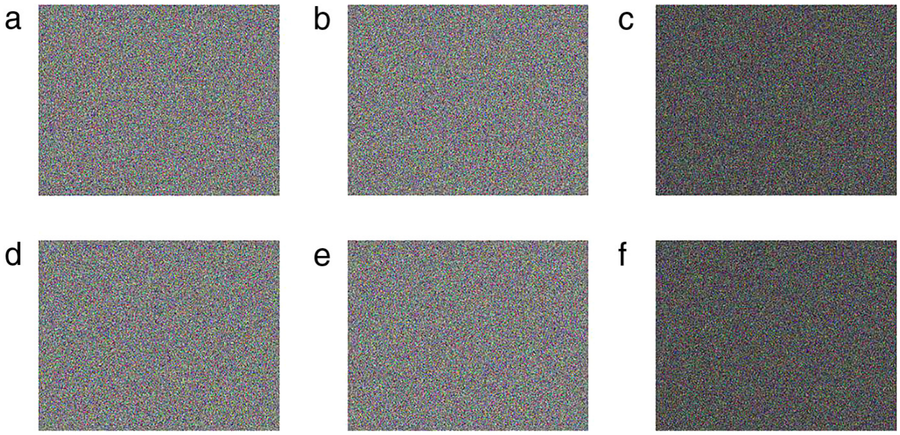

Fig. 9. Key sensitivity analysis at the encryption/decryption stage. (a) The encrypted image CI1. (b) The encrypted image CI2. (c) The image difference |CI1 − I2|. (d) The decrypted image DI1. (e) The decrypted image DI2. (f) The image difference |DI1 − DI2|.

Table 4
The secret keys sensibility tests.

Key change	x_0	y_0	υ	ε	τ
NPRC	99.6105	99.6082	99.6112	99.5966	99.6125
UACI	33.4365	33.4794	33.4825	33.4665	33.4525

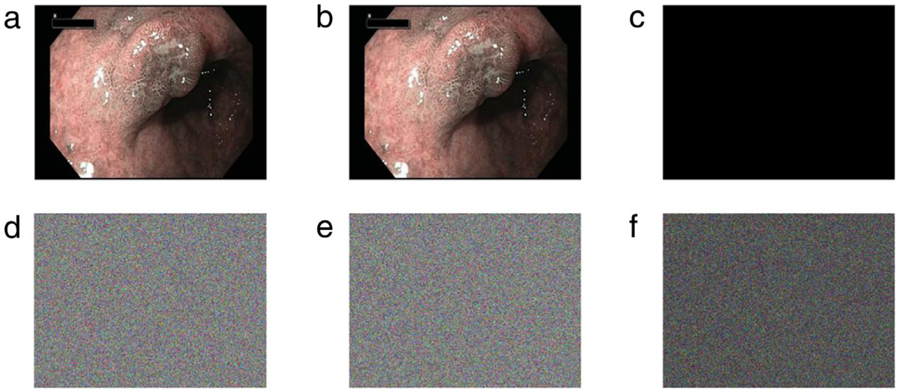

Fig. 10. Tests of the keyframe sensitivity, (a) the plain keyframe I, (b) the modified keyframe J (only in one bit compared to "I"), (c) the image difference $|I - J|$, (d) the encrypted image CI, (e) the encrypted image CJ, and (f) the image difference |CI − CJ|.

Table 4 shows the NPRC and UACI test results for pair ciphered images. The encrypted images are obtained with the same plain keyframe using a single slight change $+10^{-15}$ in one of the secret key. Fig. 9 shows some tests of sensibility on the secret keys. In order to test the encryption/decryption sensibility, we use two secret keys. Each secret key differs only in one tiny change in one of the initial values with $(+10^{-15})$. Fig. 9(a) shows the encrypted keyframe using the first secret key. Fig. 9(b) shows the encrypted keyframe using the second secret key. Fig. 9(d) shows the decrypted version of the keyframe in Fig. 9(b) using the first secret key. Fig. 9(e) shows the decrypted of the keyframe in Fig. 9(a) using the second secret key. Fig. 9(c) shows the abs mean difference between the encrypted images in Fig. 9(a), and (b). Fig. 9(f) shows the abs mean difference between the decrypted images in Fig. 9(d), and (e). The obtained image in Fig. 9(c) and (f) are without any black-zone (zero pixels), indicating no observation to any equal block between the ciphered/decrypted data. Therefore, any tiny adjustment of the secret keys can produce completely different cipher data and the only possible way to recover the original data is using the exact secret key.

