Hindawi
Advances in Mathematical Physics
Volume 2020, Article ID 8050934, 12 pages
https://doi.org/10.1155/2020/8050934

Research Article

Speech Encryption Algorithm Based on Nonorthogonal Quantum State with Hyperchaotic Keystreams

F. J. Farsana [1] **and K. Gopakumar** [2]

[1]*Electronics and Communication, LBS Centre for Science and Technology, University of Kerala, Kerala, India*
[2]*Electronics and Communication, TKM College of Engineering, Kerala, India*

Correspondence should be addressed to F. J. Farsana; farsanafarooq@gmail.com

Received 8 May 2019; Revised 12 July 2019; Accepted 28 August 2019; Published 14 January 2020

Guest Editor: David Carfì

With the advancement in modern computational technologies like cloud computing, there has been tremendous growth in the field of data processing and encryption technologies. In this contest there is an increasing demand for successful storage of the data in the encrypted domain to avoid the possibility of data breach in shared networks. In this paper, a novel approach for speech encryption algorithm based on quantum chaotic system is designed. In the proposed method, classical bits of the speech samples are initially encoded in nonorthogonal quantum state by the secret polarizing angle. In the quantum domain, encoded speech samples are subjected to bit-flip operation according to the Controlled–NOT gate followed by Hadamard transform. Complete superposition of the quantum state in both Hadamard and standard basis is achieved through Hadamard transform. Control bits for C-NOT gate as well as Hadamard gate are generated with a modified *Lù*-hyperchaotic system. Secret nonorthogonal rotation angles and initial conditions of the hyperchaotic system are the keys used to ensure the security of the proposed algorithm. The computational complexity of the proposed algorithm has been analysed both in quantum domain and classical domain. Numerical simulation carried out based on the above principle showed that the proposed speech encryption algorithm has wider keyspace, higher key sensitivity and robust against various differential and statistical cryptographic attacks.

1. Introduction

1.1. Background. Speech encryption techniques have been widely used in confidential areas such as defence, voice over IP, voice-conferencing, news telecasting, e-commerce etc. In these applications, Integrity protection of the voice data is the major security concern, which demands the development of secure speech cryptographic algorithms. Classical data encryption methods are poorly suited for audio encryption, due to its bulky data capacity, strong correlation between adjacent data samples and the presence of unvoiced data segments. Furthermore, there is no theoretical limit on cloning or copying of data in classical cryptography. Quantum information processing is one of the promising fields of cryptography, in which the fundamental principles of quantum mechanics like Heisenberg uncertainty principle and principle of photon polarization are directly exploited [1]. Any attempt made by an intruder to clone or copy an unknown quantum state will destroy the state and it will be detected [2]. Furthermore, nonorthogonal quantum states cannot be readily distinguished even if the states are known. Quantum cryptography was developed in 1984 by the physicist Charles Henry Bennett and it was experimentally demonstrated in 1992 [3]. In 1982, Richard Feynman introduced the idea of a quantum computer, which uses the basic principles of quantum mechanics to its advantage [4]. Quantum computational model theoretically has high computational power to solve realtime mathematical problems much faster than classical computers [5, 6]. With the development in this field, computationally efficient quantum algorithms like Shores factoring algorithm, Grover's searching algorithm and discrete algorithm have been designed which may threaten classical cryptosystem [6]. Also, quantum signal processing outperforms classical signal processing since quantum Fourier transform [7], quantum discrete cosine transform [8, 9] and quantum wavelet transforms [10] are more efficient than their classical counterparts. Thus, cryptanalysts have to design new algorithms according to the principle of quantum mechanics to protect classical information.

Chaos is another elucidating theory from the field of nonlinear dynamics, which has potential applications in several

functional areas of a digital system such as compression, encryption, and modulation. It is one of the subtle behaviours associated with the evolution of a nonlinear physical system with significant properties such as topological transitivity, aperiodicity, deterministic pseudo randomness, and sensitive dependence on initial conditions [11]. The complex chaos theory have been utilized in many conventional cryptographic approaches like RC5 stream cipher and elliptical curve cryptography to strengthen the security of encryption processes [12, 13]. Cryptographic algorithms based on chaos theory consist of two operations such as permutation and diffusion. In the permutation process data samples in the plaintext is rearranged to destroy the local correlation, making the data unable to understand. While in the diffusion stage data sample is masked by the pseudorandom number generated with the chaotic systems to change the sample values. Amin and Abd El-Latif [14] proposed a secret sharing algorithm, which combines random grids (RG), error diffusion (ED) and chaotic permutation to improve the security. Gopalakrihnan and Ramakrishnan [15] introduced an image encryption algorithm where they adopted multiple chaotic systems such as Logistic-Tent Map (LTM), Logistic-Sin Map (LSM), and Tent-Sin Map (TSM) for intermediate chaotic keystream generation. The reproducibility and deterministic nature of chaotic functions add value to cryptographic processes since the process can be repeated for the same function and same initial conditions. These properties improve the security of the cryptographic process by multiple iterations of chaotic maps based on substitution and diffusion operations [16, 17]. Moreover, S–box generation mechanism based on chaotic function along with substitution and permutation process increases the complexity of the algorithm, consequentially enhances the security [18, 19]. Wang et al. [20] proposed a dynamic keystream selection mechanism for S box generation, which avoids the possibility of the chosen plain text and chosen ciphertext attacks. Data encryption techniques based on a lower dimensional chaotic system have weak resistance to brute force attack, which cannot ensure the security of data due to the small keyspace. To improve the keyspace most of the chaos-based encryption algorithms tend to take advantage of combining more than one chaotic system, but it increases the computational complexity, system resources and time. Consequently, encryption techniques based on hyperchaotic systems have been introduced [21–23]. These systems have more than one positive Lyapunov exponent and rich complex dynamic behaviour. Nonlinear dynamics and fractional order dynamical systems have been widely studied in recent years. Synchronization of fractional order complex dynamical systems has potential applications in secure communication systems. Sheue [24] proposed a speech encryption algorithm based on fractional order chaotic systems. It is based on two-channel transmission method where the original speech is encoded using a nonlinear function of the Lorenz chaotic system. They also, analysed the conditions for synchronization between fractional chaotic systems theoretically by using the Laplace transform.

