WILEY | Hindawi

Research Article

Josephson Junction Model: FPGA Implementation and Chaos-Based Encryption of sEMG Signal through Image Encryption Technique

Colince Welba [iD],[1] **Dhanagopal Ramachandran** [iD],[2] **Alexendre Noura**,[3] **Victor Kamdoum Tamba** [iD],[4] **Sifeu Takougang Kingni** [iD],[5] **Pascal Eloundou Ntsama**,[3] **and Pierre Ele**[6]

[1]Department of Fundamental Sciences, National Advanced School of Mines and Petroleum Industries, University of Maroua, P. O. Box 46, Maroua, Cameroon
[2]Center for Systems Design, Chennai Institute of Technology, Chennai 600069, Tamilnadu, India
[3]Department of Physics, Faculty of Science, University of Ngaoundere, P.O. Box: 454, Ngaoundere, Cameroon
[4]Department of Telecommunication and Network Engineering, IUT-Fotso Victor of Bandjoun, University of Dschang, P. O. Box: 134, Bandjoun, Cameroon
[5]Department of Mechanical, Petroleum and Gas Engineering, National Advanced School of Mines and Petroleum Industries, University of Maroua, P. O. Box 46, Maroua, Cameroon
[6]Electrical and Engineering, Telecommunications Department, National Advanced School of Engineering, University of Yaoundé I, P.O. Box 812, Yaoundé, Cameroon

Correspondence should be addressed to Colince Welba; welbacolince@yahoo.fr

The field programmable gate array (FPGA) implementation of the nonlinear resistor-capacitor-inductor shunted Josephson junction (NRCISJJ) model and its application to sEMG (Surface ElectroMyoGraphic) signal encryption through image encrypted technique are reported in this study. Thanks to the numerical simulations and FPGA implementation of the NRCISJJ model, different shapes of chaotic attractors are revealed by varying the parameters. The chaotic behaviour found in the NRCISJJ model is used to encrypt the sEMG signal through image encryption technique. The results obtained are interesting and open up many perspectives.

1. Introduction

Circuits based on Josephson Junction (JJ) devices received particular attention in literature during the past two decades. This great interest is justified not only by the interesting characteristics of JJ device including high working frequency, low power consumption, and ultralow noise but also by their exploitation for constructing important technological devices such as ultrahigh sensitive detectors, high-density computer circuits, quantum-computing devices, superconducting electronic devices (e.g., terahertz pulse generator), and ultrahigh-speed chaotic signal generators [1–8]. Concerning the last application, many works have demonstrated the existence of chaos in several systems using different models of JJ [9–15]. Among them, linear and nonlinear resistor-capacitor-inductor shunted JJ models (LRCISJJ and NRCIJJ) are the most investigated in the relevant literature. This is due to their fascinating properties very suitable for high-frequency applications such as spread spectrum communication systems. Dana et al. characterized the chaotic dynamics in such models [9]. They reported some interesting results on the modulation of chaotic oscillation in such devices by an external sinusoidal signal as information. Control and synchronization of the NRCIJJ

model using the backstepping design method are discussed in [11, 12]. The authors demonstrated that the employed control method is capable to eliminate the chaotic behaviour displayed by the NRCIJJ model and assured the global asymptotic synchronization between drive-response NRCIJJ models with different system parameters. Remarkable numerical computations were carried out to confirm the feasibility of the developed control technique. Sifeu et al. [16] studied the dynamics and synchronization of the NRCLJJ model. They used the fractional-order form of the model to develop an application to digital cryptography. Implementing chaotic models with electronic devices has some inconveniences due to the limitations of bandwidth of some electronic devices such as operational amplifiers. To overcome these limitations, the implementation of chaotic models is carried out with FPGA and microcontroller devices. In this regard, the authors of [17] analyzed and implemented with FPGA a fractal JJ with unharmonic current-phase relation. They applied the system under scrutiny to chaos-based random number generator. Kadjie et al. [18] discussed the implementation with microcontroller of a NRCIJJ model and its applications in electromechanical engineering. The real electrical signals obtained from the implementation of the considered JJ model have been exploited to power an electromechanical pendulum. The numerical simulations revealed periodic and chaotic behaviours in the resulting system. Lai et al. proposed letter reports. In this letter, the authors constructed an interesting no-equilibrium chaotic system from the Lu system. The most striking feature of the new system is that it has hidden attractors and coexisting attractors [19, 20]. In [21], the authors investigated a 4D extended Lü system which coexists multiple attractors with respect to different initial conditions. Lai et al. [22] reported a new 4D chaotic system with double memristors. The numerical simulation indicated that the system is capable of yielding infinite coexisting attractors.

In recent years, considerable efforts have been devoted to the designing and investigation of image encryption systems. It is well known that image encryption is a useful technique for secure transmission. The objective of every image encryption algorithm is to generate a noisy image's having top-quality capable to keep information secret [23, 24]. Several image encryption algorithms have been proposed in relevant works. For example, some algorithms used single low-dimensional chaotic systems, such as logistic map, tent map, Baker map, and cat map, to encrypt images [25–29]. Wang and Zhang investigated an image encryption algorithm based on genetic recombination and 4D Lorenz-like hyperchaotic systems [30]. Huang et al. [31] developed a color image encryption algorithm using fractional-order chaotic sequences.

Motivated by the above discussions, this study designs and implements on FPGA a chaotic NRCISJJ model and applies it to secure sEMG signal through image encryption technique. The innovation of this study is to show that it is possible to secure a 1D signal using image encryption techniques. To our knowledge, the literature devoted to securing signals by encryption does not mention work on the

encryption of EMG signals. On the other hand, this same literature mentions several works on the encryption of other electrophysiological signals (EEG and ECG). This lack of work on sEMG encryption highlights the originality of this study.

The study is articulated around four sections presented as follows. The FPGA implementation of the NRCISJJ model is presented in Section 2. Section 3 focuses on its application to secure surface electromyographic signals through image encryption technique. Finally, the conclusion of the paper is presented in Section 4.

2. FPGA Implementation of the NRCISJJ Model

The NRCISJJ model is described by the following dimensionless rate of equations [11]:

$$
\begin{cases}
\dfrac{dx}{dt} = \dfrac{1}{\beta_c}\left[i - y - g(x)x - \sin(z)\right], \\[4mm]
\dfrac{dy}{dt} = \dfrac{1}{\beta_L}(x - y), \\[4mm]
\dfrac{dz}{dt} = x,
\end{cases}
\tag{1}
$$

where t, x, y, and z represent the dimensionless time, the voltage in the junction, the inductor current, and the phase difference, respectively. The parameter i is an external direct current source and β_C and β_L are capacitive and inductive parameters, respectively. The function $g(x)$ is a piecewise function approximation by current voltage characteristic of the intrinsic junction shunt resistor defined as

$$
g(x) = \begin{cases}
0.366, & \text{if } |x| > 2.9, \\
0.061, & \text{if } |x| \le 2.9.
\end{cases}
\tag{2}
$$

System (1), describing the NRCISJJ model, is designed in Xilinx system generator Simulink integrated in MATLAB. The blocks of Xilinx system generator tool kit used to design system (1) are configured according to IEEE 754 standard as 32 bit (no. of bits) and 16 bit (binary bit) fixed point, where the latency is set to zero. The forward Euler's algorithm is the digital method used to design the integrator of system (1).

By using the Vivado design tool, the register-transfer level (RTL) architecture required for implementation of NRCISJJ model is presented in Figure 1.

Figure 1 is implemented in Kintex 7 XC7K325fFFG676-1 chip. The discretized state equations of system (1) are given by

$$
x_{m+1} = x_m + h\frac{[i - y_{m-1} - g(x_{m-1})x_{m-1} - \sin(z_{m-1})]}{\beta_C},
$$