In addition to the secret key sensitivity, we test the plain keyframe sensitivity in Fig. 10. Firstly, we encrypt the original keyframe as shown in Fig. 10(a). The ciphered keyframe is denoted by CI (Fig. 10(d)). Secondly, we randomly select one pixel and we change the least significant bit. The modified keyframe is denoted by J (Fig. 10(b)). Finally, Fig. 10(f) shows the abs mean image difference |CI − CJ|, where CJ is the corresponding encrypted image for J (Fig. 10(e)). The obtained image in Fig. 10(f), has no observation for a black zone, indicating the existence of non-equal blocks on the ciphered data. Therefore, the attackers cannot obtain any useful information, even with using some special attacks. The tests confirm that our proposed method is very sensitive to any tiny alteration to its secret keys as well as pixels of plain-keyframe.

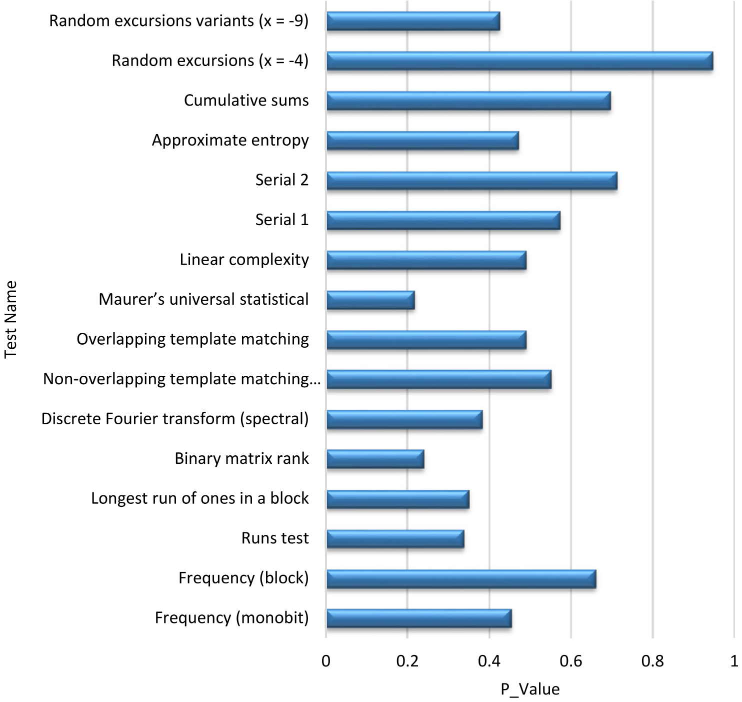

Fig. 11. Bar chart of NIST suite results for proposed method. All P-values are greater than 0.1, indicating that our method has passed all tests.

3.4. Space key

According to the IEEE floating point standard [44], the computational precision of the 64-bit double-precision numbers is about 10^{-15}. In this work, all the initial values and controlling parameters of ZCM are selected as secret keys, making the space keys for the proposed pseudo random sequence generator more than $10^{5\times 15} \simeq 2^{237}$. Moreover, we can generate each key encryption with other secret keys as we have three main encryption keys (V, V', R). This leads to a key space of around $10^{225} \simeq 2^{711}$ for the proposed algorithm, making it larger enough to withstand exhaustive attacks.