1.2. Review of Related Works. Quantitative modelling and finite precision realization of nonlinear phenomenon could be easily realized with the development of quantum computational models. Therefore researchers have attempted to combine two fundamental theories of physics like deterministic chaos and probabilistic quantum dynamics to develop new cryptographic algorithms. Vidal et al., introduced an encryption technique, which attributes rich dynamics of hyperchaotic system and some fundamental properties of quantum cryptography [25]. Arnold Cat transform is applied widely as a permutation matrix in several quantum data encryption algorithm [26–29]. Abd El-Latif et al., [26] proposed an image encryption algorithm method where he utilized the concept of toral automorphism, low frequency Y -luminance subband scrambling and quantum chaotic map. In this method discretized quantum chaotic Cat map is employed for substitution by generating an intermediate chaotic key stream. Jiang et al., proposed a quantum image scrambling circuit based on Arnold and Fibonacci transformation [27]. Zhou et al., proposed an algorithm based on double phase random coding and generalized Arnold transform [28], in which image pixels are permuted by the Arnold transform and grey level information is encrypted by the double random-phase process. Akhshani et al., studied the nature of dissipative quantum systems and proposed an image encryption algorithm based on the quantum logistic map [29]. Liang et al., proposed a method, where quantum image is encrypted by XOR operation with C-NOT gate which is controlled by pseudorandom number generated by the Logistic map [30]. Gong et al., introduced an algorithm, in which Chen hyperchaotic system is utilized to control the C-NOT operation [31], where the grey level information is encoded by quantum XOR operation. Later, Li et al., [32] designed a quantum colour image encryption based on multiple discrete chaotic systems where Logistic map, Asymmetric Tent map and Logistic Chebyshev map are used to generate control bits. Recently researchers have attempted to develop quantum key distribution in chaotic regime [33, 34].

1.3. Motivation and Objective of the Present Work. Most of the proposed classical encryption methods are flawed by limited keyspace, computational complexity and weak resistance to differential attacks. However, the proposed chaotic-quantum algorithms are computationally efficient and unconditionally secure [26–35]. But they fail to provide complete superposition of quantum states in encrypted domain. This paper introduces a speech encryption algorithm in the quantum scenario, where in classical bits are encoded in the nonorthogonal quantum states. Nonorthogonal quantum states are prepared by unitary rotations of the classical bits through secret rotation angles. Then, the encoded qubits are encrypted by controlled-NOT operation followed by Hadamard transform based on the key generated by the hyperchaotic system. Here quantum gates are controlled by the keystreams generated with the four dimensional hyperchaotic system proposed by Zhou and Yang [35] based on 3D Lü system. This proposed algorithm extends the security by encrypting quantum messages in both Standard and Hadamard basis. Both secret rotating angles and initial conditions of the hyperchaotic systems constitute the key, which enlarges the keyspace. The resulting algorithm ensures security against various differential and statistical attacks due to its enlarged keyspace.

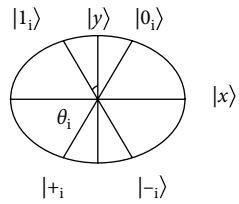

Figure 1: Nonorthogonal quantum pairs.

The rest of this paper is organized as follows: The preliminary study of the proposed speech encryption algorithm is presented in Section 2. Theoretical framework of the proposed approach is given in Section 3. Numerical simulations and performance evaluations are discussed in Section 4. Comparison of the proposed method with other state-of-art is discussed in Section 5, followed by conclusion in Section 6.

2. Preliminary Studies

2.1. Encoding Classical Bits in Nonorthogonal Quantum States. Speech samples are mapped into quantum data media as nonorthogonal quantum state which could be in Standard or Hadamard basis. Figure 1 shows the two pairs of nonorthogonal quantum states in Standard and Hadamard basis. Unlike orthogonal quantum states, nonorthogonal quantum states cannot be discriminated deterministically. Quantum data that encode the classical bits into nonorthogonal quantum states increases the robustness against PNS (photon number splitting) attacks.

Classical bits of the speech samples are encoded in the nonorthogonal quantum state by secret polarizing angle through unitary rotations. Classical binary bit to be encoded in quantum state is $m\{0, 1\}$. Sender encodes the classical bits by choosing nonorthogonal angle θ_i randomly between $[0\ 2\pi]$. The rotation operator $R(\theta_i)$ operates on classical bits m_i results the nonorthogonal quantum states $|m_i\rangle$. Tensor product generates the superposition states $|\psi_m\rangle$ corresponding to $|m_i\rangle$.

