IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 26, 2019, accepted March 27, 2019, date of publication April 15, 2019, date of current version May 1, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2909554

Chaos Based Enhanced RC5 Algorithm for Security and Integrity of Clinical Images in Remote Health Monitoring

ROMANA SHAHZADI[1], SYED MUHAMMAD ANWAR[2], FARHAN QAMAR[1], MUDASSAR ALI[1], AND JOEL J. P. C. RODRIGUES[3,4,5], (Senior Member, IEEE)

[1]Department of Computer Engineering, University of Engineering and Technology at Taxila, Taxila 47050, Pakistan
[2]Department of Software Engineering, University of Engineering and Technology at Taxila, Taxila 47050, Pakistan
[3]National Institute of Telecommunications–Inatel, Santa Rita do Sapucaí 37540-000, Brazil
[4]Instituto de Telecomunicações, 1049-001 Lisbon, Portugal
[5]PPGEE, Federal University of Piauí, Campus Ministro Petrônio Portella, Teresina 64049-550, Brazil

Corresponding authors: Farhan Qamar (farhan.qamar@uettaxila.edu.pk) and Mudassar Ali (mudassar.ali@hotmail.com)

This work was supported in part by the National Funding from the FCT-Fundação para a Ciência e a Tecnologia through the UID/EEA/50008/2019 Project, in part by the Rede Nacional de Pesquisa (RNP), with resources from the Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC), under the Centro de Referência em Radiocomunições–CRR Project of the Instituto Nacional de Telecomunicações–Inatel, Brazil, under Grant 01250.075413/2018-04, and in part by the Brazilian National Council for Research and Development (CNPq) via under Grant 309335/2017-5.

ABSTRACT The demand for remote health monitoring will significantly increase in the near future due to a decrease in the doctor/patient ratio as the world population grows. In remote health monitoring, one of the major goals is to send patient's data to clinical experts at geographically distant locations. In this scenario, the importance of implementing security on patients' clinical information increases, so that this could not be either changed or read by an unauthorized person. Rivest Cipher (RC5) algorithm is a secure and simple encryption algorithm. Due to its simplicity, fast encryption, and low memory requirements, it is considered as a suitable block cipher for resource constraint environments, such as body area networks (BAN), although it can be broken by various attacks due to poor diffusion. In this paper, we propose a chaotic-based key scheduling algorithm for the RC5 in which round keys are generated based on 2-D chaotic maps and used as a symmetric key during the encryption and decryption process. Cipher feedback mode is adapted to further increase the diffusion property of the cipher. This chaos-based key is very difficult to trace, and the cipher is extremely hard to break. A strict security analysis of the proposed cipher is performed against several attacks. The experimental results have shown that the impact of this approach is significantly better than the conventional security mechanisms in case of BAN when applied to critical clinical images.

INDEX TERMS Remote health monitoring, encryption, clinical images, wireless body area networks (WBAN), RC5, 2D-chaotic map.

I. INTRODUCTION

According to the world health organization, e-health monitoring comprises of information and communication technology (ICT) based systems, which can solve problems currently faced by low- and middle-income underdeveloped countries. These include shortage of health staff in remote areas, health care quality, emergency checkups, patient compliance and scams [1]. It is forecasted that the population of people aged above 60 years will be doubled by 2025 compared to the numbers in 1990 [2]. Thereby, providing an effective and reliable health care system, at low or same cost as of today would become a serious challenge. It is reported that more than 30% of the worldwide deaths related to heart problems can be diagnosed and prevented by using efficient, trustworthy, and health monitoring systems that are available in a timely manner [3]. Therefore, remote health monitoring systems can bring a significant change in human life through real time monitoring and early detection of patient's health. However, when deploying remote health monitoring systems, it is not acceptable to compromise on the standards currently used in

The associate editor coordinating the review of this manuscript and approving it for publication was Sajjad A. Madani.

the clinical practice. The security and integrity of the patient information is a key concern, while designing or deploying a remote health monitoring system. This is to make sure that a clinical expert located remotely could take an accurate decision, which is rightly based on authentic data. Many encryption techniques have been proposed for medical text data encryption [4], however for medical images such as magnetic resonance imaging (MRI), X-ray and computed tomography (CT), a lot of work still needs to be done.

To ensure security of patient's critical data Rivest Cipher (RC5) algorithm is considered a well-known cipher in terms of efficiency and overall performance [5]– [7]. It is simple, easy and beneficial in terms of implementation as compared to other block ciphers. It does not require huge tables or large multiplications, therefor the encryption process is computationally less complex and inexpensive to implement. RC5 is also suitable for a resource constrained environment such as sensor-based applications due to very low power, less memory usage and easy adaptability [8], [9]. However, RC5 can be broken by attackers due to its poor diffusion property in key computation [10], [11]. This can be overcome by using RC5 in combination with chaos to enhance the security level, where chaos sequences can be used for ciphering of medical images [12].

Chaos was first used in the field of cryptography by using a 1-D chaotic system, which generated chaos-based steam cipher [13]. Since then many chaos-based cryptographic techniques have been suggested and implemented for data encryption. Features such as confusion and diffusion make chaos based cryptographic systems highly secure and reliable [14], [15].

Image encryption using chaotic maps is based on the generation of pseudorandom sequence numbers, which is highly dependent on the initial condition. The complexity of a system can be further increased by controlling different parameters. Similarly, while decrypting data at the receiving side, these initial conditions play an important role [4]. A minor mismatch between the initial conditions at the encrypting and decrypting side can completely change the set of random numbers. Thus, a perfect synchronization between the encryption and decryption process is a key for chaos based cryptographic system [16]. 1-D chaotic maps are used for basic encryption, which can be used to generate secret keys [17], and are represented as follows,

$$a_{n+1} = \lambda \times a_n(1 - a_n), \quad \lambda \in [0, 4], \; a_n \in [0, 1], \qquad (1)$$

where 'λ' represents a control parameter to handle the chaos behavior, 'a_o' represents the initial conditions, 'a_n' is the system output at any value of 'n'. The bifurcation diagram for 1-D chaotic maps is given in Fig. 1, where the horizontal axis shows system parameters represented as $a_n = [0, 1]$, and the vertical axis represents the trajectory of the logistic maps. The system shows changed chaotic behaviors at different ranges of control parameter i.e.,

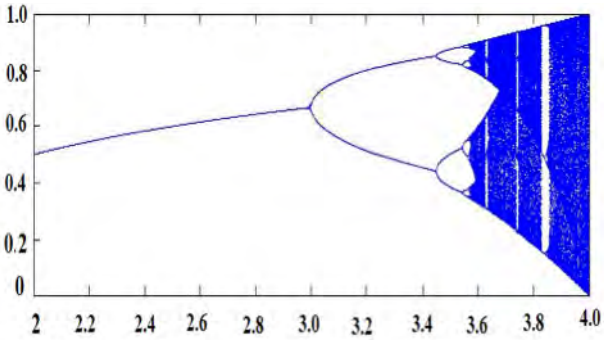

FIGURE 1. Bifurcation diagram for 1-D chaotic maps.

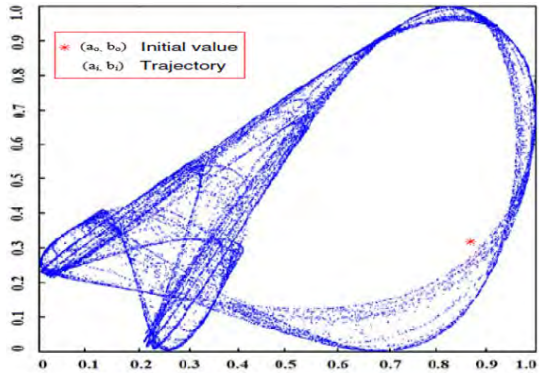

FIGURE 2. Bifurcation diagram for 2-D chaotic maps.

- For $\lambda \in [0 - 2, 3]$
  System shows no chaotic behavior, hence cannot be used for the proposed model of image encryption.
- For $\lambda \in [3, 3.6]$
  Above a value 3.0, the system starts to bifurcate until 3.6, a quasiperiodic behavior is observed.
- For $\lambda \in [3.6, 4]$
  The system seems to be fully chaotic and can be used to generate the required random keys.