3.5. Randomness tests

The tests of NIST suite come with 15 statistical tests to prove the randomness of any sequence. The tests require binary sequence with at least 10^6 bits to find potential defects with any binary sequence, producing an output P_{value}. The values of P_{value} are confined between 0 and 1, and must be larger than 0.01 to pass the tests [45]. We have used the default values of the NIST suits tests [45]. Fig. 11 shows bar chart of NIST suite results for our proposed keyframe encryption. We produce the ciphered data using our approach and we pass all encrypted binary data to the test (7 372 800 bits). The ciphered data passed successfully all the tests of SP 800-22. These results verify that the ciphered data has better statistical characteristics and can resist various statistical attacks.

3.6. Entropy test

The pixel values of a ciphered image are expected to be uniformly distributed to achieve a high security level. Shannon's entropy [46] can measure the randomness of the ciphered data, which can be mathematically defined as follows:

$$E(C) = -\sum_{i=1}^{n} P(c_i)\log_2 P(c_i). \tag{4}$$

Herein, $P(c_i)$ is the probability of $c_i \in C$, C is a set of symbols, and "n" is the total number of symbols. To achieve high-level security, the local Shannon entropy score should be equal to 8 for a random frame with 256 gray levels [47]. The local Shannon entropy is calculated to check the level of randomness between the input image and its ciphered version. Therefore, the entropy score of an encrypted image generated by any effective encryption method should be close to 8. Tables 5 and 6 show the information related to local Shannon entropy for various ciphered keyframes and non-keyframes. All the results demonstrate that the ciphered keyframes/ non-keyframes are almost close to a random source, validating the effectiveness of our proposed scheme.

Please cite this article in press as: R. Hamza, et al., Secure video summarization framework for personalized wireless capsule endoscopy, Pervasive and Mobile Computing (2017), http://dx.doi.org/10.1016/j.pmcj.2017.03.011

Table 5
The entropy tests for a set of data keyframe.

Frame/entropy	0065	0379	0449	0485	0527	0595	0606	0659	0667	0690	700
Original	7.3656	7.4360	7.4328	7.4028	7.3647	7.3674	7.3208	7.3700	7.1773	7.2786	7.1891
Ciphered	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998

Table 6
The entropy tests for a set of data non-keyframes.

Frame/entropy	0026	0033	0046	0165	0169	0170	0180	0199	0348	0457	0676
Original	6.9921	7.2897	7.1880	6.5479	7.1084	6.5409	7.0044	7.3128	7.2388	5.4406	7.3120
Ciphered	7.9998	7.9998	7.9998	7.9998	7.9998	7.9998	7.9997	7.9998	7.9998	7.9998	7.9998

3.7. Chosen/known attack

In previous sections, we explained that our proposed algorithm has high sensitivity to any tiny modification in the plain frame as well as in its secret keys. Furthermore, no information can be obtained by cryptanalysis regardless of the attack type by malicious users because each encryption is related completely to the plain frames and the secret keys. Moreover, according to the previous tests, our proposed scheme is immune to the chosen attacks. It is a well-known fact that any cipher resistant to the chosen-plaintext attacks is considered as immune to other chosen/known attacks [48]. This confirms the better ability of the proposed method to resist chosen/known attacks.

3.8. Correlation coefficient analysis

In this sub-section, we investigate the correlation coefficient effect on the ciphered frames. The relationship between correlation and security is described as follows. "The lesser the correlation of two adjacent pixels is, the safer the ciphered frame is". Therefore, we randomly select 2048 pairs of adjacent pixels for testing the correlations between two adjacent pixels in the three directions: vertically, horizontally, and diagonally, respectively. The correlation of two adjacent pixels can be computed using Eqs. (5)–(8) as follows:

$$CC_{xy} = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)} \times D(y)} \tag{5}$$

$$\text{where, } \operatorname{cov}(x, y) = \frac{1}{n}\sum_{i=1}^{n}(x_i - E(x))(y_i - E(y)) \tag{6}$$

$$D(x) = \frac{1}{n}\sum_{i=1}^{n}(x_i - E(x))^2 \tag{7}$$

$$E(x) = \frac{1}{n}\sum_{i=1}^{n}x_i. \tag{8}$$

The test results of the plain frames and ciphered frames for each component are listed in Table 7. The correlation coefficients are all greater than 0.98 in the original frames, indicating strong correlation between adjacent pixels of each direction in plain frames. On the other hand, the correlation coefficients are all almost 0.001 in the ciphered frames, representing negligible correlation and nearby to the ideal value ($CC = 0$) for an encrypted frame [13]. Fig. 12 illustrates the plot of the correlation distribution for the plain frame and its corresponding ciphered frame. The strong correlation between adjacent pixels is obvious with agglomeration of the dots for the plot of the plain frame. However, in case of ciphered frame, the dots are scattered over the entire plot. Therefore, our proposed method can efficiently minimize the strong correlation between adjacent pixels of the plain frames.