$$
y_{m+1} = y_m + h\frac{(x_{m-1} - y_{m-1})}{\beta_L},
\tag{3}
$$

$$
z_{m+1} = z_m + h(x_{m-1}),
$$

where $\beta_R, \beta_L, \beta_C,$ and i are the parameter values of system (1) and the step size $h = 0.01$.
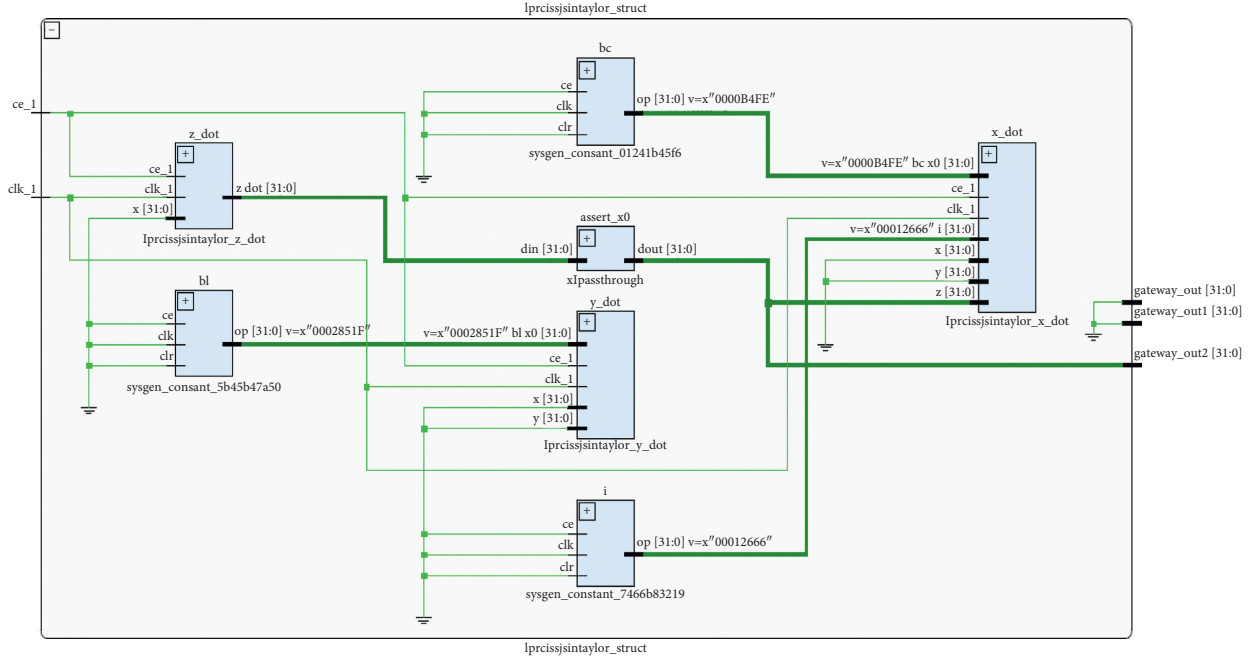
Figure 1: RTL architecture of the NRCISJJ model.

The results of numerical simulations and FPGA implementation of NRCISJJ model are illustrated in Figure 2.

Four different shapes of chaotic attractors are depicted in Figure 2 for given values of parameters i, β_C, and β_L. Moreover, in Figure 2, there is a good qualitative agreement between the numerical simulations and FPGA results.

3. Application of the Chaotic NRCISJJ Model to Secure sEMG Signal Using Chaotic Logistic Map Image Encryption Technique

The proposed encryption technique is based on that used in image encryption by the chaotic logistics map. Innovation takes place in the chaotic sequence. Indeed, the chaotic sequence of the logistic map is replaced in the algorithm by the chaotic sequence of the NRCISJJ model.

The NRCISJJ model is used as a chaotic sequence to apply the sEMG signal encryption technique rather than the chaotic logistic map sequence due to the sensitivity of its key. During the simulation, we found that the key of the NRCISJJ was more sensitive than that of the logistics map. The proposed sEMG signal encryption scheme is shown in Figure 3.

The method presented in Figure 3 consists in transforming the sEMG signal (sEMG_1D) in the form of an image (sEMG_2D). Several works have shown that the manipulation of sEMG in 2D gives better results than sEMG in 1D [32, 33]. The 2D sEMG signal is easily manipulated for pixel swapping. The process of transforming sEMG_1D into sEMG_2D used is described in [34, 35]. Once the signal is transformed into two dimensions as a grayscale image, the encryption algorithm is applied.

The following lines summarize step by step the encrypted proposed scheme of Figure 3.

Step 1 : transform the sEMG_1D signal into sEMG_2D as a grayscale image

Step 2 : generate the chaotic sequence by the chaotic NRCISJJ with the parameters: $i = 1.15$, $\beta_L = 3$, and $\beta_C = 0.707$, and the initial conditions are $(x(0), y(0), z(0)) = (0, 0, 0)$

Step 3 : generate n-iteration with the NRCISJJ model of system (1) to have $h(i)$ for different orbits

Step 4 : match the chaotic sequences with the sEMG_2D image pixels

Step 5 : make a permutation in the lines in N-iteration

Step 6 : make a permutation in the columns in M-iteration and obtain the encrypted sEMG_2D signal

Step 7 : display the encrypted image

Step 8 : transform the sEMG_2D into sEMG_1D and display.

The sEMG signals used are the clinical data acquired from a database. PhysioBank ATM database is used in [36]. In the following, different resolutions of surface EMG_2D are used in Table 1.

KHEIR1, KHEIR2, and JOUVE3 S_EMG 1D signals belong to holy patients, while EMG_MYOPATHY and EMG_HEALTHY S_EMG 1D signals are for not holy patients.

3.1. Key Sensitivity Analysis

3.1.1. Correlation Analysis. The formula for the correlation between two neighboring pixels (w and c, for example) is given by the following relation:

(a)

(b)

(c)

(d)

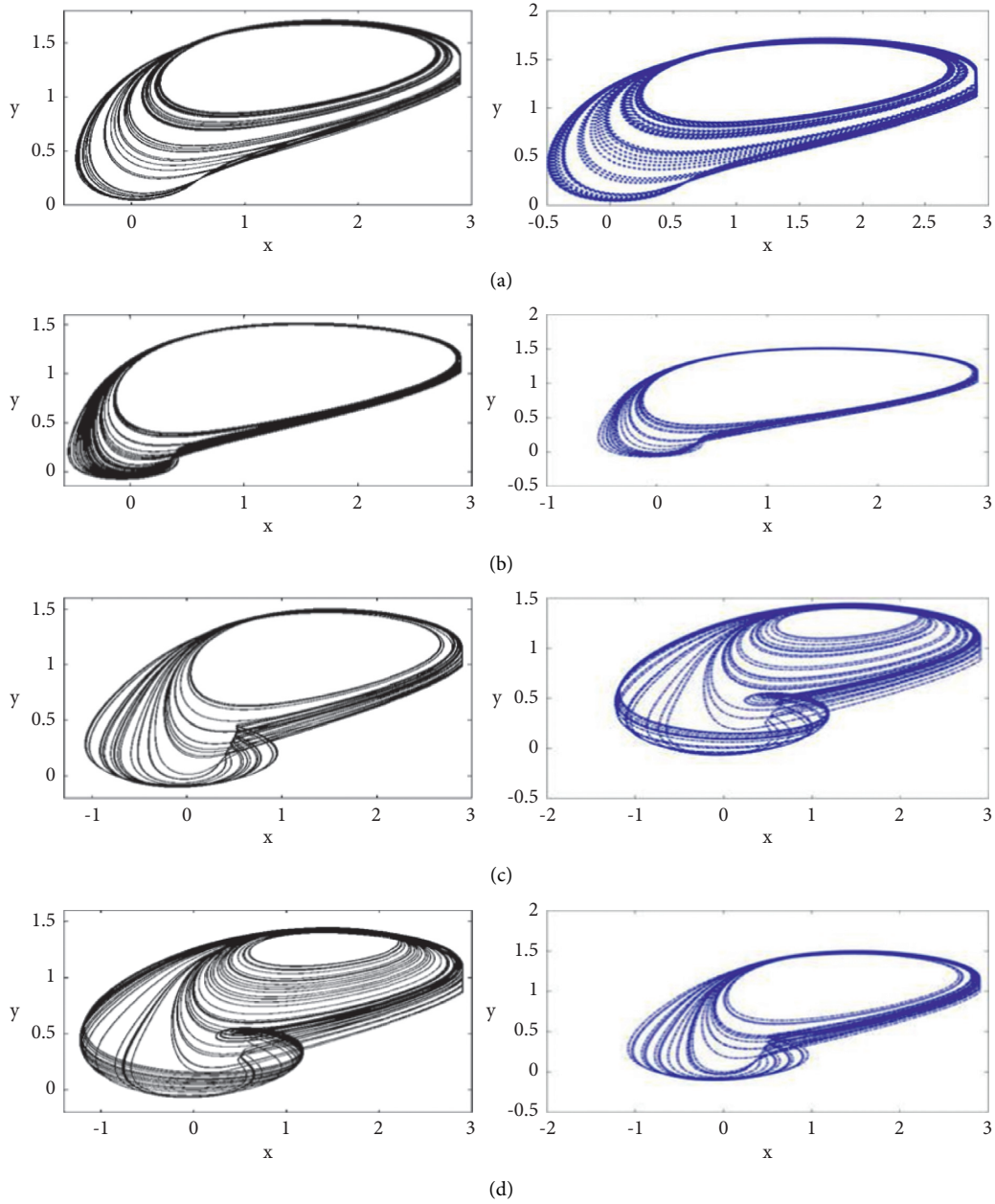Figure 2: 2D phase portraits of numerical simulations and FPGA implementation of the NRCISJJ model for given values of parameter i and β_L: (a) $i = 1.36$ and $\beta_L = 2.07$, (b) $i = 1.15$ and $\beta_L = 2.52$, (c) $i = 1.15$ and $\beta_L = 2.6$, and (d) $i = 1.15$ and $\beta_L = 3$. The other parameter is $\beta_C = 0.707$ and the initial conditions are (x(0), y(0), z(0))=(0, 0, 0).

$$\gamma_{x,y} = \frac{E(y - E(y))(x - E(x))}{\sqrt{D(y)D(x)}},$$

$$E(x) = \frac{1}{T}\sum_{i=1}^{T} x_i,$$

$$D(x) = \frac{1}{T}\sum_{i=1}^{T}(x_i - E(x))^2,$$

(4)

where the integer T refers to the total number of adjoining pixels and $D(x)$ and $E(x)$ are the variance and expectation of x, respectively.