2-D chaotic logistic maps are much more complex as compared to the 1-D chaotic maps and represent a highly non-linear and complex dynamical system. The bifurcation diagram for a 2-D chaotic map is shown in Fig 2, which is a scatterplot of 30,000 points from the trajectory of a 2-D logistic map using parameter $\lambda = 1.19$ and initial values (a_o, b_o) at (0.89, 0.33) [18]. Mathematically, these maps are represented as follows, where 'λ' represents the control parameter to handle the

$$a_{n+1} = \lambda(3b_n + 1)\, a_n(1 - a_n) \qquad (2)$$

$$b_{n+1} = \lambda(3a_{n+1} + 1)\, b_n(1 - b_n) \qquad (3)$$

chaos behavior and (a_n, b_n) represents the pair of points for n^{th} iteration. The chaotic behavior of 2-D logistic map can be analyzed as,

- For $\lambda \in [-1, 1]$
  Both x and y axis show unstable manifolds.
- For $\lambda = 1$
  The plot follows Neimark Hopf bifurcation.

- For $\lambda \in [1, 1.11]$
  System indicates repulsive behavior and oscillations have started.
- For $\lambda \in [1, 1.19]$
  Logistic mapping shows complete chaotic behavior at this system parameter range, which is of specific interest for the proposed model.

Due to the greater complexity of 2-D logistic maps, these maps are well suited for producing chaotic keys as compared to 1-D maps. These 2-D maps provide greater space for generating keys due to the availability of two dimensions and a greater number of initial conditions. Hence, the proposed image encryption algorithm uses these 2-D maps. Lyapunov exponents are used to predict the chaotic behavior for 1-D and 2-D chaotic maps. The Lyapunov toolbox in MATLAB is used for this purpose, where exponents are measured with respect to each eigen value. A higher positive value of the Lyapunov exponent shows a greater chaotic behavior of the system [19].

The major contributions of this study are as follows:

1. The security of a simple RC5 algorithm is enhanced by introducing a strong chaotic key generation mechanism. This improves the diffusion property of the algorithm making it robust against various attacks
2. The proposed algorithm is used for the first time to the best of our knowledge in remote health monitoring to make clinical images secure.
3. The proposed work is also useful in a sense that, in addition to normal clinical images it takes 1-D physiological signals i.e. ECG/EEG to send them in the form of images, which eliminates or at least reduces the chances of error while interpretation of these signals at the receiving side.
4. The performance of the proposed algorithm is compared with RC5 algorithm and the effectiveness is proved through different security analysis tests.

The rest of the paper is arranged in the following order. Section-II presents background and related work. Section-III shows the proposed setup for simulations. Results and discussions are presented in Section-IV, followed by conclusions in Section-V.

II. BACKGROUND AND RELATED WORK

Remote health monitoring is an emerging field, where sensors and devices are used to get medical data such as blood pressure, intracranial pressure and heart beat rate. This data is wirelessly transferred for further processing and analysis. Advances in recent technology and very large-scale integration of physical sensors and microprocessors on a single chip has enabled a new field based on sensor networks, which is suitable for a wide variety of new applications [20].

E-health sensors attached to a patient's body are equipped with a radio trans-receiver, memory, microcontroller and power supply, which form a network called wireless body area network (WBAN). These sensors can be further divided into two main categories of implantable devices and wearable devices [21]. Implantable devices can be implanted invasively in the body through surgery, while wearable devices are non-invasively attached with a patient's body [22]. The patient data is highly sensitive therefore, security issues are a major concern in such type of networks. For the best possible care, the right information at the right time is required. An unauthorized person can access and change this data, which not only is an attack on the patient privacy but could also leads to unwanted clinical outcomes. Therefore, maintaining the security and integrity of data is a primary requirement in e-health systems. Some important schemes/protocols proposed by different researchers in this area are listed in Table 1, where the benefits and the disadvantages of these systems are highlighted.

III. PROPOSED SCHEME

The aim of e-health technology is to reduce medical expenses by integrating different technologies such as communication, computer, and multimedia technology with medical diagnosis and analysis methods. Although, different types of e-health architectures have been proposed in literature but generally all e-health systems mainly consist of sensors, remote medical health monitoring server (R-MHMS) and a communication medium between the sensors and the R-MHMS. The proposed architecture for secure remote health monitoring of clinical images is presented in Fig 3. In view of the future requirements, where global clinical consultation would be preferred, medical imaging acquisition systems are also included in the proposed architecture. These could be placed at near the patient premises or in a clinic geographically located at a far-off place from the clinical expert with whom the medical data needs to be shared.

In the proposed architecture both sides process digital information for the ease of exchange of data. Health information is collected by using different types of sensors placed on a patient body and medical image acquisition machines. E-health monitoring sensors are of different types and mainly classified into two categories. Implantable sensors are invasive and used to measure force, pressure, torque and temperature of the human body. These sensors include pacemakers, endoscope capsules and biosensors to measure the metabolite level in a diabetic patient to name a few [4]. Wearable sensors can be deployed non-invasively over the human body. These sensors include electrocardiogram (ECG), electroencephalography (EEG), blood pressure (BP), blood oxidation level (SpO2) and breath sensors. Image acquisition machines include X-ray, ultrasound, CT-Scan and MRI and can be used to get clinical images near the patient premises, which could be sent to a distant place for clinical diagnosis.

Keeping in view the power, communication range and data limitations of these sensors a central node or hub is used to collect data from these attached sensors. The collected data is transferred to the proposed data aggregation and processing unit, whose function is to convert sensor data into image and collect images from clinical imaging devices.

TABLE 1. Related security schemes/protocols for BAN in e-health.

Sr.#	Authors	Properties/Benefits of encryption protocols/schemes	Disadvantages
1	Murillo-Escobar [24]	Encryption/decryption time is minimized.	Applicable to clinical signals only.
2	Sufi et al. [25]	Multi-scroll type chaos is utilized to encrypt ECG data.	Difficult to extract ECG signal from chaos during decryption.
3	Jin-Meng [26]	Protocol for authentication, uses scheme based on pre-shared passwords.	Cost of computing is high.
4	Zhaoyang Zhang et al. [27]	No key distribution overhead, energy efficient.	Limited to ECG signals only, susceptible to errors during decryption.
5	Jing wei et al. [28]	Protocol use no certificate for authentication, it uses user index instead of user identity.	Very complex algorithm.
6	Lu-Zhang et al. [29]	Light-weight mutual authentication protocol, certificateless, it allows user authentication for BNC access.	Greater computational complexity due to a complex algorithm.
7	Faragallah [30]	Strengthening of diffusion and confusion operation by combining cryptographic primitive operation and chaos.	Security lack due to absence of cipher feedback mode.
8	Sathya D. et al [31]	Combines the symmetric algorithm and attribute-based encryption.	Due to the use of symmetric algorithm, key distribution is an issue for large number of users.
9	Krishna K. Venkata subramania n et al. [32]	Initialization not required, specially designed for the use of army personals.	Difficult hardware implementation. Based on scheme of fuzzy vault.
10	S.M Razi et al. [33]	Uses three types of keys for data confidentiality, integrity & security. It is distributed key management protocol.	High computation cost.
11	M. Mana et al. [34]	Useful in energy saving, ensure secure link.	Complexity due to four phases.
12	Lin Yao [35]	Low Latency, Random, Fuzzy, High tolerance against noise. Temporal and distinctive variant keys.	Not effective in non-reputation attacks & replaying.
13	Ming et al. [36]	No additional hardware requirement, effective in communication and computing. Based on group pairing keys.	Difficult key management in pairing of group devices.
14	Zhao yang et al. [37]	Secure communication, no key distribution, plug n play, energy efficient	Extracted attributes are not impressive, vault size problem.
15	Chunqiang Hu [38]	Efficient & secure protocol. Ordered, no pre-key distribution requirement, less computing cost, less memory storage required. Overall low overhead in communication.	Key establishment problem if sending features are not in accordance with receiver.
16	Sofia et al. [39]	Authentication protocol based on ECG, No chance of data mixing of two or more patients.	Authentication in addition to data integrity.
17	Jingwei et al. [40]	An efficient secure approach by combining the attributes of symmetric & asymmetric keys at a time.	Complexity due to hybrid scheme.
18	Abdulaziz et al. [41]	Procedure of key management is fast less complex.	Authentication not provided properly.