The rotation operator in matrix form is expressed by:

$$R(\theta_i) = \begin{bmatrix} \cos\theta_i & \sin\theta_i \\ -\sin\theta_i & \cos\theta_i \end{bmatrix}. \tag{1}$$

In order to retrieve the classical data, the receiver has to rotate the i^{th}quantum bit by the secret angle in the opposite direction. The rotation operator $R(\theta_i)$ is unitary since $R(\theta_i)R^{\dagger}(\theta_i)=\mathbb{I}$, where $R^{\dagger}(\theta_i)$is the adjoint of the matrix and $\mathbb{I}$ is the identity matrix.

$$R(\theta_i)R^{\dagger}(\theta_i) = \begin{bmatrix} \cos^2\theta_i + \sin^2\theta_i & 0 \\ 0 & \cos^2\theta_i + \sin^2\theta_i \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \tag{2}$$

Quantum states corresponding to each classical bit can be expressed as follows:

$$\begin{aligned} |m_1\rangle &= \cos\theta_0|0\rangle + \sin\theta_0|1\rangle, \\ |m_1\rangle &= \cos\theta_0|0\rangle + \sin\theta_0|1\rangle, \\ |m_1\rangle &= \cos\theta_0|0\rangle + \sin\theta_0|1\rangle, \\ |m_1\rangle &= \cos\theta_0|0\rangle + \sin\theta_0|1\rangle, \quad 1 \in [1, n], \end{aligned} \tag{3}$$

where $|m_i\rangle$ is the quantum state corresponding to classical bits m_i for the secret rotation angle θ_i. Tensor product between the quantum states refer to (3) generate the superposition states given as in (4):

$$|\psi_m\rangle = |m_1\rangle \otimes |m_2\rangle \ldots \otimes |m_i\rangle \ldots \otimes |m_n\rangle. \tag{4}$$

Here the n qubit quantum system $|\psi_m\rangle$, exist as the superposition of 2^n states with equal probability.

$$\begin{aligned} |\psi_m\rangle &= \frac{1}{2^n}\sum_{i=0}^{2^n-1} |\psi_{m_i}\rangle \quad i \in [0, 2^n - 1], \\ |\psi_m\rangle &= |0_1 0_2 \ldots 0_n\rangle + |0_1 0_2 \ldots 1_n\rangle \ldots + |\ldots + |1_1 1_2 \ldots 1_n\rangle|. \end{aligned} \tag{5}$$

Superposition states for a three qubit quantum system is described as follows:

$$\begin{aligned} |\psi_m\rangle = |0_1 0_2 0_3\rangle + 0_1 0_2 1_3\rangle + 0_1 1_2 0_3\rangle + |0_1 1_2 1_3\rangle + |1_1 0_2 0_3\rangle \\ + 1_1 0_2 1_3 + |1_1 1_2 0_3\rangle + |1_0 1_1 1_3\rangle. \end{aligned} \tag{6}$$

2.2. Quantum Gates. Quantum gates are the basic tool for quantum information processing. It can be represented as unitary matrix of size $2^n \times 2^n$, if the quantum logic gates acts on a n qubit quantum system. A suitable network of quantum gates can process quantum information much faster than the corresponding classical networks. In the proposed algorithm, quantum gates like Controlled-NOT (C-NOT) gates and Hadamard gates are used.

2.2.1. Controlled-NOT Gate. Controlled-NOT (C-NOT) is the classical counter part of XOR gate. It has two input bits, one control bit and one target bit. If the control bit is set to $|1\rangle$, the gate flips the target qubit. If the control bit is set to $|0\rangle$ target qubit remains same. Mathematical expression of the Controlled-NOT gate can be given as follows:

$$C_{x,y}|x\rangle|y\rangle \rightarrow |x\rangle|x \oplus y\rangle \text{ with } x, y \in \{0, 1\}. \tag{7}$$

CNOT $= \begin{bmatrix} \mathbb{I} & 0 \\ 0 & X \end{bmatrix}$ is the matrix form of CNOT gate, where $\mathbb{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ & $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.

2.2.2. Hadamard Gate. In Hadamard basis qubit can be represented as $\{|+\rangle, |-\rangle\}$, which gives the sense of complete superposition between ground state $|0\rangle$ and excited state $|1\rangle$.

$$\begin{aligned} |+\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \\ |-\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle). \end{aligned} \tag{8}$$

Hadamard gate operation on single qubit operation is given by:

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{\sqrt{2}}(X + Z), \tag{9}$$

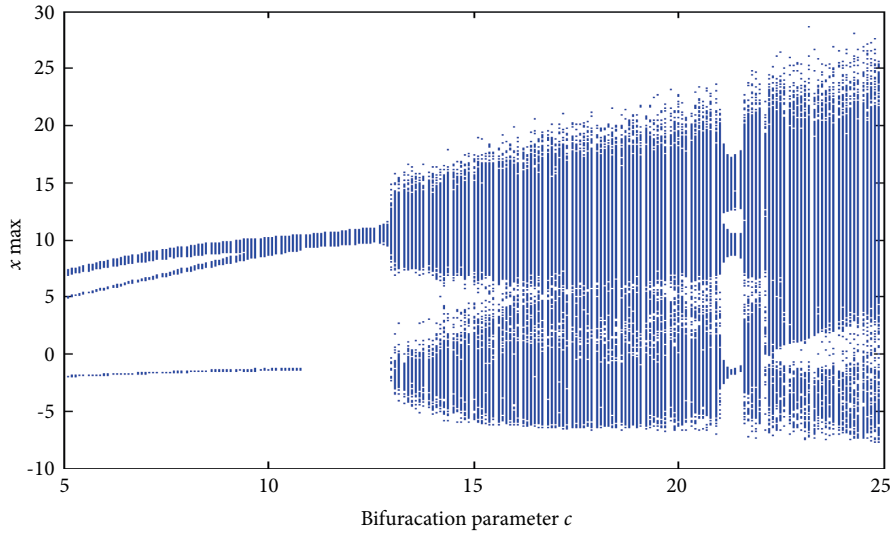

Figure 2: Bifurcation diagram of modified *Lù* system.