4. Comparison tests

In this section, we evaluate the performance of our proposed method by conducting several tests based on image quality and other evaluation metrics. The metrics for comparative study include mean square error (MSE) [49], structural similarity index metric (SSIM) [50], NCC [51], NPCR, UACI, entropy, and correlation coefficient [47,52,53]. The mathematical equations for the last three metrics are already given in previous sub-sections. The remaining three metrics (MSE, SSIM, and NCC) can be computed using Eqs. (9)–(11) as follows:

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}\left(I_{xy} - E_{xy}\right)^2 \tag{9}$$

Table 7
The correlation coefficient of adjacent pixels tests.

Keyframe#	Component	Keyframe			Ciphered		
		Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
0065	R	0.9931	0.9907	0.9856	0.0028	−0.0016	8.609e−04
	G	0.9886	0.9847	0.9764	−3.991e−04	1.833e−04	−0.0019
	B	0.9872	0.9828	0.9735	0.0017	0.0047	0.0013
0379	R	0.9963	0.9944	0.9919	−8.509e−04	−7.219e−04	−7.116e−04
	G	0.9929	0.9900	0.9853	0.0013	−7.229e−04	−0.0034
	B	0.9913	0.9881	0.9824	−0.0040	0.0013	6.472e−04
0527	R	0.9917	0.9914	0.9849	−0.0042	−0.0022	9.524e−04
	G	0.9860	0.9862	0.9754	−7.046e−05	−0.0019	−6.470e−04
	B	0.9843	0.9846	0.9726	−0.0021	−0.0025	0.0030