In the proposed work, security is applied on EEG and ECG signals in addition to CT and MR images. The EEG and ECG signals are first converted into 2-D signals or images, whereas medical images for brain and abdomen regions are acquired from MRI and CT scans, respectively. One of the advantages of converting sensor data into images is that the information is transmitted in its original form. There are other ways to secure the signals, where they can be transformed into a noise like signal. These noisy representations could not be interrupted by intruders, but in such cases the signal

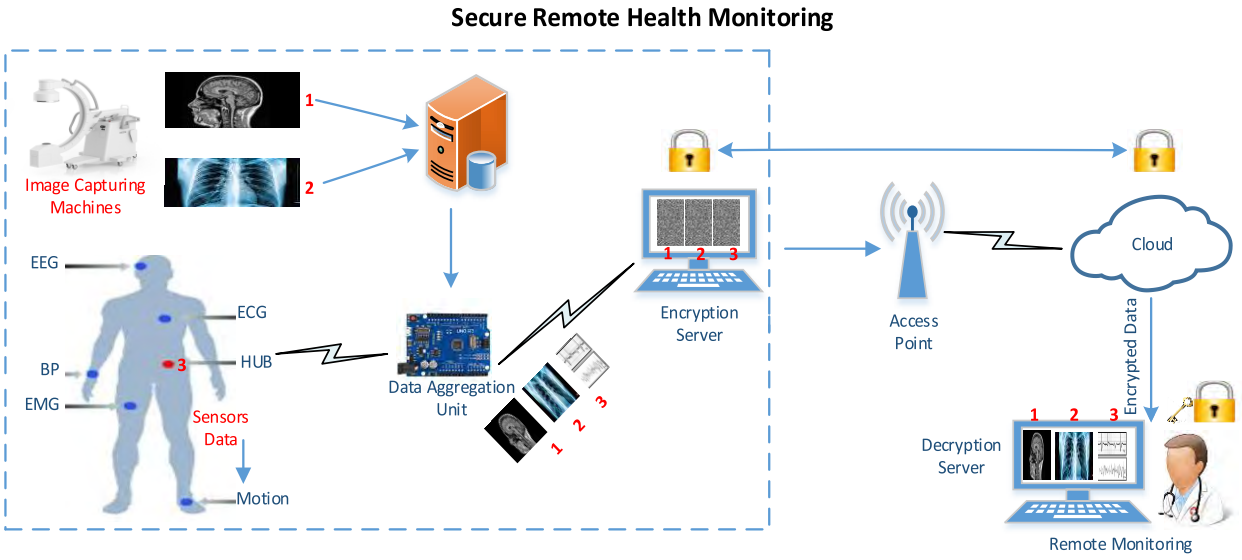

FIGURE 3. Proposed e-heath architecture.

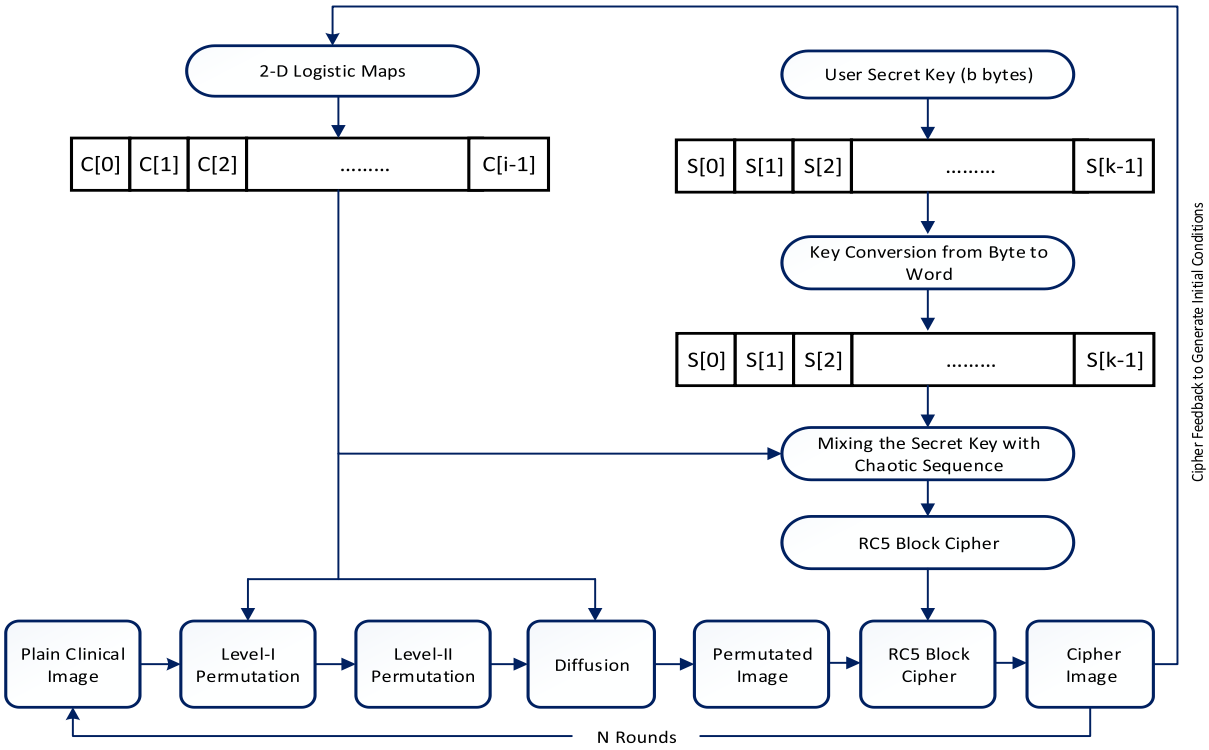

FIGURE 4. Encryption process.

transformation may results in a loss of information either due to the medium or during the encryption/decryption processes. Due to the critical nature of EEG and ECG signals, such loss of information cannot be afforded. We consider WBAN architecture as a core part of our proposed architecture.

The encryption scheme for the proposed architecture is shown in Fig 4, which consists of two main phases. The chaotic key generation is based on 2D logistic map and the encryption phase uses the RC5 encryption algorithm. RC5 is a symmetric block cipher in which the same cryptographic key is used for both the encryption and decryption process. It is a parameterized algorithm and is denoted by RC5-w/r/b, where 'w' indicates word size, 'r' represents number of rounds and 'b' shows the number of bytes in private key. Table 2. shows these parameters and their values.

The RC5 algorithm is based on three steps i.e., expansion of key, encryption and decryption of data. The encryption

TABLE 2. RC5-w/r/b parameters.

Parameters	Description	Values
w	Word size (bits)	16, 32, 64
r	Total no. of rounds	0, 1, 2, 3….255
b	No. of bytes in a secret key	0, 1, 2, 3….255

TABLE 3. Primitive operations of RC5.

Notation	Meaning
X+Y	Integer addition modulo 2w
X-Y	Integer subtraction modulo 2w
X⊕Y	Bit-wise XOR of w-bit words
X*Y	Integer multiplication modulo 2w
X<<<Y	The cyclic rotation of word X left by Y bits
X>>>Y	The cyclic rotation of word X right by Y bits

TABLE 4. Hexadecimal values of magic constants for RC5 key extension.

(word size)	16-bit	32-bit	64-bit
P_w	0xB7E1	0xB3E15163	0xB7E151628AED2A6B
Q_w	0x9E37	0x9E3779B9	0x9E3779B97F4A7C15

process used primitive operations including addition, subtraction, exclusive OR and rotation and are shown in Table 3.

In key expansion routine sub keys [sub(n)] are created by using the secret key (k[n]). Three simple arithmetic steps and two magic constants are involved in the RC5 key generation phase. The two magic constants 'P_w', and 'Q_w' are defined for arbitrary 'w' as follows,

$$P_w = odd[(e-2) * 2^w] \tag{4}$$

$$Q_w = odd[(\Phi - 1) - 2^w] \tag{5}$$

where 'e' is the Euler's number and 'Φ' is the golden ratio (approximately 1.6180). The hexadecimal format of P and Q magic constants for the RC5 algorithm are shown in Table 4.

The key expansion phase includes three steps, which are conversion, initialization and mixing as shown in Fig 5. In the first step, sender's secret key k[0.… b-1] is copied into a new array L[0.…c-1] of words c = [b/u], where 'u' is the number of bytes/words. Zero padding is performed for the unfilled bytes of L. The second step is initialization of the array 'S' to a fixed random bit pattern by choosing an arithmetic progression modulo 2w and it can be determined by the two magic constants 'P_w', and 'Q_w' that is defined for an arbitrary 'w' parameter. In the third step, sender's secret key is mixed with the sub key array in three passes.

The three operations used in RC5 encryption include addition and subtraction of words denoted as +/−, bit wise XOR +, and left shift and right Shift denoted as >>>, <<<. during the encryption process 2w bits plain text is entered. The sub key is S[2r+2] and iterative number of rounds is r.