where

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{10}$$

General operation of Hadamard gate on target qubits, which is both in Standard and Hadamard basis are as follows:

$$H|0\rangle = |+\rangle;\ H|1\rangle = |-\rangle;\ H|+\rangle = |0\rangle;\ H|-\rangle = |1\rangle. \tag{11}$$

2.3. Hyperchaotic System. To improve keyspace and security, hyperchaotic systems are widely used in data encryption systems. In the proposed algorithm, keystream for the encryption process is generated from the 4-D hyperchaotic system discovered by Zhou and Yang by the fourth order Runge-Kutta method. The system is described as follows:

$$\begin{aligned} \dot{x} &= 36(y - x), \\ \dot{y} &= -xz + cy, \\ \dot{z} &= xy - 3z, \\ \dot{w} &= 18x - 0.5w. \end{aligned} \tag{12}$$

It has infinite number of real equilibrium. The system (12) shows multiple dynamic behaviour over a wide range of control parameter c. The evolution of chaotic dynamics such as periodic, quasi periodic and chaotic attractors in this system can be obtained by varying control parameter c [0, 25] by fixing all other parameters constant. When $c \in [13, 25]$ the system generates hyperchaotic attractor and this region is utilized for encryption purpose. The encryption process in higher dimensional space eliminates periodic window problems such as limited chaotic range and nonuniform distribution. Figure 2 illustrates the bifurcation diagram of modified *Lù* system.

3. Proposed Algorithm

3.1. Encryption Process. In this section we systematically demonstrate the various steps in encryption process. Figure 3 illustrates the proposed algorithm.

Step 1. Set the values for initial conditions and system parameter for the hyperchaotic system. Generate four different hyperchaotic sequences by iterating the hyperchaotic system by Runge-Kutta method for $l = 2^n$.

The generated sequences are $\{x_i\}, \{y_i\}, \{z_i\}$, and $\{w_i\} (1 \le i \le l)$.

Step 2. Convert the four hyperchaotic sequences into integer sequences $\{x_i^*\}, \{y_i^*\}, \{z_i^*\}$, and $\{w_i^*\}$ as follows:

$$\begin{aligned} x_i^* &= \left|\text{fix}(x_i - \text{fix}(x_i)) \times 10^{14}\right| \text{mod} 2^n, \\ y_i^* &= \left|\text{fix}(y_i - \text{fix}(y_i)) \times 10^{14}\right| \text{mod} 2^n, \\ z_i^* &= \left|\text{fix}(z_i - \text{fix}(z_i)) \times 10^{14}\right| \text{mod} 2^n, \\ w_i^* &= \left|\text{fix}(w_i - \text{fix}(w_i)) \times 10^{14}\right| \text{mod} 2^n. \end{aligned} \tag{13}$$

Step 3. Generate keystream k_1 & k_2 as control bits for C-NOT operation and Hadamard operation.

Control bits k_1 for CNOT operation is given by:

$$\begin{aligned} k_1 &= z_i^n, z_i^{n-1} \ldots z_i^0, \quad z_i^j \in \{0, 1\}, \\ i &= 0, 1, \ldots, 2^n - 1, \quad j = 0, 1, \ldots n. \end{aligned} \tag{14}$$

Control bits k_2 for Hadamard transform is given by:

$$\begin{aligned} k_2 &= w_i^n, w_i^{n-1} \ldots w_i^0, \quad w_i^j \in \{0, 1\}, \\ i &= 0, 1, \ldots, 2^n - 1, \quad j = 0, 1, \ldots n. \end{aligned} \tag{15}$$

Step 4. Controlled NOT gate perform bit flip operation on quantum speech sample $|\psi_m\rangle$ according to the control bits k_1.Where k_1 is realized from keystream $z_i^j\{0, 1\}$ generated with hyperchaotic sequence. Construct a C-NOT operator C_{k_1} as follows:

$$C_{K_1} = \begin{cases} I, \text{when} & z_i^j = 0, \\ X, & z_i^j = 1, \end{cases} \tag{16}$$

where X is the bit flip operator, that operates on the quantum state $|\psi_m\rangle$ according to the control bit z_i^j resulting into new state $|\psi_{m_1}\rangle$.