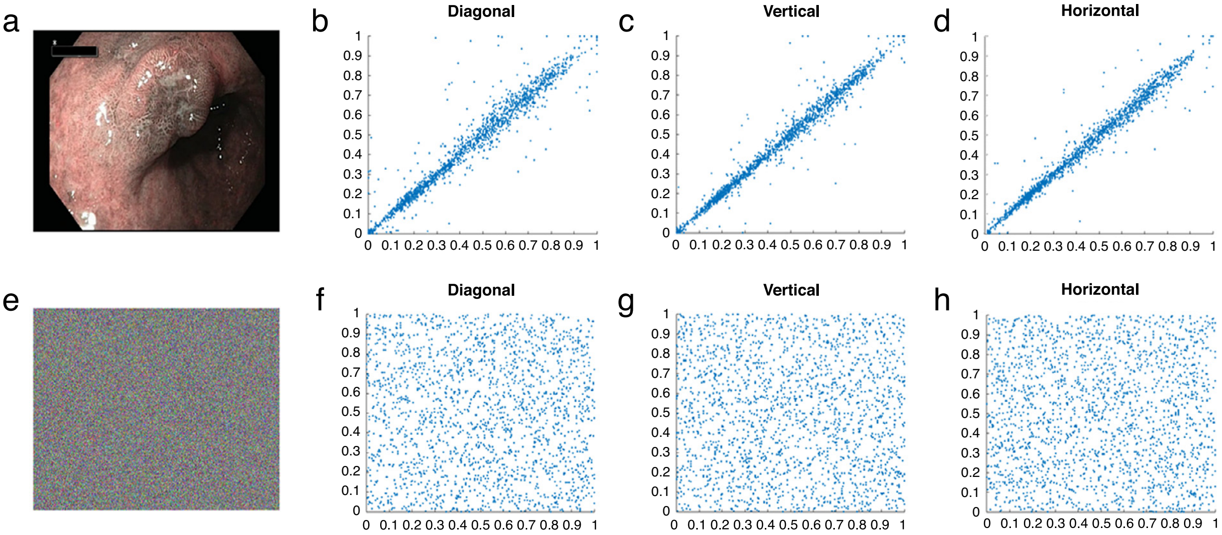

Fig. 12. Correlation coefficient diagrams (blue channel). (a) Keyframe, (b), (c), (d) correlation distribution for keyframe in diagonal, vertical, and horizontal direction, respectively. (e) Ciphered keyframe, (f), (g), (h) correlation distribution for ciphered keyframe in diagonal, vertical, and horizontal direction, respectively. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

$$NCC = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N}\left(E_{xy} \times I_{xy}\right)}{\sum_{x=1}^{M}\sum_{y=1}^{N}\left(E_{xy}\right)^{2}} \tag{10}$$

$$SSIM = \frac{\left(2\mu_x\mu_y + const_1\right) \times \left(2\sigma_{xy} + const_2\right)}{\left(\mu_x^2 + \mu_y^2 + const_1\right) \times \left(\sigma_x^2 + \sigma_y^2 + const_2\right)}. \tag{11}$$

Herein, I is the input frame, E is encrypted frame, x and y are loop counters, M and N show frame dimension, and $const_1$ and $const_2$ avoid division by zero exception. MSE should be as minimum as possible for better performance. Conversely, the value of NCC and SSIM should be as closer to 1 as possible [52,54].

In the comparison tests, initialization steps were introduced by packing the corresponding matrices of RGB frames into one matrix. The Matlab source code for other papers was obtained and the tests were performed on the same data keyframe using the same configurations for fair evaluation and comparison. Table 8 tabulates the performance values of the cipher-keyframe encrypted by different image encryption schemes [10,37,40,41]. All the presented image encryption schemes in Table 8 have good confusion and diffusion properties. Each scheme has the same entropy and NCC score. The correlation coefficient values are approximately zero for all reviewed schemes. However, there is some variation in the MSE and SSIM tests, where the performance of our proposed scheme is better than Zhou et al. [10] and Zhou et al. [41]. The authors in [41] have used a random pixel insertion in the beginning of each row in the original image, which led to the highest score of MSE among the methods under consideration.

The recent existing schemes [10,37,41] are computationally complex in terms of encryption and decryption compared to our proposed method for keyframes encryption. The proposed framework of WCE is a real-time procedure, requiring real-time fast response in terms of encryption. Therefore, these methods cannot be used in the proposed framework. The

Table 8
Comparison of the proposed image encryption method with recent state-of-the-art encryption algorithms based on multiple performance evaluation metrics.

Method name	Space keys	Time encrypt (s)	Time decrypt (s)	MSE	SSIM	NCC	NPCR	UACI	Entropy	Correlation coefficient
Our	2^{711}	2.58	2.65	0	1	1	99.609	33.450	7.9998	0.0019
Wu et al. [37]	2^{256}	180.60	180.97	0	1	1	99.613	33.409	7.9998	0.0014
Zhou et al. [40]	2^{215}	1.3831	1.6248	0	1	1	99.609	33.434	7.9998	0.0013
Zhou et al. [41]	2^{265}	8.642	5.3614	97.2274	0.9770	1	99.686	33.246	7.9998	0.0008
Zhou et al. [10]	2^{256}	41.0262	41.5787	0.0763	0.9999	1	99.605	33.490	7.9998	0.0026

method introduced in [40] has lower execution time compared to our method, however, its key space is too short, making its security limited for the proposed sensitive WCE framework according to Kirchhoff's principle [55]. Moreover, our key space is also better than the other methods mentioned in Table 8. This validates the suitability of the proposed encryption method for integration with the proposed video summarization assisted WCE procedure for healthcare centers.