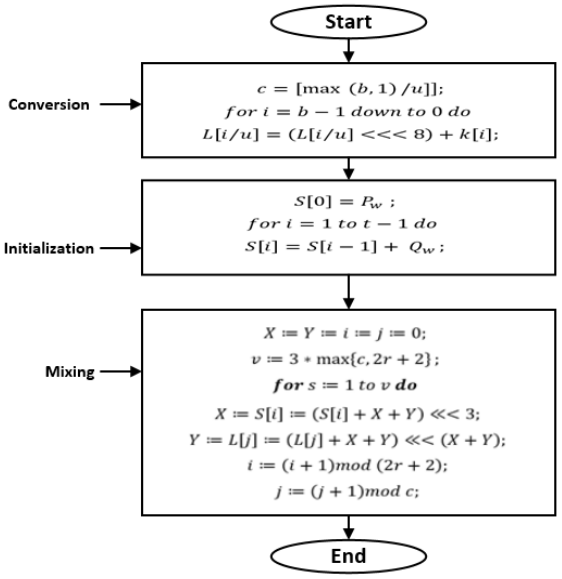

FIGURE 5. RC5 key generation phase.

The input block of data is given to two w-bit registers named X and Y, and the corresponding output is placed in registers X and Y. The RC5 encryption algorithm is given as follows:

Algorithm 1 :

$$Input(X, Y)$$
$$X := X + S[0];$$
$$Y := Y + S[1];$$
$$for\ i := 1\ to\ r\ do$$
$$X_{i+1} := ((X_i \oplus Y_i) <<< y_i) + S[2i];$$
$$Y_{i+1} := ((Y_i \oplus X_i) <<< X_i) + S[2i+1];$$
$$Output(X_{i+1}, Y_{i+1})$$

The decryption process is a reverse of encryption and is given in Algorithm 2.

Algorithm 2 :

$$Input(X_{i+1}, Y_{i+1})$$
$$for\ i = r\ dowm\ to\ do$$
$$Y_{i-1} = ((Y_i - S[2i+1]) >>> X_i) \oplus X_i$$
$$X_{i-1} = ((X_i - S[2i]) >>> Y_i) \oplus Y_{i-1}$$
$$X = X - S[0]$$
$$Y = Y - S[1]$$
$$Output(X, Y)$$

In order to increase the initial value and randomness sensitivity of the algorithm, the existing RC5 key computation process is enhanced by proposing a 2D-chaos based key generation phase. The proposed algorithm depends on the word size 'w' (16, 32, 64 bit), 'r' number of encryption and decryption rounds, value of 'λ' [1.11-1.19] which is the control parameter of 2D-logistic map, and initial value $x_o \in [0-1]$ and $y_o \in [0-1]$. For decryption 'r' and (x_o, y_o) will be used as initial value by the sub key to generate a 2-D chaotic map sequence.

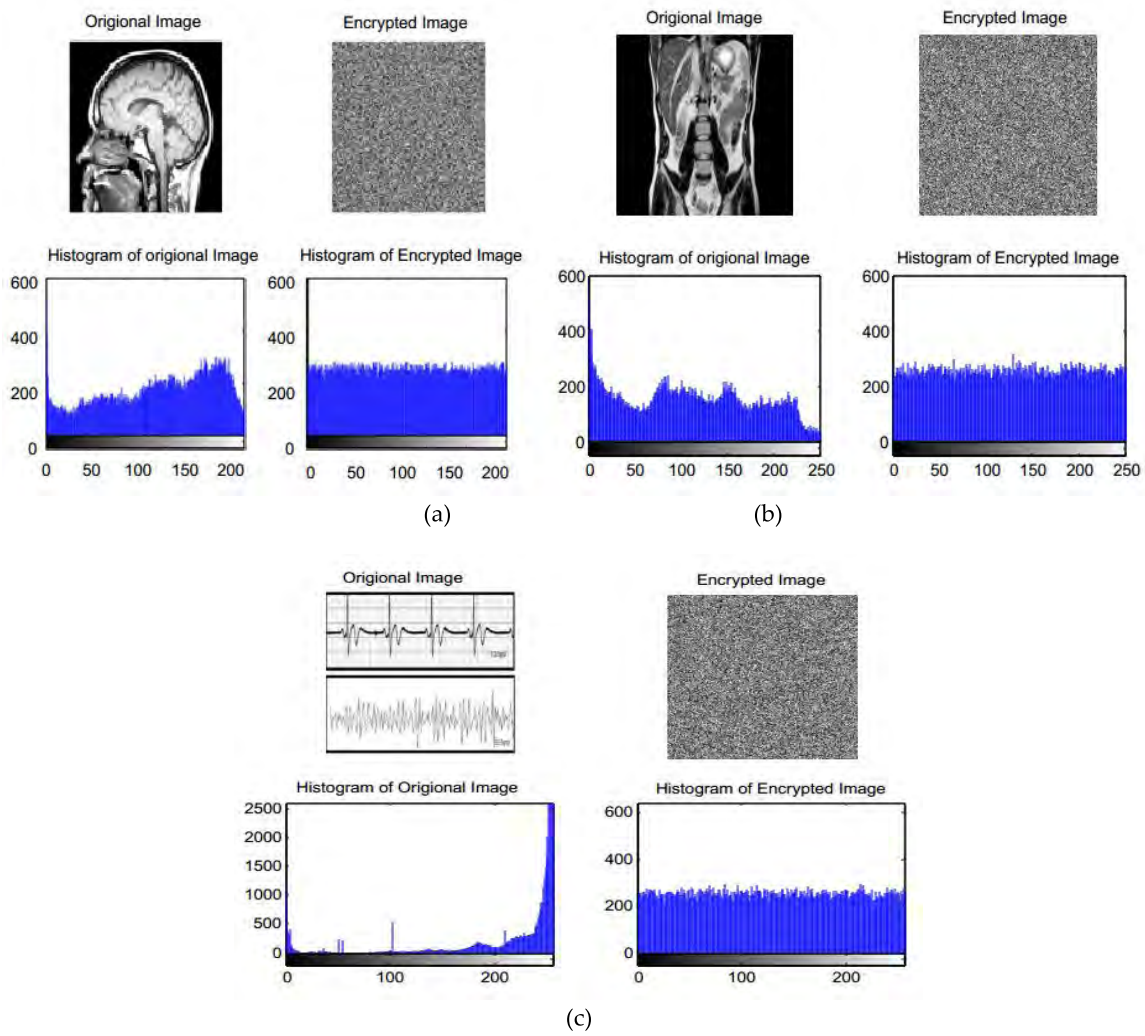

FIGURE 6. Histogram analysis. (a) MRI image, (b) CT scan image, (c) ECG/EEG waveform image.

In the proposed scheme, new features are introduced for ciphering of medical images. Initially, primary or user key is used to initiate the process. A chaotic sequence is calculated based on the primary key. This sequence is generated using 2-D logistic map on a certain initial condition, which is then used to perform confusion and diffusion processes. In the confusion process, the generated chaos sequence is used to shuffle the rows in permutation level-I, while in the permutation level-II, columns of matrix are shuffled to further enhance confusion. Due to the high-level sensitivity of the initial conditions for a chaotic map, the confusion process is well satisfied as only a 1-bit change creates huge impact on the cipher image in terms of encryption.

Each pixel value of the original medical image is added with the chaotic sequence values generated by 2-D map so that the diffusion process is also introduced to increase the resistance against attacks. In diffusion, each pixel value is transformed into a new one by using the same chaotic sequence, which was generated through the primary key.

Sub key generation process consists of three main stages i.e. initialization, conversion and mixing. In the first step the user secret key is converted from bytes to words. 'K' bytes of 'S' are copied into a new array 'W' in ascending order i.e., from lower order byte to higher order byte. Zero padding is done to fill any idle positions. In the 2^{nd} step, initialization is performed with the 2-D logistic map. The array 'C' is initialized to a random bit pattern generated by the 2-D logistic map. Finally, the user secret key 'W' and the chaotic key 'C' are mixed to create a sequence, which is used as a sub-key to pass it to the RC5 block cipher for the final encryption of the permutated medical images.

To retrieve the original medical image, all encryption steps are performed in a reverse order. The decryption key is generated by the same chaotic sequence, which is used by the RC5 block cipher to decrypt the cipher image. Then diffusion is performed, where each pixel value is subtracted by using the same chaotic sequence which was used during the encryption process. Finally, inverse row and column wise

TABLE 5. Correlation analysis of medical images.