Table 2 shows the correlation coefficients of the original sEMG_2D and sEMG_2D encrypted using the proposed approach.

It can be seen from Table 2 that the correlation coefficients of the input images are close to 1, while the correlation coefficients of the cipher images are close to 0, indicating that the pixels of the cipher images are not correlated. These
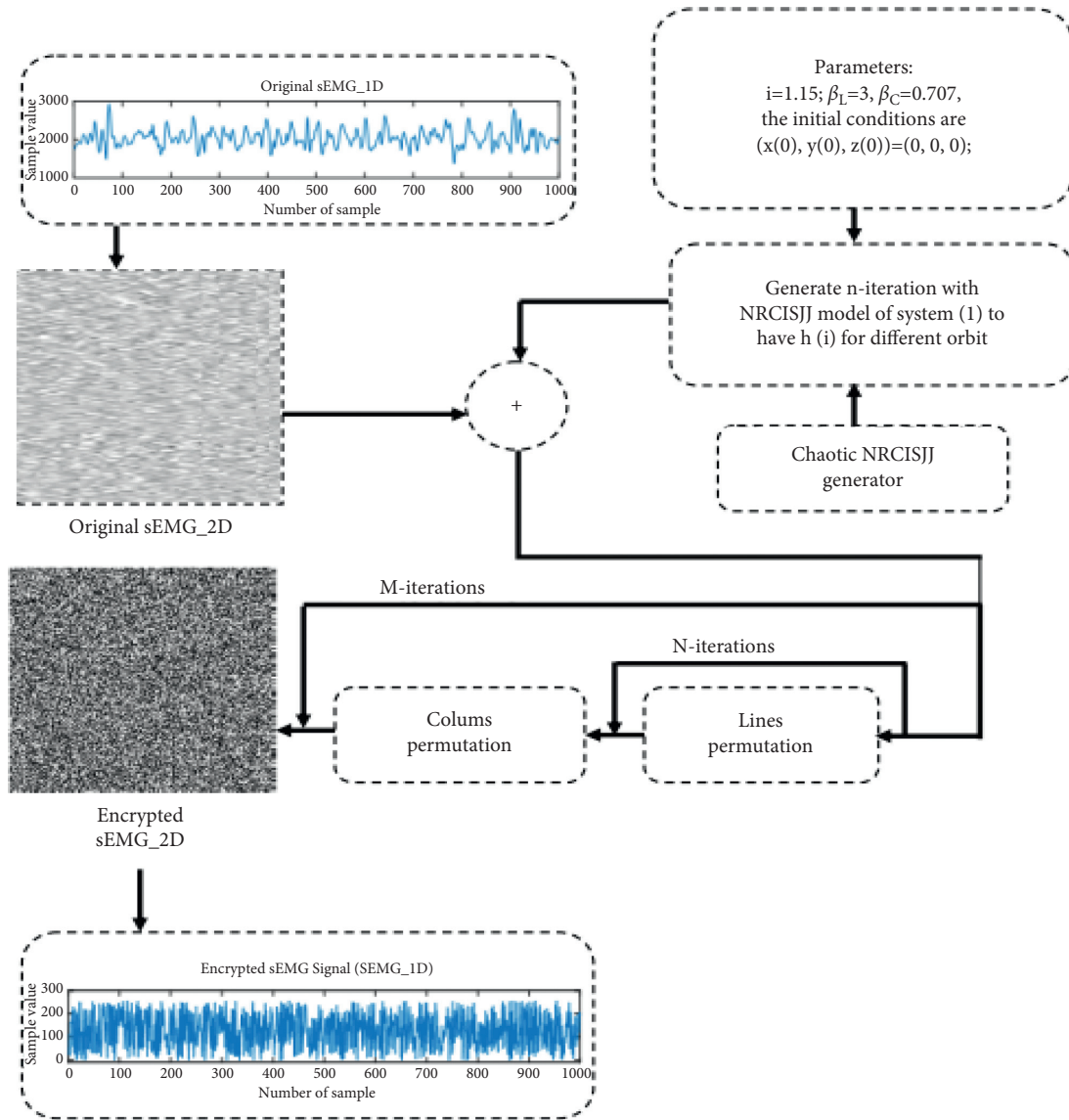
FIGURE 3: Schematic diagram of the proposed encryption scheme.

TABLE 1: S_EMG 2D and their resolutions.

S_EMG 1D	S_EMG 2D	RESOLUTION
KHEIR1	KHEIR1_2D	$180 * 180$
KHEIR2	KHEIR2_2D	$180 * 180$
JOUVE3	JOUVE3_2D	$180 * 180$
EMG_MYOPATHY	EMG_MYOPATHY_2D	$148 * 148$
EMG_HEALTHY	EMG_HEALTHY_2D	$53 * 53$

results confirm that the proposed algorithm can remove the correlation between adjacent pixels in the encrypted sEMG signals. These results sufficiently show that the encryption algorithm is well suited to EMG signals. Figures 4–8 show a visual representation of the correlation coefficients of the original, encrypted, and decrypted sEMG_2D signal.

From Figures 4 to 8, 200, 300, or even 400 pairs of adjacent pixels are randomly selected from the images to show their adjacent pixel distribution maps. This implies the strong correlation effect in the input and decrypted sEMG_2D signals, while there is a weak correlation effect in the encrypted sEMG_2D signals. These figures verify well that there is no significant correlation between pixels of the encrypted sEMG_2D signals. In addition to the encouraging encryption result offered by the proposed algorithm, Figures 4 to 8 also show that the proposed algorithm gives a decrypted sEMG_2D image very close to the original sEMG_2D image.

TABLE 2: The correlation coefficient γ of signals (S_EMG 2D).

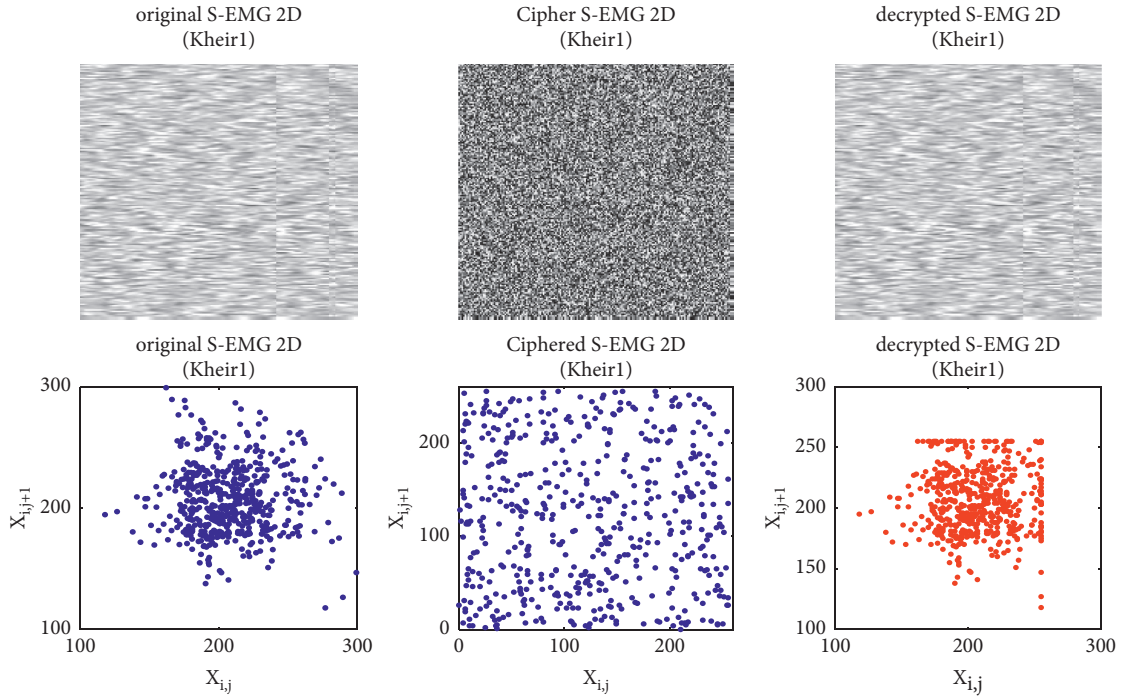| S_EMG 2D	γ	γ of input signal	Proposed chaotic NRCISJJ
KHEIR1_2D	γ_h	0.9510	−0.0005
	γ_v	−0.0054	0.0028
	γ_d	−0.0050	−0.0009
KHEIR2_2D	γ_h	0.9170	0.0095
	γ_v	0.0017	−0.0012
	γ_d	−0.0009	−0.0078
EMG_MYOPATHY_2D	γ_h	0.4520	−0.0073
	γ_v	0.0158	−0.0069
	γ_d	0.0067	−0.0001
EMG_HEALTHY_2D	γ_h	0.7484	−0.0021
	γ_v	0.0984	−0.0032
	γ_d	0.0852	−0.0113
JOUVE3_2D	γ_h	0.9526	−0.0032
	γ_v	−0.0368	−0.0032
	γ_d	0.0379	−0.0076

FIGURE 4: Correlations of KHEIR1_2D. The first column is the input signal with its correlation, the second column is the corresponding cipher signal with its correlation and the third column is the decrypted signal with its correlation.