5. Conclusion

In this paper, we formulated the problem of effective management of wireless capsule's data and its secure dissemination to remote health monitoring centers for personalized WCE. Considering the limited resources during WCE such as smartphone's battery, processing, and transmission cost, an energy-efficient video summarization algorithm is devised to automatically extract the keyframes from the sequence of WCE frames. The proposed VS scheme is based on integral-image, which is a light-weight process, making it more suitable for real-time application such as WCE. Next, we proposed a cryptosystem for secure dissemination of the keyframes extracted using our VS scheme to gastroenterologists and healthcare centers. We used the 2D chaotic map to generate the permutation keys, which shift the position of the plain keyframe pixels, followed by diffusion per block using the arithmetic matrix multiplication over finite field. The proposed method has a larger key space with high sensitivity to any tiny modification. Any minor bit adjustment on the original keyframe can produce completely different ciphered keyframe. Moreover, the proposed cryptosystem scheme has a higher ability to resist the chosen/known attacks and differential attacks. The proposed encryption method is fast and provides a high level of security with large space keys compared to other state-of-the-art encryption schemes. These characteristics verify the suitability of our framework for secure dissemination of the keyframes to healthcare centers and remote gastroenterologists, facilitating them with correct real-time decisions, leading to improved healthcare facilities.

The current work considers fixed block size of 32 × 32 pixels, which can be made adaptive in future work. We also tend to investigate the suitability of our method for integration with steganographic techniques [56–58], compression, and watermarking algorithms [54,59]. Finally, we plan to apply the current encryption scheme with further improvements to the keyframes of diagnostic hysteroscopy videos.

References

[1] X. Zhang, Separable reversible data hiding in encrypted image, IEEE Trans. Inf. Forensics Secur. 7 (2012) 826–832.
[2] A. Gutub, A. Al-Qahtani, A. Tabakh, Triple-A: Secure RGB image steganography based on randomization, in: IEEE/ACS International Conference on Computer Systems and Applications, 2009. AICCSA 2009. 2009, pp. 400–403.
[3] 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 Appl. 75 (2016) 14867–14893.
[4] S.A. Parah, J.A. Sheikh, A.M. Hafiz, G. Bhat, Data hiding in scrambled images: A new double layer security data hiding technique, Comput. Electr. Eng. 40 (2014) 70–82.
[5] R. Hamza, F. Titouna, A novel sensitive image encryption algorithm based on the Zaslavsky chaotic map, Inf. Secur. J.: Global Perspect. 25 (2016) 162–179. http://dx.doi.org/10.1080/19393555.2016.1212954, 2016/12/01.
[6] A.A.-A. Gutub, F.A.-A. Khan, Hybrid Crypto Hardware Utilizing Symmetric-Key and Public-Key Cryptosystems, in: 2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT), 2012, pp. 116–121.
[7] 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. 243–250.
[8] M.T. Parvez, A.A.-A. Gutub, Vibrant color image steganography using channel differences and secret data distribution, Kuwait J. Sci. Engrg. 38 (2011) 127–142.
[9] N.A. Al-Otaibi, A.A. Gutub, 2-Leyer security system for hiding sensitive text data on personal computers, Lect. Notes Inform. Theory 2 (2014).
[10] Y. Zhou, Z. Hua, C.-M. Pun, C.P. Chen, Cascade chaotic system with applications, IEEE Trans. Cybern. 45 (2015) 2001–2012.
[11] N.K. Pareek, V. Patidar, K.K. Sud, Image encryption using chaotic logistic map, Image Vis. Comput. 24 (2006) 926–934.
[12] T. Shah, An algorithm based on 1D chaotic system and substitution box, Signal Process. 117 (2015) 219–229.
[13] 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 Appl. 71 (2014) 1469–1497.
[14] Y. Wu, Y. Zhou, J.P. Noonan, S. Agaian, Design of image cipher using latin squares, Inform. Sci. 264 (2014) 317–339.
[15] R. Bechikh, H. Hermassi, A.A. Abd El-Latif, R. Rhouma, S. Belghith, Breaking an image encryption scheme based on a spatiotemporal chaotic system, Signal Process., Image Commun. 39 (Part A) (2015) 151–158. 11//.