Direction of adjacent pixel	Correlation (Plain Image)	(Correlation coefficient for Bain MRI Image)	
		Correlation (RC5 Cipher Image)	Correlation Proposed Algorithm
Horizontal (H)	0.9926	0.0096	0.0023
Vertical (V)	0.9835	0.0085	0.0020
Diagonal (D)	0.9690	0.0078	0.0017
Direction of adjacent pixel	**Correlation (Plain Image)**	**(Correlation coefficient for Abdomen CT Scan Image)**	
		Correlation (RC5 Cipher Image)	**Correlation Proposed Algorithm**
Horizontal (H)	0.9938	0.0095	0.0020
Vertical (V)	0.9840	0.0089	0.0019
Diagonal (D)	0.9696	0.0075	0.0016
Direction of adjacent pixel	**Correlation (Plain Image)**	**(Correlation coefficient for ECG/EEG Image)**	
		Correlation (RC5 Cipher Image)	**Correlation Proposed Algorithm**
Horizontal (H)	0.9919	0.0091	0.0024
Vertical (V)	0.9820	0.0087	0.0020
Diagonal (D)	0.9672	0.0077	0.0018

permutation is performed using the same chaotic sequence generated by the 2-D logistics map.

IV. RESULTS AND DISCUSSION

The performance of a cryptosystem can be measured by its resistance against known cryptanalyst attacks. The capability of any cryptosystem to withstand against unauthorized attempts of intruder to access plain text information is an important measure to check the quality. Confusion and diffusion are two important measures to check the security of an image-based cryptosystem. In order to verify the effectiveness and speed of the proposed cryptosystem a comprehensive security analysis is presented in this subsection. Several security analysis techniques are applied including statistical and differential analysis, key space analysis, correlation analysis, key sensitivity analysis, plain image sensitivity analysis, histogram analysis, pseudo randomness test with National institute of standards and technology (NIST) suite and noise attack analysis. Tests are performed on three medical images (MRI, ECG and CT Scan) of different sizes. The results clearly demonstrate the adequate security of the proposed algorithm.

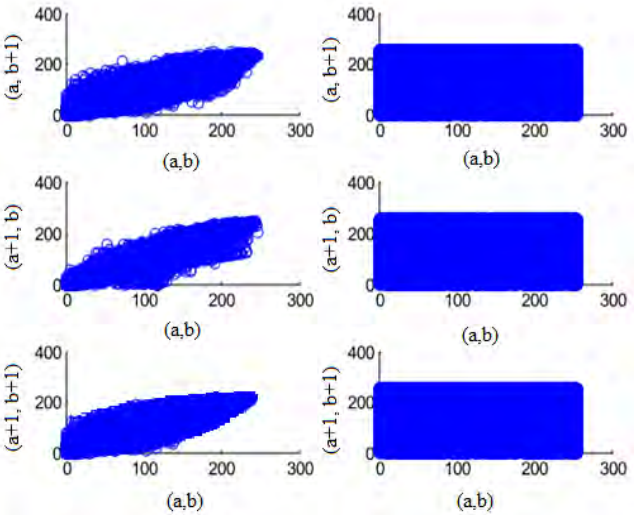

FIGURE 7. Correlation analysis.

A. KEY SPACE ANALYSIS

In cryptography, security of the key is very important. According to Kerckhoffs's axiom security of an algorithm depends on the security of the key. So, the key of any cipher algorithm must be sensitive, secure and its key space must be large enough to be resistive against brute force attacks. The RC5 algorithm consists of variable key lengths. In brute force attack, the attacker attempts using every possible combination of the key to recover the plain text. It requires 2^n attempts to get to the right key, where 'n' is its key length. The larger the key size the better the cipher would be in terms of security, but this would also require more resources, memory and computation time. A trade-off must be made between security and execution time, since time is critically important in e-health applications along with security. In this research work, 12 rounds and 128-bit key are considered, which is further enhanced by a 2D-chaotic map for providing an improved security key. The new key space is calculated as $2^n \times r \times l$, where 'r' is the number of rounds, 'n' is the key length and 'l' is the total number of input blocks. The resultant value is large and strong enough to resist against most cryptanalysis attacks. Thus, cryptanalysis may bypass the brute force attack, since many operations would be required for breaking the key.

B. HISTOGRAM ANALYSIS

A histogram is a graphical display, where data is grouped into different ranges and plotted in the form of bars. An image histogram is used to illustrate the pixel distribution in an image according to the intensity level of each color. A good image encryption scheme should generate a uniform histogram for any image. Histogram analysis is presented in the Fig. 6, which clearly shows that the histogram of a cipher image generated using the proposed algorithm is uniform and is fairly distributed over the pixel range. These results indicate that the histogram of the encrypted image is entirely different

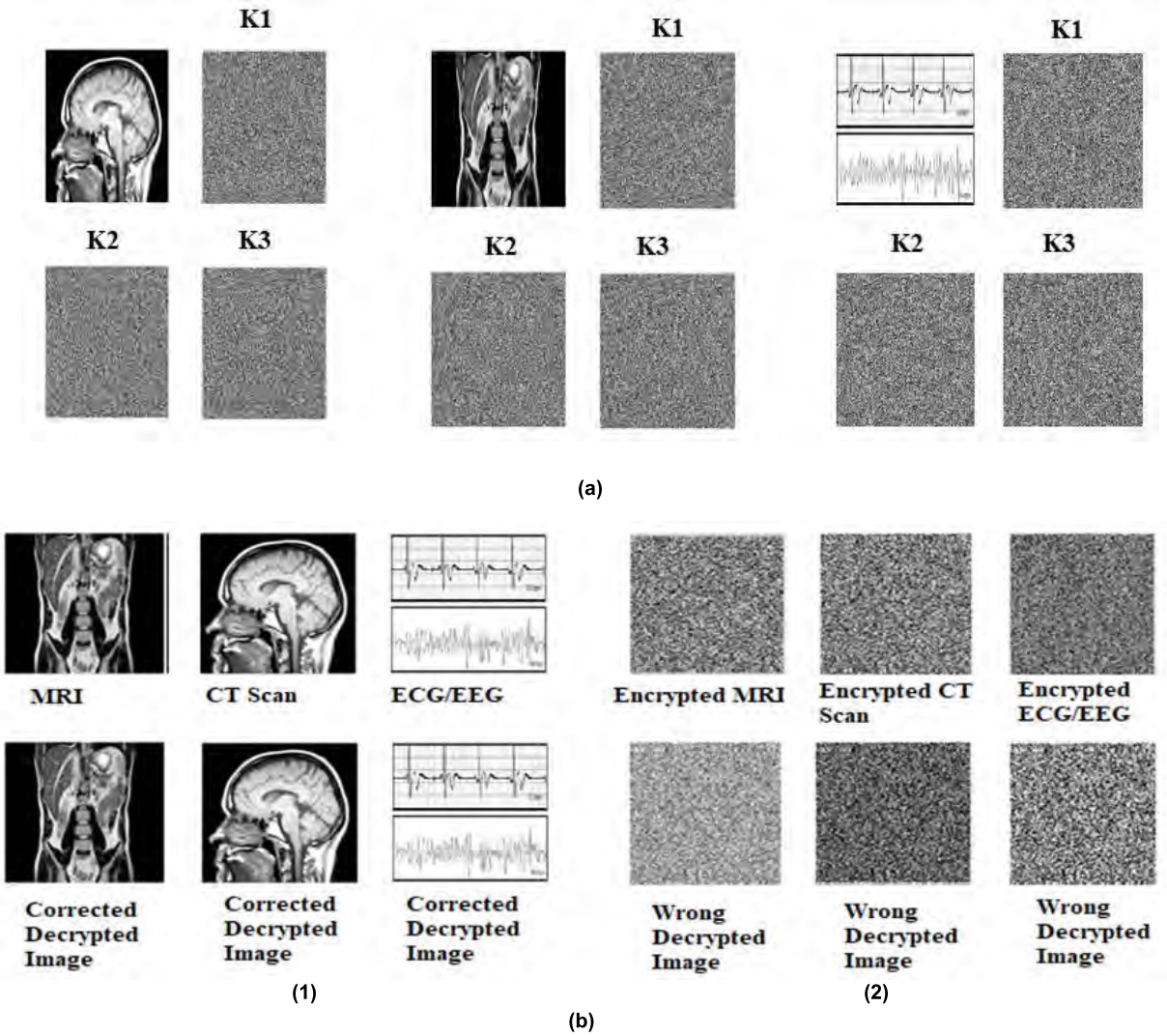

FIGURE 8. (a) Secret key analysis (Encryption of clinical images using K1, K2 & K3 keys, having 1-bit difference with each other). (b) Secret key analysis. 1) Decryption using same key. 2) Decryption using key with 1-bit difference.

from the original image and hence, the proposed scheme is robust against histogram based statistical attacks.