3.2. Information Entropy.

For a grayscale image, the intensity has 2^8 possible types of values, so its ideal IFE is 8. The IFE can be defined by

$$E(n) = \sum_{i=0}^{M-1} p(n_i)\log_2\left(\frac{1}{p(n_i)}\right), \tag{5}$$

where M is the total number of samples $n_i \varepsilon n$, $p(n_i)$ denotes the probability of occurrence of the sample n_i, and log with base 2 signifies the entropy expressed in bits.

When the signal sEMG_1D is transformed into sEMG_2D in the form of an image, the image obtained has the characteristics of a grayscale image. Thus, to have a high security encrypted image, the entropy of the encrypted image must be as high as possible, i.e., very close to 8 [37, 38]. As can be seen in Table 3, the information entropy of the various encrypted sEMG_2D signals is close to 8, as shown in Table 3.

These results of Table 3 once again confirm that the data of the sEMG signals are well encrypted and with a high level of security.

3.3. Resistance to One Bit Changing Attack.

To ensure the security of an image encryption scheme against differential scanning, two quantitative measures are used: the NPCR
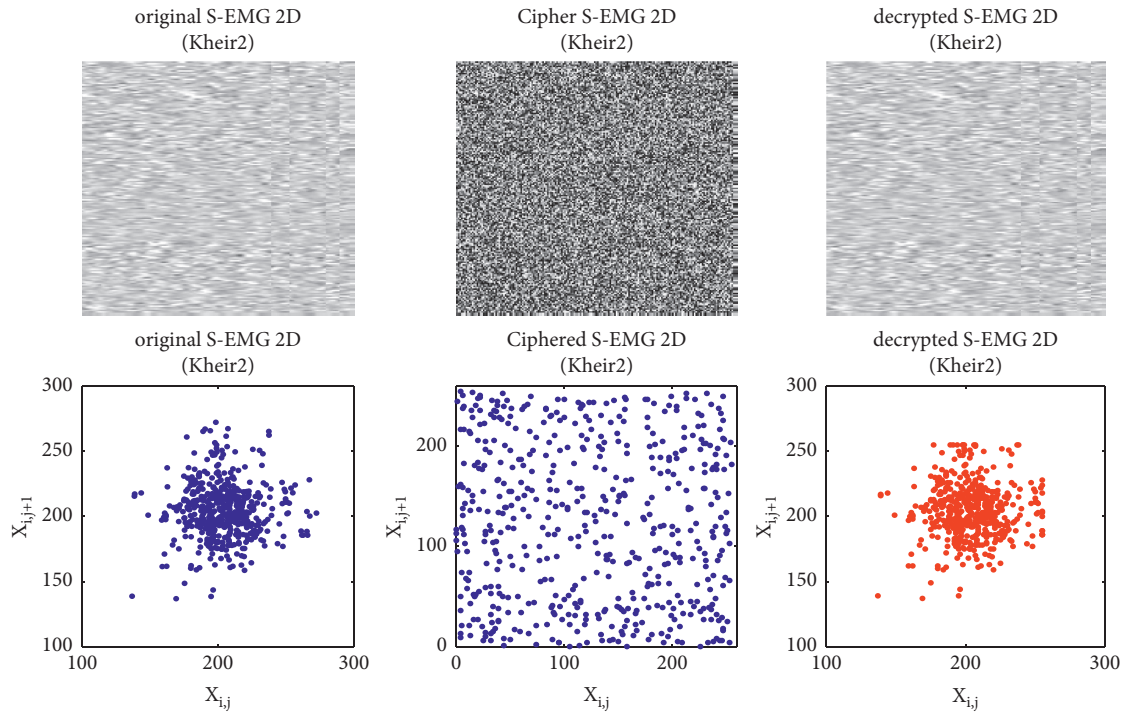
FIGURE 5: Correlations of KHEIR2_2D. The first column is the input signal with its correlation, the second column is the corresponding cipher signal with its correlation, and the third column is the decrypted signal with its correlation.
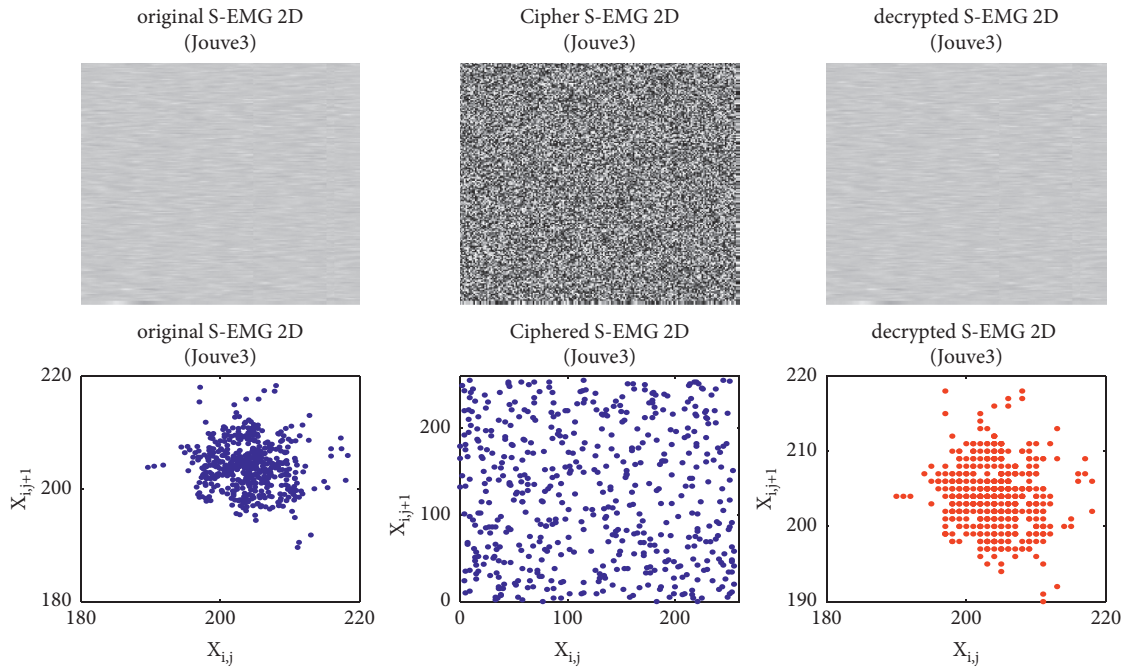

FIGURE 6: Correlations of JOUVE3_2D. The first column is the input signal with its correlation, the second column is the corresponding cipher signal with its correlation, and the third column is the decrypted signal with its correlation.

original S-EMG 2D
(emg-myopathy)

Cipher S-EMG 2D
(emg-myopathy)

decrypted S-EMG 2D
(emg-myopathy)

original S-EMG 2D
(emg-myopathy)

Ciphered S-EMG 2D
(emg-myopathy)

decrypted S-EMG 2D
(emg-myopathy)

Figure 7: Correlations of MYOPATHY_2D. The first column is the input signal with its correlation, the second column is the corresponding cipher signal with his correlation, and the third column is the decrypted signal with its correlation.

original S-EMG 2D
(emg-healthy)

Cipher S-EMG 2D
(emg-healthy)

decrypted S-EMG 2D
(emg-healthy)

Original S-EMG 2D
(emg-healthy)

Ciphered S-EMG 2D
(emg-healthy)

decrypted S-EMG 2D
(emg-healthy)