Please cite this article in press as: R. Hamza, et al., Secure video summarization framework for personalized wireless capsule endoscopy, Pervasive and Mobile Computing (2017), http://dx.doi.org/10.1016/j.pmcj.2017.03.011

[16] Y.-G. Yang, X. Jia, P. Xu, J. Tian, Analysis and improvement of the watermark strategy for quantum images based on quantum Fourier transform, Quantum Inf. Process. 12 (2013) 2765–2769.

[17] M. Ali, C.W. Ahn, Comments on Optimized gray-scale image watermarking using DWT-SVD and Firefly Algorithm', Expert Syst. Appl. 42 (2015) 2392–2394. 4/1/.

[18] C. Zhu, A novel image encryption scheme based on improved hyperchaotic sequences, Opt. Commun. 285 (2012) 29–37.

[19] J. Qi, P. Yang, M. Hanneghan, S. Tang, Multiple density maps information fusion for effectively assessing intensity pattern of lifelogging physical activity, Neurocomputing 220 (2017) 199–209.

[20] J. Qi, P. Yang, D. Fan, Z. Deng, A survey of physical activity monitoring and assessment using internet of things technology, in: 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), 2015, pp. 2353–2358.

[21] P. Yang, D. Stankevicius, V. Marozas, Z. Deng, E. Liu, A. Lukosevicius, et al., Lifelogging data validation model for internet of things enabled personalized healthcare, IEEE Trans. Syst. Man Cybern.: Syst. (2016) https://doi.org/10.1109/TSMC.2016.2586075.

[22] L. Atzori, A. Iera, G. Morabito, The Internet of things: A survey, Comput. Netw. 54 (2010) 2787–2805.

[23] M. Sajjad, K. Muhammad, S.W. Baik, S. Rho, Z. Jan, S.-S. Yeo, et al., Mobile-cloud assisted framework for selective encryption of medical images with steganography for resource-constrained devices, Multimedia Tools Appl. 76 (2016) 3519–3536.

[24] 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, J. Med. Syst. 40 (2016) 1–16.

[25] A. Wang, S. Banerjee, B.A. Barth, Y.M. Bhat, S. Chauhan, K.T. Gottlieb, et al., Wireless capsule endoscopy, Gastrointest. Endosc. 78 (2013) 805–815.

[26] M.R. Basar, F. Malek, K.M. Juni, M.S. Idris, M.I.M. Saleh, Ingestible wireless capsule technology: A review of development and future indication, Int. J. Antennas Propag. 2012 (2012) http://dx.doi.org/10.1155/2012/807165.

[27] I. Mehmood, M. Sajjad, S.W. Baik, Mobile-cloud assisted video summarization framework for efficient management of remote sensing data generated by wireless capsule sensors, Sensors 14 (2014) 17112–17145.

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

[29] K. Muhammad, M. Sajjad, M.Y. Lee, S.W. Baik, Efficient visual attention driven framework for key frames extraction from hysteroscopy videos, Biomed. Signal Process. Control 33 (2017) 161–168.

[30] J. Yang, Y. Chen, W. Trappe, J. Cheng, Detection and localization of multiple spoofing attackers in wireless networks, IEEE Trans. Parallel Distrib. Syst. 24 (2013) 44–58.

[31] J.-J. Yang, J. Li, J. Mulder, Y. Wang, S. Chen, H. Wu, et al., Emerging information technologies for enhanced healthcare, Comput. Ind. 69 (2015) 3–11.

[32] Z. Lv, J. Chirivella, P. Gagliardo, Bigdata oriented multimedia mobile health applications, J. Med. Syst. 40 (2016) 1–10.

[33] A. Buke, F. Gaoli, W. Yongcai, S. Lei, Y. Zhiqi, Healthcare algorithms by wearable inertial sensors: a survey, Commun. China 12 (2015) 1–12.

[34] M. Sajjad, I. Mehmood, S.W. Baik, Sparse representations-based super-resolution of key-frames extracted from frames-sequences generated by a visual sensor network, Sensors 14 (2014) 3652–3674.

[35] I. Mehmood, M. Sajjad, S.W. Baik, Video summarization based tele-endoscopy: a service to efficiently manage visual data generated during wireless capsule endoscopy procedure, J. Med. Syst. 38 (2014) 1–9.