C. CORRELATION ANALYSIS

Correlation coefficient is an important factor to determine the quality of an image cryptosystem. This analysis shows that no correlation exists between pixels in the plain image and its corresponding encrypted image. The correlation coefficient is calculated as,

$$\mathrm{cov}(a, b) = E[a - E(a)][b - E(b)] \tag{6}$$

$$R_{ab} = \frac{\mathrm{cov}(a, b)}{\sqrt{D(a)}\sqrt{D(b)}} \tag{7}$$

where 'a' and 'b' are the corresponding grayscale values of the adjacent pixels. The correlation between two horizontally adjacent, vertically adjacent and diagonally adjacent pixels of a plain image and its corresponding cipher image are tested. The correlation coefficient is determined by randomly taking 100 pairs of adjacent pixels from an image and using equations 6 and 7, where the correlation coefficient $r_c \in (-1,1)$. A lower value of the correlation coefficient indicates better quality of the cryptosystem, while zero value indicates null correlation. The following discrete formulas are used in numerical computation to find the value of correlation coefficient.

$$E(a) = \frac{1}{N}\sum_{i=1}^{N} a_i \tag{8}$$

$$D(a) = \frac{1}{N}\sum_{i=1}^{N} (a_i - E(a))^2 \tag{9}$$

$$\mathrm{cov}(a, b) = \frac{1}{N}\sum_{i=1}^{N} (a_i - E(a)(b_i - E(b)) \tag{10}$$

where, 'N' indicates the number of pixels involved. The correlation coefficient results of the proposed algorithm are listed in the Table 5. The horizontal, vertical and diagonal correlation distributions for the MR image are shown in Fig. 7. From these results it can be concluded

TABLE 6. Secret key sensitivity analysis through correlation coefficients (brain image).

Image 1	Image 2	Correlation coefficient
Encrypted K1-Brain	Encrypted K2-Brain	0.0026
Encrypted K2-Brain	Encrypted K3-Brain	0.0040
Encrypted K3-Brain	Encrypted K1-Brain	0.0021

that the proposed cipher provides good encryption quality as compared to the normal RC5 encryption process and produce highly uncorrelated cipher images.

D. SECRET KEY SENSITIVITY ANALYSIS

Good encryption algorithms are highly sensitive to the key, which means that the encrypted information cannot be decrypted correctly until the same key is used on both sides. The proposed cipher combines chaotic map and user's secret key for generating the round keys, where a slight difference in keys may results in wrong decryption. A key space analysis is performed using the encryption/decryption key sensitivity tests for the proposed cryptosystem. In the first stage, three similar keys are generated differing from each other by just one bit for encrypting the same image. The encrypted images are compared, and their key sensitivity is measured by using the correlation coefficient between the adjacent pixels of all three encrypted images. The results are presented in Fig. 8(a) and Table 6, which clearly shows that there is no correlation between the three encrypted images even though they are generated using slightly different keys.

In the 2nd stage, an image is encrypted by using secret key "5214A76CF00DE3DBE0CC89D287" (26 hex digits) and the resultant encrypted image is stored. The image is decrypted with the same key "5214A76CF00DE3DBE0CC8 9D287" and the resultant decrypted image is stored. A slight change in the key is performed by modifying the middle bit (E) in the key, where the updated key is "5214A76CF00DE3**E**BE0CC89D287". Decryption is performed on the same image with same parameters using the new key. The resultant decrypted image is entirely different from the original image as shown in Fig 8(b), hence it is concluded that the proposed cryptosystem is highly key sensitive.

E. PLAIN IMAGE SENSITIVITY ANALYSIS

In this analysis two similar plain images (*C1 and C2*) are encrypted by using the same cipher key. The selected plain images are similar except a difference in 1-pixel value, where C_1 (i, j) and C_2 (i, j) are the grayscale values of the pixel at index i and j. Two quantity methods, net pixel change rate (NPCR) and unified average changing intensity (UACI) [40] are used for differential analysis in chaos-based image cryptosystems, where NPCR is determined by using,

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \tag{11}$$

$$D(i,j) \begin{Bmatrix} 0, & if\ C_1(i,j) \neq C_2(i,j) \\ 1, & if\ C_1(i,j) \neq C_2(i,j) \end{Bmatrix} \tag{12}$$

where 'W' and 'H' denotes the width and height of the encrypted image respectively.

UACI is used to measure average intensity difference between two encrypted images and is defined as,

$$UACI = \frac{1}{W \times H}\left[\frac{\sum_{i,j} |C_1(i,j) - C_2(i,j)}{255}\right] \times 100\% \tag{13}$$

A larger value of UACI indicates better performance of the cryptographic algorithm. These tests have been performed using the grayscale brain MR image. The image C1 is kept similar, while C2 is encrypted 1000 times by randomly selected 1000 keys. An average value of NPCR in all these tests is 99.53%, and UACI is 33.4%. Therefore, it is concluded that the proposed algorithm is highly sensitive to small changes in plain image as shown in the Fig. 9.

TABLE 7. MSE values with three different noise densities (MRI image).

Density	RC5	Proposed Algorithm
0.029	1.60×10^3	1.65×10^3
0.059	2.64×10^4	2.82×10^4
0.159	4.71×10^4	4.87×10^4

F. NOISE ATTACK

The cipher image can be changed by external noise, when it is transmitted over the network. Mean-squared error (MSE) is used to evaluate the robustness of the proposed cryptosystem and is defined as,

$$MSE = \frac{1}{w \times h}\sum_{i=1}^{w}\sum_{j=1}^{H}[p_1(i,j) - p_2(i,j)]^2 \tag{14}$$

where $w \times h$ is the image size, P_1 (i, j) and P_2 (i, j) denotes the values of original and decrypted noised image for pixels i, j. Salt-and-pepper noise (i.e., 0 or 1) is added with three noise densities: 0.029, 0.059, 0.159 for 2%, 5% and 15% of noise, respectively. Fig. 10 shows the results after adding salt-and-pepper noise to the cipher image, when the proposed algorithm is used, and their corresponding decrypted images after retrieval. The MSE value of an input image and its corresponding decrypted image of brain with salt and pepper noise of different intensities is shown in Table 7. The results clearly show that the proposed algorithm is robust against noise.

G. SPEED PERFORMANCE ANALYSIS

Speed test analysis is performed to measure the efficiency of the proposed scheme, where the computation time is

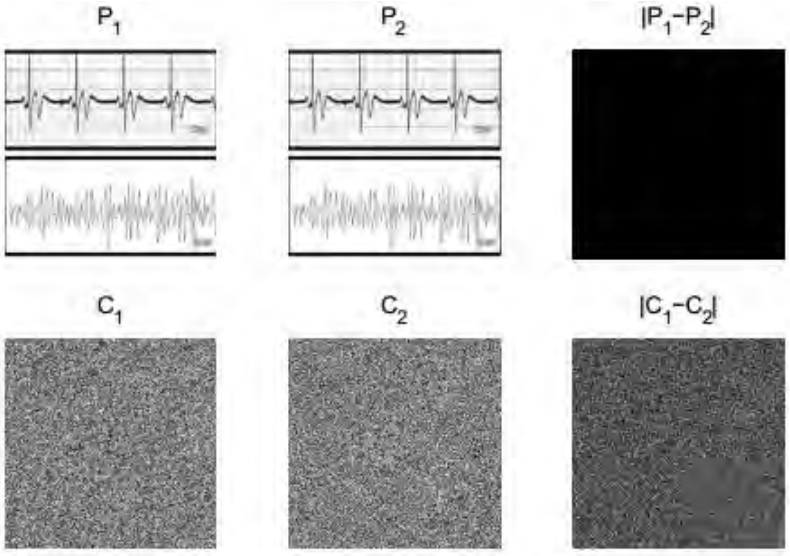

FIGURE 9. Plain image sensitivity analysis.

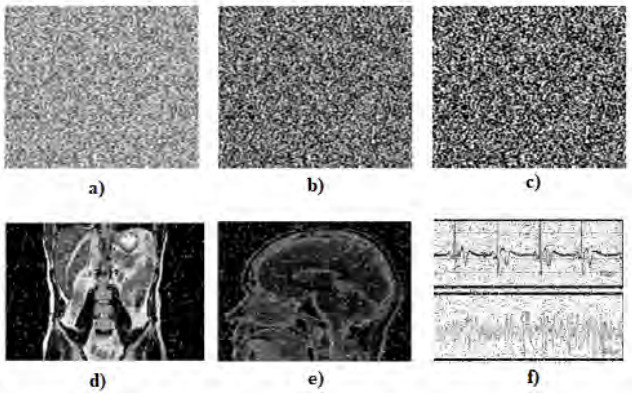

FIGURE 10. Noise attack a), b) & c) Encrypted images with different noise densities d), e) & f) Corresponding decrypted images.

calculated for encryption/decryption of clinical images. The proposed scheme is implemented in MATLAB v.13 with AMD 2.4 GHz processor, 4-GB RAM and 64-bit operating system (Windows-7). An average encryption and decryption time for the proposed scheme in comparison of simple RC5 is given in Table 8. The results show that at the cost of a slight increase in computing time, an increased level of security for clinical images in remote health monitoring is achieved by the proposed algorithm. The reason for this overhead is the computations performed while generating the key through chaos, which is not required for the implementation of a simple RC5 algorithm.