Figure 8: Correlations of HEATHY_2D. The first column is the input signal with its correlation, the second column is the corresponding cipher signal with its correlation, and the third column is the decrypted signal with its correlation.
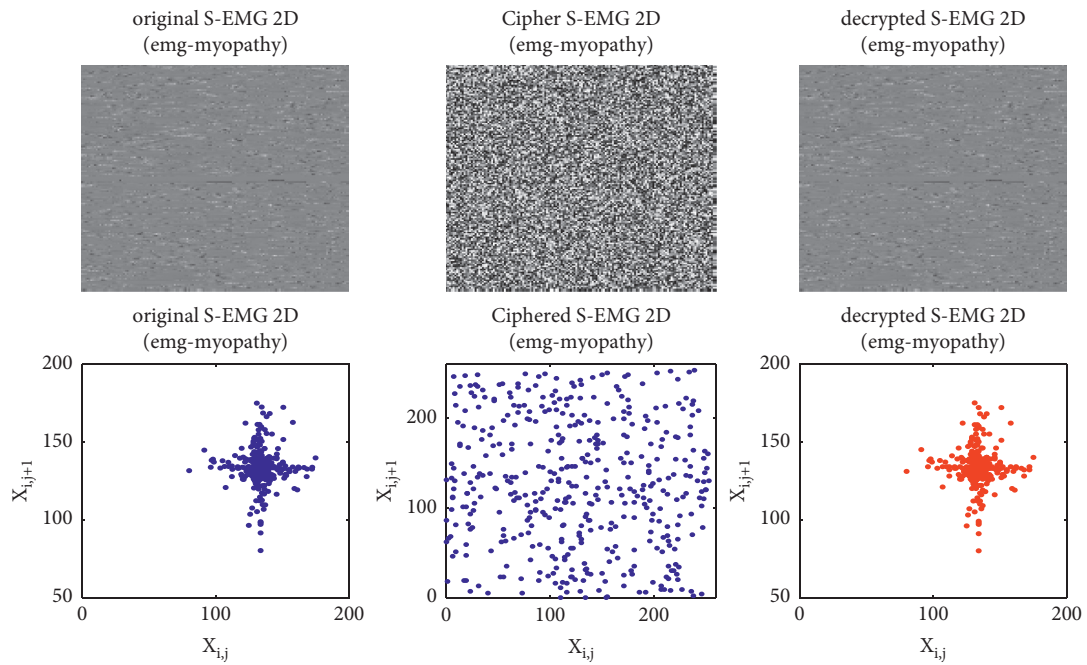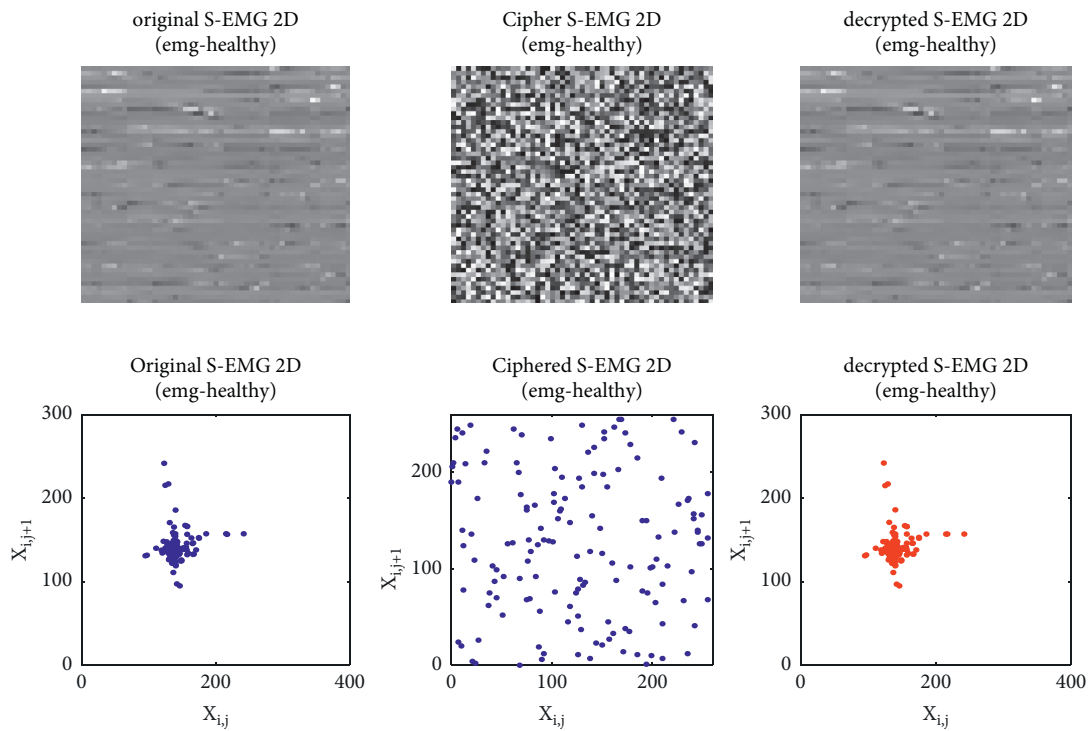
Table 3: Information entropy performance of cipher S_EMG 2D.

S_EMG 2D	Chaotic NRCISJJ
KHEIR1_2D	7.9941
KHEIR2_2D	7.9936
EMG_MYOPATHY_2D	7.9885
EMG_HEALTHY _2D	7.9388
JOUVE3_2D	7.9923

(number of pixels' change rate) and the UACI (unified average changing intensity). The NPCR represents the rate of different pixels between the two encrypted images, while the UACI represents the difference in average intensity [39].

The formula used to calculate these two percentages is defined as follows [37]:

$$NPCR = \frac{1}{M \times N} \sum_{i+1}^{M} \sum_{j=1}^{N} DIF(i, j) \times 100,$$

$$UACI = \frac{1}{M \times N} \sum_{i+1}^{M} \sum_{j=1}^{N} \frac{|C_2(i, j) - C_1(i, j)|}{255} \times 100 \, (\%),$$

$$with \, DIF(i, j) = \begin{cases} 0, & C_2(i, j) = C_1(i, j), \\ 1, & C_2(i, j) \neq C_1(i, j), \end{cases}$$

(6)

where C_2 refers to the crypted image that is encrypted from the original image by changing only one pixel, while C_1 refers to the cipher image encrypted from the same plain image.

When an NPCR > 99.6094%, a UACI > 33.4635% ensures that an image encryption scheme is secure against this attack [40, 41]. Table 4 depicts the values of NPCR and UACI obtained on the sEMG_2D signal.

From the results obtained and presented in Table 4, it appears that all the NPCR values are greater than the optimum value of 99.6094%. As for the values of the UACI, we record two values lower than the optimal value of 33.4635%. Curiously, these two UACI values are obtained on the sEMG signals of patients who are not holy. This observation thus opens another axis of reflection that will furnish our perspective. Apart from these two values, we can conclude that an image encryption scheme is secure against the differential attack.

3.4. Quality Metrics Analysis between Plain and Encrypted.

Table 5 shows the analysis of signal quality. After encrypting the signal in 2D, we transform it into 1D to analyze the effect of the encryption on it. The medical personnel who receive the encrypted signal decrypt it for a diagnosis. To avoid misdiagnosis, medical personnel should not receive a corrupt signal. This is why in Table 5 we study the distortion between the original signal and the decrypted signal. This distortion is quantified by the following metrics: the percent root mean square difference (PRD) (%) and the signal to noise ratio (SNR).

3.4.1. Mean Square Error (MSE). The most commonly used quality measure is mean square error (MSE) and is defined by

$$MSE = \frac{1}{N} \sum_{n=1}^{N} (y_O[n] - y_r[n])^2,$$

(7)

where $y_O[n]$ is the original surface EMG signal, $y_r[n]$ is the decrypted surface EMG signal, and N is the number of samples of the signal.

3.4.2. Signal-to-Noise Ratio (SNR).

$$SNR = 10Log_{10}\left(\frac{\sigma_x^2}{\sigma_e^2}\right).$$

(8)

where Log is decimal logarithm. With σ_x^2 as the spectral power of the original SEMG signal and σ_e^2 as the spectral power of the decrypted error.

3.4.3. Percent Root Mean Square Difference (PRD). The PRD (percent root mean square difference) is defined by

$$PRD = \sqrt{\frac{\sum_{n=0}^{N-1}(y_O[n] - y_r[n])^2}{\sum_{n=0}^{N-1}(y_O[n] - \mu)^2}} \cdot 100\%,$$

(9)

where N is the number of samples of the original sEMG signal, μ is the reference value of the DAC (digital analog converter) used for data acquisition s(n) ($\mu = 0$ for EMG signals), $y_r[n]$ is the decrypted sEMG signal, and $y_O[n]$ is the original sEMG signal [34].

Analysis of the values in Table 5 shows that the decrypted sEMG signal resembles the original signal. This can be seen through the value of the PRD which must be as small as possible and that of the SNR must be high. This statement can be verified by observing Figures 9–13.

Figures 9 to 13 present the original, encrypted, and decrypted sEMG signals of the signals KHEIR1, KHEIR2, JOUVE3, MYOPATHY, and HEALTHY, respectively. For each figure, the first line is the input signal, the second line is the corresponding cipher signal, and the third line is the decrypted signal.

3.5. Encryption Time.

In telemedicine, the interaction between two health specialists can be in real time. So, the communications must be as fast as possible. Therefore, the encryption and decryption times should be as small as possible. Table 6 shows the encryption and decryption time of the proposed algorithm. The proposed algorithm is implemented in MATLAB R2015a and the "*run and time*" function is used. The characteristics of the machine are as follows:

(i) Name: DESKTOP-FO74VUD

(ii) RAM installed: 8,00 Go (7,85 Go useable)

(iii) Device ID: DD9D7612-CE5F-4069-85ED-6F57D40 3F31C

TABLE 4: Average performance of NPCR (%) and UACI (%).