[36] Y.B. Pesin, Characteristic Lyapunov exponents and smooth ergodic theory, Russian Math. Surveys 32 (1977) 55–114.

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

[38] M.-H. Jing, J.-H. Chen, Z.-H. Chen, Y. Chang, The secure DAES design for embedded system application, in: International Conference on Embedded and Ubiquitous Computing, 2007, pp. 617–626.

[39] M. Spain, M. Varia, Diversity within the Rijndael design principles for resistance to differential power analysis, in: International Conference on Cryptology and Network Security, 2016, pp. 71–87.

[40] Y. Zhou, L. Bao, C.P. Chen, Image encryption using a new parametric switching chaotic system, Signal Process. 93 (2013) 3039–3052.

[41] Y. Zhou, L. Bao, C.P. Chen, A new 1D chaotic system for image encryption, Signal Process. 97 (2014) 172–182.

[42] G. Zhang, Q. Liu, A novel image encryption method based on total shuffling scheme, Opt. Commun. 284 (2011) 2775–2780.

[43] 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, Opt. Express 20 (2012) 2363–2378.

[44] D.H. Bailey, High-precision floating-point arithmetic in scientific computation, Comput. Sci. Eng. 7 (2005) 54–61.

[45] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, DTIC Document, 2001.

[46] C.E. Shannon, A mathematical theory of communication, ACM SIGMOBILE Mob. Comput. Commun. Rev. 5 (2001) 3–55.

[47] F. Sun, Z. Lü, S. Liu, A new cryptosystem based on spatial chaotic system, Opt. Commun. 283 (2010) 2066–2073.

[48] X. Wang, L. Teng, X. Qin, A novel colour image encryption algorithm based on chaos, Signal Process. 92 (2012) 1101–1108.

[49] A.A.-A. Gutub, Pixel indicator technique for RGB image steganography, J. Emerg. Technol. Web Intell. 2 (2010) 56–64.

[50] R.J. Mstafa, K.M. Elleithy, A video steganography algorithm based on Kanade-Lucas-Tomasi tracking algorithm and error correcting codes, Multimedia Tools Appl. 75 (2015) 10311–10333.

[51] K. Muhammad, J. Ahmad, H. Farman, Z. Jan, M. Sajjad, S.W. Baik, A secure method for color image steganography using gray-level modification and multi-level encryption, KSII Trans. Internet Inf. Syst. (TIIS) 9 (2015) 1938–1962.

[52] 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 Appl. 76 (2016) 8597–8626.

[53] J. Yang, Y. Lin, Z. Gao, Z. Lv, W. Wei, H. Song, Quality index for stereoscopic images by separately evaluating adding and subtracting, PLoS One 10 (2015) e0145800.

[54] Z. Liu, F. Zhang, J. Wang, H. Wang, J. Huang, Authentication and recovery algorithm for speech signal based on digital watermarking, Signal Process. 123 (2015) 157–166.

[55] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, S.W. Baik, Image steganography using uncorrelated color space and its application for security of visual contents in online social networks, Future Gener. Comput. Syst. (2016) http://dx.doi.org/10.1016/j.future.2016.11.029.

[56] K. Muhammad, J. Ahmad, S. Rho, S.W. Baik, Image steganography for authenticity of visual contents in social networks, Multimedia Tools Appl. (2017) 1–20. http://dx.doi.org/10.1007/s11042-017-4420-8.

[57] R.J. Mstafa, K.M. Elleithy, A highly secure video steganography using Hamming code (7, 4), in: Systems, Applications and Technology Conference (LISAT), 2014 IEEE Long Island, 2014, pp. 1–6.

[58] K. Muhammad, J. Ahmad, M. Sajjad, M. Zubair, Secure image steganography using cryptography and image transposition, NED Univ. J. Res. 12 (2015) 81–91.

[59] C.-C. Lin, X.-L. Liu, S.-M. Yuan, Reversible data hiding for VQ-compressed images based on search-order coding and state-codebook mapping, Inform. Sci. 293 (2015) 314–326.