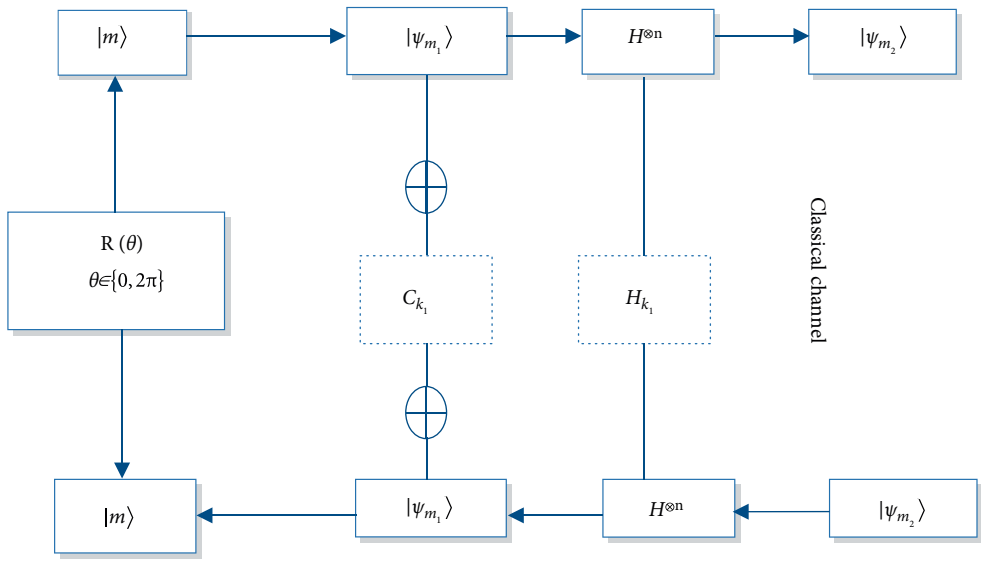

Figure 3: Block diagram of the proposed algorithm.

Table 1: Controlled-NOT operations.

$\lvert\psi_{m_i}\rangle$	C_{K_1}	$\lvert\psi_{m_{1i}}\rangle$
$\lvert\psi_{m_0}\rangle = \lvert 000\rangle$	$\lvert k_{10}\rangle = \lvert 100\rangle$	$\lvert\psi_{m_{10}}\rangle = \lvert 100\rangle$
$\lvert\psi_{m_1}\rangle = \lvert 001\rangle$	$\lvert k_{11}\rangle = \lvert 001\rangle$	$\lvert\psi_{m_{11}}\rangle = \lvert 000\rangle$
$\lvert\psi_{m_2}\rangle = \lvert 001\rangle$	$\lvert k_{12}\rangle = \lvert 110\rangle$	$\lvert\psi_{m_{12}}\rangle = \lvert 100\rangle$
$\lvert\psi_{m_3}\rangle = \lvert 011\rangle$	$\lvert k_{13}\rangle = \lvert 101\rangle$	$\lvert\psi_{m_{13}}\rangle = \lvert 110\rangle$
$\lvert\psi_{m_4}\rangle = \lvert 100\rangle$	$\lvert k_{14}\rangle = \lvert 111\rangle$	$\lvert\psi_{m_{14}}\rangle = \lvert 011\rangle$
$\lvert\psi_{m_5}\rangle = \lvert 101\rangle$	$\lvert k_{15}\rangle = \lvert 011\rangle$	$\lvert\psi_{m_{15}}\rangle = \lvert 110\rangle$
$\lvert\psi_{m_6}\rangle = \lvert 110\rangle$	$\lvert k_{16}\rangle = \lvert 010\rangle$	$\lvert\psi_{m_{16}}\rangle = \lvert 100\rangle$
$\lvert\psi_{m_7}\rangle = \lvert 111\rangle$	$\lvert k_{17}\rangle = \lvert 000\rangle$	$\lvert\psi_{m_{17}}\rangle = \lvert 111\rangle$
$\lvert\psi_{m_0}\rangle = \lvert 000\rangle$	$\lvert k_{10}\rangle = \lvert 100\rangle$	$\lvert\psi_{m_{10}}\rangle = \lvert 100\rangle$

Table 2: Hadamard Transformations.

$\lvert\psi_{m_{1i}}\rangle$	H_{K_2}	$\lvert\psi_{m_{2i}}\rangle$
$\lvert\psi_{m_{10}}\rangle = \lvert 100\rangle$	$\lvert k_{20}\rangle = \lvert 100\rangle$	$\lvert\psi_{m_{20}}\rangle = \lvert -00\rangle$
$\lvert\psi_{m_{11}}\rangle = \lvert 000\rangle$	$\lvert k_{21}\rangle = \lvert 001\rangle$	$\lvert\psi_{m_{21}}\rangle = \lvert 00+\rangle$
$\lvert\psi_{m_{12}}\rangle = \lvert 1000\rangle$	$\lvert k_{22}\rangle = \lvert 110\rangle$	$\lvert\psi_{m_{22}}\rangle = \lvert - + 0\rangle$
$\lvert\psi_{m_{13}}\rangle = \lvert 110\rangle$	$\lvert k_{23}\rangle = \lvert 101\rangle$	$\lvert\psi_{m_{23}}\rangle = \lvert -1+\rangle$
$\lvert\psi_{m_{14}}\rangle = \lvert 011\rangle$	$\lvert k_{24}\rangle = \lvert 111\rangle$	$\lvert\psi_{m_{24}}\rangle = \lvert + - -\rangle$
$\lvert\psi_{m_{15}}\rangle = \lvert 110\rangle$	$\lvert k_{25}\rangle = \lvert 011\rangle$	$\lvert\psi_{m_{25}}\rangle = \lvert 1 - +\rangle$
$\lvert\psi_{m_{16}}\rangle = \lvert 100\rangle$	$\lvert k_{26}\rangle = \lvert 010\rangle$	$\lvert\psi_{m_{26}}\rangle = \lvert 1 + 0\rangle$
$\lvert\psi_{m_{17}}\rangle = \lvert 111\rangle$	$\lvert k_{27}\rangle = \lvert 000\rangle$	$\lvert\psi_{m_{27}}\rangle = \lvert 111\rangle$
$\lvert\psi_{m_{10}}\rangle = \lvert 100\rangle$	$\lvert k_{20}\rangle = \lvert 100\rangle$	$\lvert\psi_{m_{20}}\rangle = \lvert -00\rangle$