S_EMG 2D	NPCR (%)	UACI (%)
KHEIR1_2D	99.9660	35.5353
KHEIR2_2D	99.9599	34.9161
EMG_MYOPATHY_2D	100	24.5620
EMG_HEALTHY _2D	100	25.3572
JOUVE3_2D	99.9568	35.5353

TABLE 5: Quality metrics analysis.

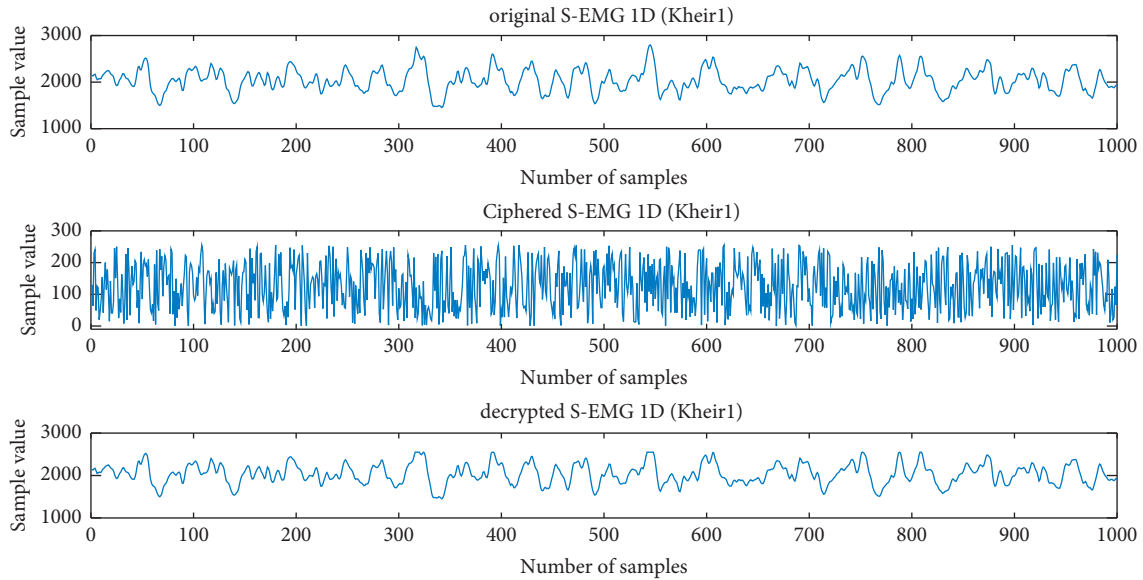| S_EMG_1D	PRD (%)	SNR (dB)	MSE
KHEIR1_1D	1.66	35.62	1165.37
KHEIR2_1D	0.87	41.24	317.92
EMG_MYOPATHY_1D	3.00	30.46	859.00
EMG_HEALTHY _1D	1.93	34.28	183.29
JOUVE3_1D	0.14	56.90	8.49

FIGURE 9: Input signal, cipher signal, and decrypted signal of KHEIR1_1D. The first is the input signal, the second is the corresponding cipher signal, and the third is the decrypted signal.

FIGURE 10: Input signal, cipher signal, and decrypted signal of KHEIR2_1D. The first is the input signal, the second is the corresponding cipher signal, and the third is the decrypted signal.

FIGURE 11: Input signal, cipher signal, and decrypted signal of JOUVE3_1D. The first is the input signal, the second is the corresponding cipher signal, and the third is the decrypted signal.

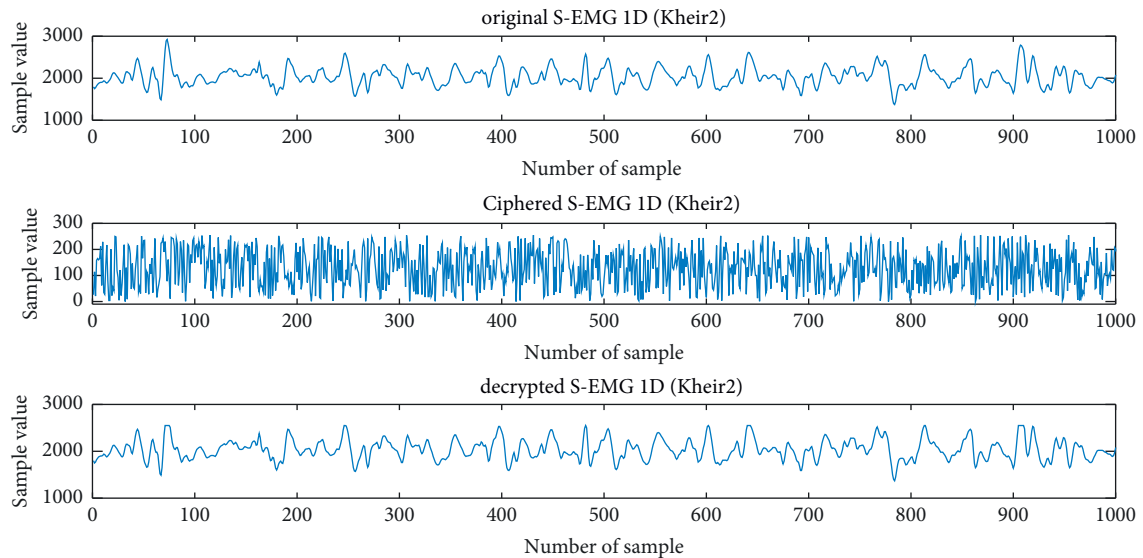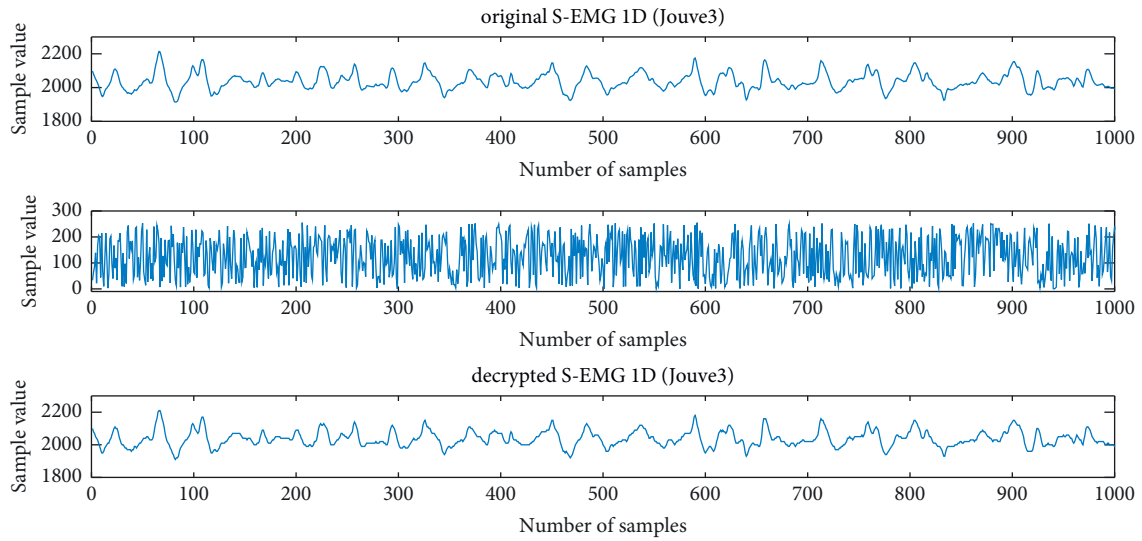

FIGURE 12: Input signal, cipher signal, and decrypted signal ofMYOPATHY_1D. The first is the input signal, the second is the corresponding cipher signal, and the third is the decrypted signal.

Figure 13: Input signal, cipher signal, and decrypted signal of HEALTY_2D. The first is the input signal, the second is the corresponding cipher signal, and the third is the decrypted signal.