H. RANDOMNESS TEST USING NIST SP-800-22 TEST SUIT

NIST SP 800-22 test suit is one of the most commonly used statistical test suit. The proposed algorithm is tested by using NIST with the same parameter to evaluate the degree of randomness in output. NIST consists of fifteen tests and each test generates a p-value, whose range is between 0 to 1.

TABLE 8. NIST test's results (MRI scan).

Image Size (In pixels)	Image Size	RC5 (Average Encryption/Decryption Time)	Proposed Scheme (Average Encryption/Decryption Time)
256x256	412 KB	0.19-0.22	0.20-0.23
512x512	766 KB	0.39-0.43	0.41-0.48
1024x1024	3 MB	1.06-1.13	1.16-1.21
2048x2048	10 MB	2.55-2.72	3.21-3.88

The statistical test is passed successfully with 99% confidence, if the 'p' value is greater than the significance level. According to the NIST test results, it is concluded that the proposed cipher produces chaotic sequence, which exhibit random behavior as shown in Table 9.

TABLE 9. NIST test's results (MRI scan).

Test Performed	p-value	Results
Approximate Entropy	0.044	Passed
Block frequency	0.832	Passed
Cumulative Sums	0.813	Passed
FFT	0.985	Passed
Frequency	0.206	Passed
Linear Complexity	0.316	Passed
Longest Run	0.035	Passed
Overlapping Template	0.082	Passed
Random Excursions	0.504	Passed
Rank	0.237	Passed
Runs	0.010	Passed
Serial	0.015	Passed
Universal Test	0.431	Passed

V. CONCLUSION

An efficient image cryptosystem based on RC5 and 2D-chaotic map is proposed for providing security in remote health monitoring. A strong key generation mechanism is introduced, which is based on chaos to enhance the key strength. Some important features of chaos such as sensitivity to the initial values, non-deterministic behavior and lack of periodicity make it a potential candidate for the proposed scheme. The encryption key is iterated based on feedback mode for every round in order to get a higher encryption strength. The performance analysis of the proposed cryptosystem is done both visually and numerically. The statistical and experimental analysis clearly shows that the proposed scheme is very secure due to its large key space, strong resistance to different types of attacks and extremely sensitive to the cipher key and plain images. It is concluded that the proposed scheme provides more security to patient's data, while preserving confidentiality and integrity. Also, this is the first time to the best of our knowledge, that 1-D physiological signals are secured in the form of images with chaos based enhanced RC5 algorithm for their transmission in remote health monitoring. Future work will involve the security enhancement of RC5 and RC6 schemes using higher order chaotic maps and security of clinical signals through optical chaos.

REFERENCES

[1] T. Lewis, C. Synowiec, G. Lagomarsino, and J. Schweitzer, "E-health in low-and middle-income countries: Finings from the center for health market innovations," *Bull. World Health Org.*, vol. 90, no. 5, pp. 332–340, 2012.

[2] S. Ullah, H. Higgin, M. A. Siddiqui, and K. S. Kwak, "A study of implanted and wearable body sensor networks," in *Proc. KES Int. Symp. Agent Multi-Agent Syst., Technol. Appl.* Berlin, Germany: Springer, 2008, pp. 464–473.

[3] H. Fotouhi, A. Causevic, K. Lundqvist, and M. Björkman, "Communication and security in health monitoring systems—A review," in *Proc. IEEE 40th Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, vol. 1, Jun. 2016, pp. 545–554.

[4] S. M. Ismail, L. A. Said, A. G. Radwan, A. H. Madian, and M. F. Abu-Elyazeed, "Generalized double-humped logistic map-based medical image encryption," *J. Adv. Res.*, vol. 10, pp. 85–98, Mar. 2018.

[5] J. Kukkurainen, M. Soini, and L. Sydänheimo, "RC5-based security in wireless sensor networks: Utilization and performance," *WSEAS Trans. Comput*, vol. 9, no. 10, pp. 1191–1200, 2010.

[6] H. El-din H. Ahmed, H. M. Kalash, and O. S. F. Allah, "Implementation of RC5 block cipher algorithm for image cryptosystems," *Int. J. Inf. Technol.*, vol. 3, no. 4, pp. 1–6, 2007.

[7] N. Bajaj and A. Thakur, "Enhancement of RC5 for image encryption," in *Proc. Int. Conf. Image Inf. Process.*, Nov. 2011, pp. 1–5.

[8] J. Lee, K. Kapitanova, and S. H. Son, "The price of security in wireless sensor networks," *Comput. Netw.*, vol. 54, no. 17, pp. 2967–2978, 2010.

[9] K. Biswas, V. Muthukkumarasamy, X.-W. Wu, and K. Singh, "Performance evaluation of block ciphers for wireless sensor networks," in *Advanced Computing and Communication Technologies*. Singapore: Springer, 2016, pp. 443–452.

[10] S. Suresh, M. Varghese, and D. Aj, "An efficient and optimized RC5 image encryption algorithm for secured image transmission," *Int. J. Imag. Robot.*, vol. 15, no. 3, pp. 117–125, 2015.

[11] E. B. Villanueva, R. P. Medina, and B. D. Gerardo, "An enhanced RC5 (ERC5) algorithm based on simple random number key expansion technique," in *Proc. IEEE Symp. Comput. Appl. Ind. Electron. (ISCAIE)*, Apr. 2018, pp. 134–138.

[12] C. Lakshmi, K. Thenmozhi, J. B. B. Rayappan, and R. Amirtharajan, "Encryption and watermark-treated medical image against hacking disease—An immune convention in spatial and frequency domains," *Comput. Methods Programs Biomed.*, vol. 159, pp. 11–21, Jun. 2018.

[13] R. Matthecws, "On the derivation of a 'chaotic' encryption algorithm," *Cryptologia*, vol. 13, no. 1, pp. 29–42, 1989.

[14] N. Masuda, G. Jakimoski, K. Aihara, and L. Kocarev, "Chaotic block ciphers: From theory to practical algorithms," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 53, no. 6, pp. 1341–1352, Jun. 2006.

[15] M. Ahmad, E. Al Solami, X.-Y. Wang, M. N. Doja, M. M. S. Beg, and A. A. Alzaidi, "Cryptanalysis of an image encryption algorithm based on combined chaos for a BAN system, and improved scheme using SHA-512 and hyperchaos," *Symmetry*, vol. 10, no. 7, p. 266, 2018.

[16] F. Qamar, M. K. Islam, S. Z. Ali Shah, R. Farhan, and M. Ali, "Secure duobinary signal transmission in optical communication networks for high performance & reliability," *IEEE Access*, vol. 5, pp. 17795–17802, 2017.

[17] M. Alghoniemy and A. H. Tewfik, "Geometric invariance in image watermarking," *IEEE Trans. Image Process.*, vol. 13, no. 2, pp. 145–153, Feb. 2004.

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

[19] A. Niaz, F. Qamar, M. Ali, R. Farhan, and M. K. Islam, "Performance analysis of chaotic FSO communication system under different weather conditions," *Trans. Emerg. Telecommun. Technol.*, vol. 30, no. 2, p. e3486, 2019.

[20] A. P. Abidoye, N. A. Azeez, A. O. Adesina, K. K Agbele, and H. O. Nyongesa, "Using wearable sensors for remote healthcare monitoring system," *J. Sensor Technol.*, vol. 1, no. 2, pp. 22–28, 2011.

[21] J. Shen, S. Chang, J. Shen, Q. Liu, and X. Sun, "A lightweight multi-layer authentication protocol for wireless body area networks," *Future Gener. Comput. Syst.*, vol. 78, pp. 956–963, Jan. 2018.

[22] D. Bresnahan and Y. Li, "Measurement of around-body creeping waves using wearable sensor modules," in *Proc. Texas Symp. Wireless Microw. Circuits Syst. (WMCS)*, Apr. 2018, pp. 1–4.