$$
\begin{aligned}
\left|\psi_{m_i}\right\rangle &= \frac{1}{2^n}\sum_{i=0}^{2^n-1}\otimes_{j=0}^{j=n}\left|\psi_{m_i}\otimes C_{k_1}\right\rangle,\\
C_{k_1} &= z_i^n, z_i^{n-1}\ldots z_i^0,\ z_i^j \in \{0,1\},\\
\left|\psi_{m_1}\right\rangle &= \frac{1}{2^n}\sum_{i=0}^{2^n-1}\otimes_{j=0}^{j=n}\left|\psi_{m_i}\otimes z_i^j\right\rangle,\\
\left|\psi_{m_1}\right\rangle &= z_i^n, z_i^{n-1}\ldots z_i^0, z_i^j\otimes_{j=0}^{n}\frac{1}{2^n}\sum_{i=0}^{2^n-1}\left|\psi_{m_i}\right\rangle.
\end{aligned}
\tag{17}
$$

Table 1, describe the whole possible quantum states for three qubit system and its C-NOT transformations.

Step 5. Hadamard gate operates on $\left|\psi_{m_1}\right\rangle$ after the bit flip operation performed by Controlled-NOT gate. In this operation k_2 is the control bit and it is realized from keystream $w_i^j\{0,1\}$ generated with the hyperchaotic system. Hadamard gate operates on the target qubit only when the control qubit is $|1\rangle$ or else the target qubit remains the same.

Controlled Hadamard gate operator H_{K_2} is given by:

$$
H_{K_2} = \begin{cases} I, \text{when} & w_i^j = 0,\\ H, & w_i^j = 1. \end{cases}
\tag{18}
$$

Hadamard gate for the n qubit operation

$$
H^{\otimes n} = \frac{1}{\sqrt{2^n}}\sum_{i,j\{0,1\}}(-1)^{ij}.
\tag{19}
$$

Apply Hadamard gate $\left|\psi_{m_i}\right\rangle$ under the control of key element k_2

$$
\left|\psi_{m_2}\right\rangle = \underbrace{\frac{1}{2^n}\sum_{i=0}^{2^n-1}\mathbb{I}\otimes\left|\psi_{m_{1i}}\right\rangle}_{w_i^j=0} + \underbrace{\frac{1}{2^n}\sum_{i=0}^{2^n-1}\rho_{m_{1i}}}_{w_i^j=1}\otimes H^{\otimes n},
\tag{20}
$$

where $\rho_{m_{1i}}$ is the density matrix for the quantum state $\left|\psi_{m_{1i}}\right\rangle$, $\rho_{m_{1i}} = \left|\psi_{m_{1i}}\right\rangle\left\langle\psi_{m_{1i}}\right|$. Hadamard transformation for three qubit system is given in Table 2.

Table 3: Complete operation of four qubit quantum system.