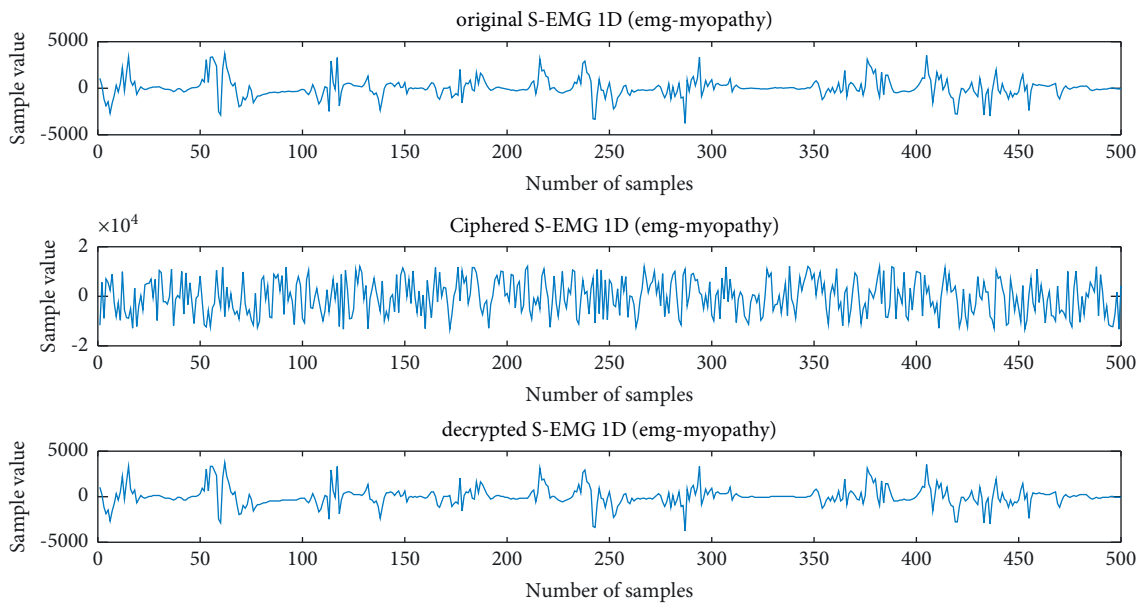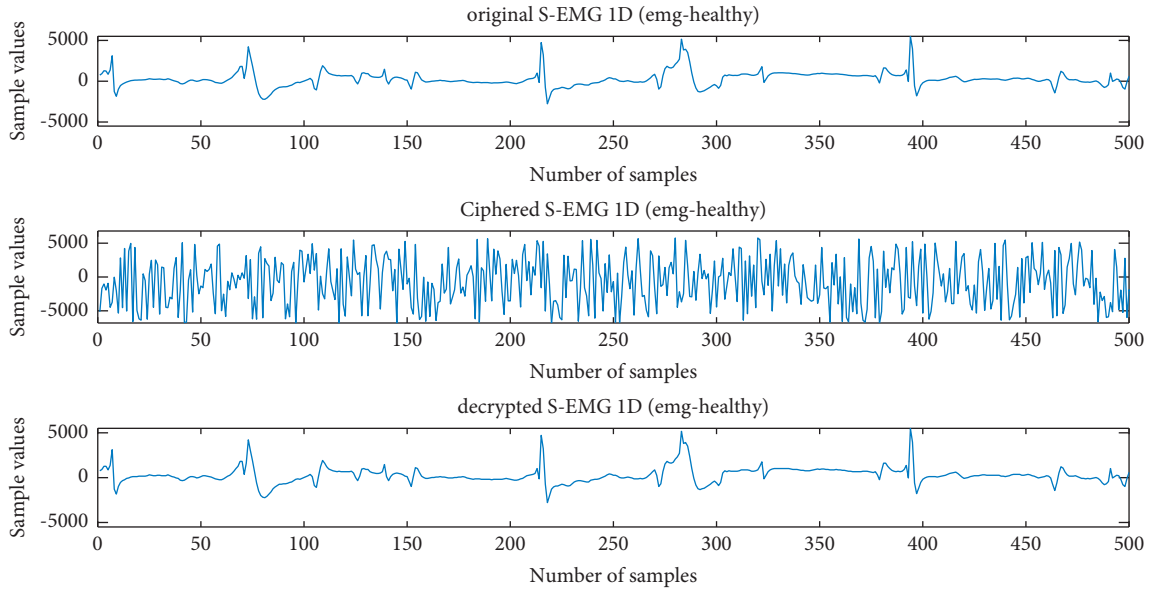Table 6: Encrypted and decrypted time.

S_EMG 2D	Resolution	Proposed chaotic NRCISJJ	
		Encrypted time (s)	Decrypted time (s)
KHEIR1_2D	180 * 180	0.336	1.701
KHEIR2_2D	180 * 180	0.351	1.676
EMG_MYOPATHY_2D	148 * 148	0.223	1.241
EMG_HEALTHY_2D	53 * 53	0.028	0.169
JOUVE3_2D	180 * 180	0.361	1.757

Table 7: Comparison of the proposed encryption scheme with recent schemes reported in literature, where $\sqrt{}$ means "achieved" and — means "not achieved."

	[42]	[43]	[44]	[45]	Proposed chaotic NRCISJJ
Clinical signals					
ECG	$\sqrt{}$	$\sqrt{}$	—	—	—
BP	$\sqrt{}$	—	—	—	—
EEG	$\sqrt{}$	—	$\sqrt{}$	$\sqrt{}$	—
EMG	—	—	—	—	$\sqrt{}$
Acquisition method					
Live sensing	—	—	—	—	—
Database technique	PhysioBank ATM	MIT−BIH	UCI KDD	NTOU	PhysioBank ATM
Encryption	$\sqrt{}$	$\sqrt{}$	$\sqrt{}$	$\sqrt{}$	$\sqrt{}$
Compression	—	$\sqrt{}$	—	—	—
Chaos specifications					
Chaotic map	Logistic map	Not specified	Logistic map	Logistic map	Chaotic NRCISJJ
Lyapunov exponent	$\sqrt{}$	—	—	—	—
Security analysis					
Secret key space	$\sqrt{}$	—	—	—	—
Correlation	$\sqrt{}$	—	$\sqrt{}$	—	$\sqrt{}$
Autocorrelation	$\sqrt{}$	—	—	—	$\sqrt{}$
Secret key sensitivity	$\sqrt{}$	—	—	$\sqrt{}$	$\sqrt{}$
Plain signal sensitivity	$\sqrt{}$	—	—	—	—
Floating frequency	$\sqrt{}$	—	—	—	—
Information entropy	$\sqrt{}$	—	—	—	$\sqrt{}$
Mean square error	$\sqrt{}$	—	$\sqrt{}$	—	$\sqrt{}$
Pick signal-to-noise ratio	$\sqrt{}$	—	—	—	—

Table 7: Continued.

	[42]	[43]	[44]	[45]	Proposed chaotic NRCISJJ
Structural similarity index	√	—	—	—	—
Encryption time	√	—	—	√	√
Distortion criteria					
Signal-to-noise ratio	—	—	—	—	√
Percentage residual deviation	—	√	—	√	√

(iv) Product ID: 00330-80000-00000-AA798

(v) System type: 64 bits, processor x64

These times for all signals show that the proposed algorithm is fast. The comparison analyses are presented in Table 7.

4. Conclusion

The field programmable gate array implementation of the nonlinear resistor-capacitor-inductor shunted Josephson junction model and its application to secure surface electromyographic signal were investigated in this study. Different shapes of chaotic attractors were revealed by using numerical simulations and field programmable gate array implementation of the nonlinear resistive-capacitive-inductive shunted Josephson junction model. The aim of this paper was to show that it is possible to encrypt the surface electromyographic signal through image encryption techniques which was achieved. For a first experiment on the encryption of sEMG signals, the results obtained are encouraging. However, it appears that the results are not as powerful as when the encryption technique is applied to surface electromyographic signal of patients with pathology. This can be due to the fact that the signals of holy patients concentrated more information towards the lower frequencies while the signals of pathological patients concentrated the most information towards the higher frequencies. This will be the subject of a study in future works.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

On behalf of all authors, the corresponding author states that there are no conflicts of interest.

Acknowledgments

References

[1] T. G. Zhou, D. C. Wang, F. L. Liu, L. Fang, X. J. Zhao, and S. L. Yan, "Simulation of chaos in different models of josephson junctions," *Journal of System Simulation*, vol. 22, pp. 666–669, 2010.

[2] S. Das, S. Datta, and D. Sahdev, "Mode-locking, hysteresis and chaos in coupled josephson junctions," *Physica D: Nonlinear Phenomena*, vol. 101, no. 3-4, pp. 333–345, 1997.

[3] C. R. Nayak and V. C. Kuriakose, "Dynamics of coupled josephson junctions under the influence of applied fields," *Physics Letters A*, vol. 365, no. 4, pp. 284–289, 2007.

[4] X.-S. Yang and Q. Li, "A computer-assisted proof of chaos in josephson junctions," *Chaos, Solitons & Fractals*, vol. 27, no. 1, pp. 25–30, 2006.

[5] T. Kawaguchi, "Directed transport and complex dynamics of vortices in a josephson junction network driven by modulated currents," *Physica C: Superconductivity and its Applications*, vol. 470, no. 20, pp. 1133–1136, 2010.

[6] S. Al-Khawaja, "Chaotic dynamics of underdamped josephson junctions in a ratchet potential driven by a quasiperiodic external modulation," *Physica C: Superconductivity and its Applications*, vol. 420, no. 1-2, pp. 30–36, 2005.

[7] M. MacHida, T. Koyama, A. Tanaka, and M. Tachiki, "Theory of the superconducting phase and charge dynamics in intrinsic Josephson-junction systems: microscopic foundation for longitudinal Josephson plasma and phenomenological dynamical equations," *Physica C: Superconductivity*, vol. 331, no. 1, pp. 85–96, 2000.

[8] M. Hayashi, M. Suzuki, J. Onuki, and H. Ebisawa, "Nonlinear dynamics of intrinsic Josephson junctions under an applied current," *Applications*, vol. 463-465, pp. 993–996, 2007.