[23] M. A. Murillo-Escobar, L. Cardoza-Avendaño, R. M. López-Gutiérrez, and C. Cruz-Hernández, "A double chaotic layer encryption algorithm for clinical signals in telemedicine," *J. Med. Syst.*, vol. 41, no. 4, p. 59, 2017.

[24] F. Sufi, F. Han, I. Khalil, and J. Hu, "A chaos-based encryption technique to protect ECG packets for time critical telecardiology applications," *Secur. Commun. Netw.*, vol. 4, no. 5, pp. 515–524, 2011.

[25] J.-M. Ho, "A versatile suite of strong authenticated key agreement protocols for body area networks," in *Proc. 8th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Aug. 2012, pp. 683–688.

[26] Z. Zhang, H. Wang, A. V. Vasilakos, and H. Fang, "ECG-cryptography and authentication in body area networks," *IEEE Trans. Inf. Technol. Biomed.*, vol. 16, no. 6, pp. 1070–1078, Nov. 2012.

[27] J. Liu, Z. Zhang, R. Sun, and K. S. Kwak, "An efficient certificateless remote anonymous authentication scheme for wireless body area networks," in *Proc. IEEE ICC*, Jun. 2012, pp. 3404–3408.

[28] L. Zhang, J. Liu, and R. Sun, "An efficient and lightweight certificateless authentication protocol for wireless body area networks," in *Proc. 5th Int. Conf. Intell. Netw. Collaborative Syst.*, Sep. 2013, pp. 637–639.

[29] O. S. Faragallah, "An enhanced chaotic key-based RC5 block cipher adapted to image encryption," *Int. J. Electron.*, vol. 99, no. 7, pp. 925–943, 2012.

[30] D. Sathya and P. G. Kumar, "Secured remote health monitoring system," *Healthcare Technol. Lett.*, vol. 4, no. 6, pp. 228–232, 2017.

[31] K. K. Venkatasubramanian, A. Banerjee, and S. K. S. Gupta, "Plethysmogram-based secure inter-sensor communication in Body Area Networks," in *Proc. IEEE Mil. Commun. Conf.*, Nov. 2008, pp. 1–7.

[32] S. M. Khaliq-ur-Rahman Raazi, H. Lee, S. Lee, and Y.-K. Lee, "BARI: A distributed key management approach for wireless body area networks," in *Proc. IEEE Int. Conf. Comput. Intell. Secur.*, Dec. 2009, pp. 324–329.

[33] M. Mana, M. Feham, and B. A. Bensaber, "Trust key management scheme for wireless body area networks," *Int. J. Netw. Secur.*, vol. 12, no. 2, pp. 75–83, 2011.

[34] L. Yao, B. Liu, K. Yao, G. Wu, and J. Wang, "An ECG-based signal key establishment protocol in body area network," in *Proc. 7th Int. Conf. Ubiquitous Intell. Comput.*, Oct. 2010, pp. 233–238.

[35] M. Li, S. Yu, W. Lou, and K. Ren, "Group device pairing based secure sensor association and key management for body area networks," in *Proc. IEEE INFOCOM*, Mar. 2010, pp. 1–9.
[36] C. Hu, X. Cheng, F. Zhang, D. Wu, X. Liao, and D. Chen, "OPFKA: Secure and efficient Ordered-Physiological-Feature-based key agreement for wireless Body Area Networks," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 2274–2282.
[37] S. N. Ramli, R. Ahmad, M. F. Abdollah, and E. Dutkiewicz, "A biometric-based security for data authentication in Wireless Body Area Network (WBAN)," in *Proc. IEEE ICACT*, Jan. 2013, pp. 998–1001.
[38] J. Liu and K. S. Kwak, "Hybrid security mechanisms for wireless body area networks," in *Proc. IEEE ICUFN*, Jun. 2010, pp. 98–103.
[39] A. Alsadhan and N. Khan, "An LBP based key management for Secure Wireless Body Area Network (WBAN)," in *Proc. 14th ACIS Int. Conf. Softw. Eng., Artif. Intell., Netw. Parallel/Distrib. Comput.*, Jul. 2013, pp. 85–88.
[40] S. Cai, L. Huang, X. Chen, and X. Xiong, "A symmetric plaintext-related color image encryption system based on bit permutation," *Entropy*, vol. 20, no. 4, p. 282, 2018.

ROMANA SHAHZADI received the B.Sc. Engg. and M.Sc. Engg. degrees (Hons.) in computer engineering from the University of Engineering and Technology at Taxila, Pakistan, in 2008 and 2011, respectively, where she is currently pursuing the Ph.D. degree with the Department of Computer Engineering. Her research interests include data, networks, and system security with a focus on e-health systems.

SYED MUHAMMAD ANWAR received the B.Sc. degree (Hons.) in computer engineering from the University of Engineering and Technology (UET) at Taxila, Pakistan, in 2005, and the M.Sc. degree (Hons.) in data communications and the Ph.D. degree in electronic and electrical engineering from the University of Sheffield, U.K., in 2007 and 2012, respectively. He has been an Associate Professor with the Department of Software Engineering, UET, and the Head of the Signal, Image, Multimedia Processing and LEarning (SIMPLE) Research Group, since 2012. He was a recipient of the Faculty Development Program Scholarship of Higher Education Commission (HEC), Pakistan, for his M.Sc. and Ph.D. studies. His research interests include biomedical signal processing, medical imaging, physiological signal processing, and deep learning.

FARHAN QAMAR received the B.Sc. degree in computer engineering, the M.Sc. degree in telecommunication engineering, and the Ph.D. degree in telecommunication engineering from the University of Engineering and Technology (UET) at Taxila, Taxila, Pakistan. After his graduation, he remained attached with different sections of Huawei and Mobilink for more than seven years. Since last six years, he has been an Assistant Professor with the Telecom Engineering Department of UET, where he is also acting as a Principal Investigator of the Advance Optical Communication Group, AOCG. His research interests include chaos communication, optical networks, 5G networks, advance modulation formats, and radio over fiber.

MUDASSAR ALI received the B.S. degree in computer engineering and the M.S. degree in telecom engineering from the University of Engineering and Technology at Taxila, Pakistan, 2006 and 2010, respectively, with a major in wireless communication, and the Ph.D. degree from the School of Electrical Engineering and Computer Science (SEECS), National University of Sciences and Technology (NUST), Pakistan, in 2017. From 2006 to 2007, he was a Network Performance Engineer with Mobilink (An Orascom Telecom Company). From 2008 to 2012, he was a Senior Engineer Radio Access Network Optimization with Zong (A China Mobile Company). Since 2012, he has been an Assistant Professor with the Telecom Engineering Department, University of Engineering and Technology at Taxila. His research interests include 5G wireless systems, heterogeneous networks, interference coordination, and energy efficiency in 5G green heterogeneous networks.

JOEL J. P. C. RODRIGUES (S'01–M'06–SM'06) received the B.Sc. degree (Licentiate) in informatics engineering from the University of Coimbra, Portugal, the M.Sc. degree and the Ph.D. degree in informatics engineering from UBI, and the Habilitation degree in computer science and engineering from the University of Haute Alsace, France. He is currently a Professor with the National Institute of Telecommunications–Inatel, Brazil, a Senior Researcher with the Instituto de Telecomunicações, Portugal, and a Visiting Professor with the Federal University of Piauí, Brazil. He is also the Leader of the Internet of Things Research Group (CNPq). He has authored or coauthored more than 700 papers in refereed international journals and conferences, three books, and holds two patents. He is a member of many international TPCs and has participated in several international conferences organization. He is a Licensed Professional Engineer (as a Senior Member), a member of the Internet Society, and a Senior Member of ACM. He received the Academic Title of Aggregated Professor in informatics engineering from UBI. He has received several outstanding leadership and outstanding service awards by the IEEE Communications Society and several best papers awards. He is the Technical Activities Committee Chair of the IEEE ComSoc Latin America Region Board, the President of the Scientific Council with ParkUrbis–Covilhã Science and Technology Park, the Past Chair of the IEEE ComSoc Technical Committee on eHealth and the IEEE ComSoc Technical Committee on Communications Software, a Steering Committee Member of the IEEE Life Sciences Technical Community, the Publications Co-Chair, and a Member Representative of the IEEE Communications Society on the IEEE Biometrics Council. He is the Director for the Conference Development—the IEEE ComSoc Board of Governors. He is the Editor-in-Chief of the *International Journal on E-Health and Medical Communications* and the Editorial Board Member of several high-reputed journals. He has been the General Chair and the TPC Chair of many international conferences, including the IEEE ICC, the IEEE GLOBECOM, the IEEE HEALTHCOM, and the IEEE LatinCom. He is an IEEE Distinguished Lecturer.