$\lvert\psi_{m_i}\rangle$	C_{K_1}	$\lvert\psi_{m_{1i}}\rangle$	H_{K_2}	$\lvert\psi_{m_{2i}}\rangle$
$\lvert\psi_{m_0}\rangle = \lvert 0000\rangle$	$\lvert k_1\rangle = \lvert 0011\rangle$	$\lvert\psi_{m_{10}}\rangle = \lvert 0011\rangle$	$\lvert k_2\rangle = \lvert 1010\rangle$	$\lvert\psi_{m_{20}}\rangle = \lvert -0+1\rangle$
$\lvert\psi_{m_1}\rangle = \lvert 0001\rangle$		$\lvert\psi_{m_{11}}\rangle = \lvert 0010\rangle$		$\lvert\psi_{m_{21}}\rangle = \lvert -0+0\rangle$
$\lvert\psi_{m_2}\rangle = \lvert 0010\rangle$		$\lvert\psi_{m_{12}}\rangle = \lvert 0001\rangle$		$\lvert\psi_{m_{22}}\rangle = \lvert -0-1\rangle$
$\lvert\psi_{m_3}\rangle = \lvert 0011\rangle$		$\lvert\psi_{m_{13}}\rangle = \lvert 0000\rangle$		$\lvert\psi_{m_{23}}\rangle = \lvert -0-0\rangle$
$\lvert\psi_{m_4}\rangle = \lvert 0100\rangle$		$\lvert\psi_{m_{14}}\rangle = \lvert 0111\rangle$		$\lvert\psi_{m_{24}}\rangle = \lvert -1+1\rangle$
$\lvert\psi_{m_5}\rangle = \lvert 0101\rangle$		$\lvert\psi_{m_{15}}\rangle = \lvert 0110\rangle$		$\lvert\psi_{m_{25}}\rangle = \lvert -1+0\rangle$
$\lvert\psi_{m_6}\rangle = \lvert 0110\rangle$		$\lvert\psi_{m_{16}}\rangle = \lvert 0101\rangle$		$\lvert\psi_{m_{26}}\rangle = \lvert -1-1\rangle$
$\lvert\psi_{m_7}\rangle = \lvert 0111\rangle$		$\lvert\psi_{m_{17}}\rangle = \lvert 0100\rangle$		$\lvert\psi_{m_{27}}\rangle = \lvert -1-0\rangle$
$\lvert\psi_{m_8}\rangle = \lvert 1000\rangle$		$\lvert\psi_{m_{18}}\rangle = \lvert 1011\rangle$		$\lvert\psi_{m_{28}}\rangle = \lvert +0+1\rangle$
$\lvert\psi_{m_9}\rangle = \lvert 1001\rangle$		$\lvert\psi_{m_{19}}\rangle = \lvert 1010\rangle$		$\lvert\psi_{m_{29}}\rangle = \lvert +0+0\rangle$
$\lvert\psi_{m_{10}}\rangle = \lvert 1010\rangle$		$\lvert\psi_{m_{110}}\rangle = \lvert 1001\rangle$		$\lvert\psi_{m_{210}}\rangle = \lvert +0-1\rangle$
$\lvert\psi_{m_{11}}\rangle = \lvert 1011\rangle$		$\lvert\psi_{m_{111}}\rangle = \lvert 1000\rangle$		$\lvert\psi_{m_{211}}\rangle = \lvert +0-0\rangle$
$\lvert\psi_{m_{12}}\rangle = \lvert 1100\rangle$		$\lvert\psi_{m_{112}}\rangle = \lvert 1111\rangle$		$\lvert\psi_{m_{212}}\rangle = \lvert +1+1\rangle$
$\lvert\psi_{m_{13}}\rangle = \lvert 1101\rangle$		$\lvert\psi_{m_{13}}\rangle = \lvert 1110\rangle$		$\lvert\psi_{m_{213}}\rangle = \lvert +1+0\rangle$
$\lvert\psi_{m_{14}}\rangle = \lvert 1110\rangle$		$\lvert\psi_{m_{14}}\rangle = \lvert 1101\rangle$		$\lvert\psi_{m_{214}}\rangle = \lvert +1-1\rangle$
$\lvert\psi_{m_{15}}\rangle = \lvert 1111\rangle$		$\lvert\psi_{m_{15}}\rangle = \lvert 1100\rangle$		$\lvert\psi_{m_{215}}\rangle = \lvert +1-0\rangle$

Detailed encryption process for a four qubit quantum system with fixed $\lvert k_1\rangle = \lvert 0011\rangle$ and $\lvert k_2\rangle = \lvert 1010\rangle$ is given in Table 3.

3.2. Decryption Process. The procedure of decryption process is reverse of the encryption process. Since rotation operator $R(\theta)$, C-NOT gate and H-gate are unitary operators, decryption can be done easily by means of the pre-shared keys. The decryption process is described as follows:

Step 1. Generate the same keystream or control bits k_1 and k_2 according to the steps 1–3 in encryption process.

Step 2. Perform Hadamard operation on $\lvert\psi_{m_2}\rangle$.

$\lvert\psi_{m_1}\rangle = H^{\otimes n}\lvert\psi_{m_2}\rangle$; Since $H^2 = \mathbb{I}$

Step 3. Perform Controlled –NOT operation on $\lvert\psi_{m_2}\rangle$

$$\lvert\psi_m\rangle = \frac{1}{2^n}\sum_{i=0}^{2^n-1}\otimes_{j=0}^{j=n}\lvert\psi_{m_{1i}}\otimes C_{k_1}\rangle. \tag{21}$$

Step 4. Do the inverse rotation operation on $\lvert\psi_m\rangle$ to retrieve the classical data.

4. Numerical Simulation and Results

The proposed algorithm is realized by classical counterpart of circuit elements equivalent to quantum circuit. The proposed algorithm is simulated on a classical computer with MATLAB R2013a (version) software. Eight voice samples of male and female speech signal with sampling rate of 8000 samples/sec are selected for the test. The initial conditions are set as $x0 = 0.423$, $y0 = -0.531$, $z0 = 0.256$, $w0 = 1$. Time step for the fourth order Runge-Kutta method is taken as 0.005.

Table 4: Encrypted signal numerical analysis.

Sample files	*SNR*	Correlation	PRD(Ø)
A. Male voice	−12.45 dB	0.00669	0.521×10^5
B. Female voice	−13.89 dB	0.00918	0.689×10^6
C. Male voice	−21.89 dB	0.00693	0.723×10^5
D. Female voice	−14.32 dB	0.00229	0.214×10^5
E. Male voice	−22.89 dB	0.00527	0.934×10^5
F. Female voice	−19.45 dB	0.00358	0.394×10^6
G. Male voice	−11.76 dB	0.00992	0.861×10^5
H. Female voice	−23.23 dB	0.00136	0.231×10^6

4.1. Correlation Analysis. Correlation analysis is a statistical metric to evaluate the performance of cryptographic algorithm over various statistical attacks. Correlation coefficient analysis measures the mutual relationship between similar segments in the plain audio file and the encrypted audio file. A secure data encryption algorithm converts original data into random-like noisy signal with low correlation coefficient [36]. Low correlation coefficient indicates the narrow correlation between original and encrypted speech files. Correlation