[9] S. K. Dana, D. C. Sengupta, and K. D. Edoh, "Chaotic dynamics in Josephson junction," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 48, no. 8, pp. 990–996, 2001.

[10] A. B. Cawthorne, C. B. Whan, and C. J. Lobb, "Complex dynamics of resistively and inductively shunted Josephson junctions," *Journal of Applied Physics*, vol. 84, no. 2, pp. 1126–1132, 1998.

[11] U. E. Vincent, A. Ucar, J. A. Laoye, and S. O. Kareem, "Control and synchronization of chaos in RCL-shunted Josephson junction using backstepping design," *Physica C: Superconductivity*, vol. 468, no. 5, pp. 374–382, 2008.

[12] A. N. Njah, K. S. Ojo, G. A. Adebayo, and A. O. Obawole, "Generalized control and synchronization of chaos in RCL-shunted Josephson junction using backstepping design," *Physica C: Superconductivity*, vol. 470, no. 13-14, pp. 558–564, 2010.

[13] S. K. Dana, D. C. Sengupta, and C.-K. Hu, "Spiking and bursting in Josephson junction," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 53, no. 10, pp. 1031–1034, 2006.

[14] M. Canturk and I. N. Askerzade, "Numerical study of I–V characteristics of externally shunted Josephson junctions with unharmonic current-phase relation," *IEEE Transactions on Applied Superconductivity*, vol. 22, Article ID 1400111, 2012.

[15] M. Canturk and I. N. Askerzade, "Chaotic dynamics of externally shunted Josephson junction with Unharmonic CPR," *Journal of Superconductivity and Novel Magnetism*, vol. 26, no. 4, pp. 839–843, 2013.

[16] S. T. Kingni, G. F. Kuiate, R. Kengne, R. Tchitnga, and P. Woafo, "Analysis of a no equilibrium linear resistive-capacitive-inductance shunted Junction model, dynamics, synchronization, and application to digital cryptography in its fractional-order form," *Complexity*, vol. 2017, Article ID 4107358, 12 pages, 2017.

[17] S. T. Kingni, K. Rajagopal, S. Çiçek, A. Cheukem, V. K. Tamba, and G. F. Kuiate, "Dynamical analysis, FPGA implementation and its application to chaos based random number generator of a fractal Josephson junction with unharmonic current-phase relation," *The European Physical Journal B*, vol. 93, no. 3, p. 44, 2020.

[18] A. N. Kadjie, H. Tchakounté, I. Kemajou, and P. Woafo, "Microcontroller-based simulation of a nonlinear resistive-capacitive-inductance shunted Josephson junction model and applications in electromechanical engineering," *International Journal of Nonlinear Sciences and Numerical Stimulation*, vol. 22, 2021.

[19] Q. Lai and Z. Wan, "Modelling and circuit realisation of a new no-," *Electronics Letters*, vol. 56, no. 20, pp. 1044–1046, 2020.

[20] B. Ramakrishnan, A. A. Oumate, M. Tuna, İ. Koyuncu, S. T. Kingni, and K. Rajagopal, "Analysis, FPGA implementation of a Josephson junction circuit with topologically nontrivial barrier and its application to ring-based dual entropy core true random number generator, Eur," *Phys. J. Spec. Top.*, vol. 230, pp. 18–20, 2021.

[21] Q. Lai, B. Norouzi, and F. Liu, "Dynamic analysis, circuit realization, control design and image encryption application of an extended Lü system with coexisting attractors," *Chaos, Solitons & Fractals*, vol. 114, pp. 230–245, 2018.

[22] Q. Lai, Z. Wan, L. K. Kengne, P. D. K. Kuate, and C. Chen, "Two-memristor-based chaotic system with infinite coexisting attractors," *IEEE Transactions On Circuits And Systems—Ii: Express Briefs*, vol. 68, no. 6, 2021.

[23] A. Hamzenejad, S. J. Ghoushchi, V. Baradaran, and A. Mardani, "A robust algorithm for classification and diagnosis of brain disease using local linear approximation and generalized autoregressive conditional heteroscedasticity model," *Advance in Mathematics*, vol. 8, 2020.

[24] C. K. Filelis-Papadopoulos, P. T. Endo, M. Bendechache et al., "Towards simulation and optimization of cache placement on large virtual content distribution networks," *Journal of Computer Science*, vol. 39, Article ID 101052, 2020.

[25] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons & Fractals*, vol. 21, no. 3, pp. 749–761, 2004.

[26] Y. Mao, G. Chen, and S. Lian, "A novel fast image encryption scheme based on 3D chaotic baker maps," *International Journal of Bifurcation and Chaos*, vol. 14, no. 10, pp. 3613–3624, 2004.

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

[28] A. N. Pisarchik, N. J. Flores-Carmona, and M. Carpio-Valadez, "Encryption and decryption of images with chaotic map lattices," *Chaos*, vol. 16, Article ID 033118, 2006.

[29] J. W. Yoon and H. Kim, "An image encryption scheme with a pseudorandom permutation based on chaotic maps," *Communications in Nonlinear Science and Numerical Simulation*, vol. 15, no. 12, pp. 3998–4006, 2010.

[30] X. Wang and H.-l. Zhang, "A novel image encryption algorithm based on genetic recombination and hyper-chaotic systems," *Nonlinear Dynamics*, vol. 83, no. 1-2, pp. 333–346, 2016.

[31] X. Huang, T. Sun, Y. Li, and J. Liang, "A color image encryption algorithm based on a fractional-order hyperchaotic system," *Entropy*, vol. 17, no. 1, pp. 28–38, 2014.

[32] M. H. Trabuco, M. V. C. Costa, and B. Macchiavello, "S-EMG signal compression in one-dimensional and two-dimensional approaches," *IEEE Journal of Biomedical and Health Informatics*, vol. 22, no. 4, pp. 1104–1113, 2018.

[33] E. D. B. F. Lima and W. S. D. Silva Júnior, "SEMG signal compression based on two-dimensional techniques," *Bio-Medical Engineering Online*, vol. 15, no. 1, 2016.

[34] C. Welba, A. J. O. Okassa, P. N. Eloundou, and P. Ele, "Contribution to S-EMG signal compression in 1D by the combination of the modified discrete wavelet packet transform (MDWPT) and the discrete cosine transform (DCT)," *Journal of Signal and Information Processing*, vol. 11, no. 03, pp. 35–57, 2020.

[35] C. Welba, E. P. Ntsama, and P. Ele, "Exploitation of differential pulse code modulation for compression of EMG signals by a combination of DWT and DCT," *American Journal of Biomedical Engineering*, vol. 4, pp. 25–32, 2014.

[36] "PhysioBank A. T. M.," 2016, https://physionet.org/cgi-bin/atm/ATM.

[37] Y. Jiayin, X. Yaqin, G. Shiyu, Z. Yanqi, and W. Erfu, "Parallel encryption of noisy images based on sequence generator and chaotic measurement matrix," *Complexity*, vol. 18, Article ID 1987670, , 2020.

[38] K. M. Hosny, S. T. Kamal, M. M. Darwish, and G. A. Papakostas, "New image encryption algorithm using hyperchaotic system and fibonacci Q-matrix," *Electronics*, vol. 10, no. 9, 2021.

[39] K. Zhan, D. Wei, J. Shi, and J. Yu, "Cross-utilizing hyperchaotic and DNA sequences for image encryption," *Journal of Electronic Imaging*, vol. 26, no. 1, pp. 13–21, 2017.

[40] A. Beloucif, "Contribution à l'étude des mécanismes cryptographiques; Université de Batna 2, Faculté de mathématiques et d'informatique," *Thèse en vue de l'obtention du diplôme de Doctorat en Informatique*, 2016.

[41] F. Hadji, "Conception et réalisation d'un système décryptage pour les images médicales," *Mémoire présenté pour l'obtention du diplôme de Master Académique*, Université MOHAMED BOUDIAF - M'SILA, 2018.

[42] M. A. Murillo-Escobar, L. Cardoza-Avendano, R. M. Lopez-Gutierrez, and C. Cruz-Hernandez, "A double chaotic layer encryption algorithm for clinical signals in telemedicine," *Journal of Medical Systems*, vol. 41, no. 4, pp. 41–59, 2017.

[43] M. Raeiatibanadkooki, S. R. Quchani, M. KhalilZade, and K. Bahaadinbeigy, "Compression and encryption of ECG signal using wavelet and chaotically huffman code in telemedicine application," *Journal of Medical Systems*, vol. 40, pp. 73–78, 2016.

[44] C.-F. Lin, "Chaotic visual cryptosystem using empirical mode decomposition algorithm for clinical EEG signals," *Journal of Medical Systems*, vol. 40, pp. 1–10, 2016.

[45] C. F. Lin, S. H. Shih, and J. D. Zhu, "Chaos based encryption system for encrypting electroencephalogram signals," *Journal of Medical Systems*, vol. 38, pp. 49–10, 2014.