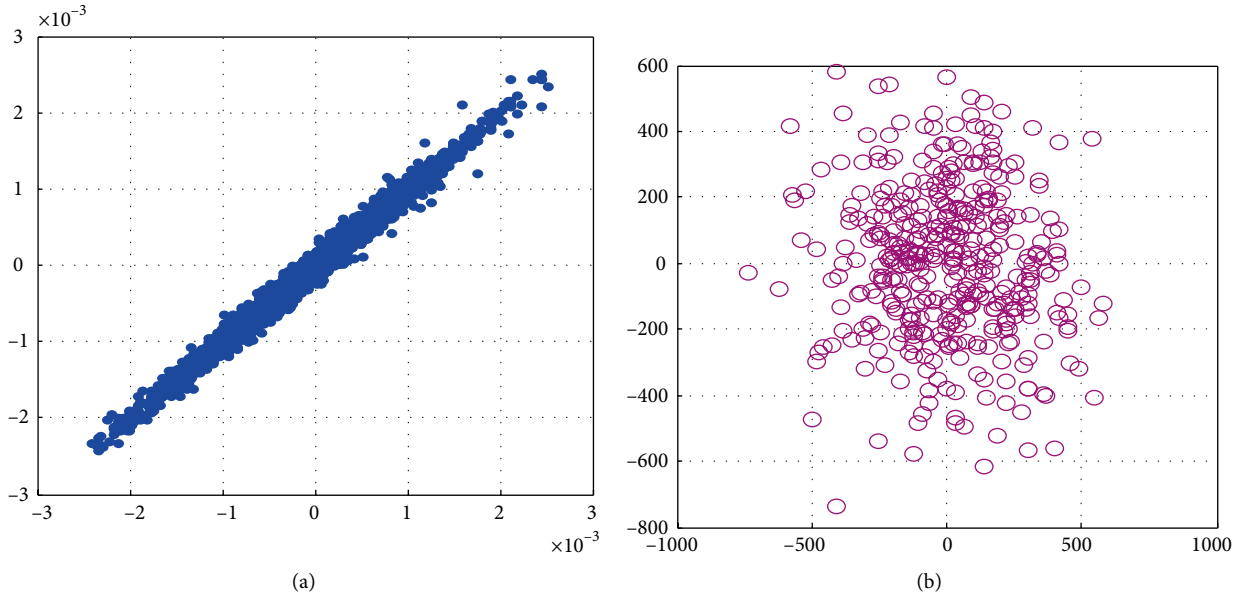

FIGURE 4: Scatter plot diagram of (a) original speech signal (b) encrypted speech signal.

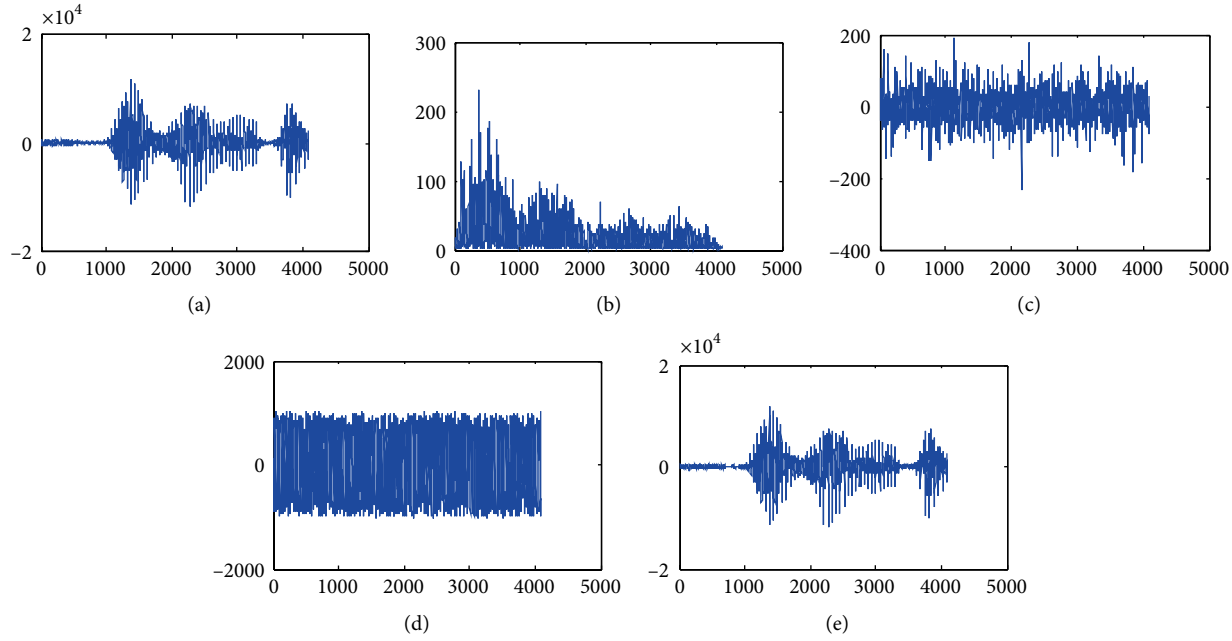

FIGURE 5: (a) Original signal. (b) Compressed signal. (c) Data samples after permutations. (d) Data samples after substitution. (e) Decrypted signal.

coefficient is evaluated based on the equation (22) and it is tabulated in Table 4.

$$r_{xy} = \frac{cov(x,y)}{\sigma_x \sigma_y},$$

$$r_{xy} = \frac{(1/N_S)\sum_{i=1}^{N_s}(x_i - E(x))(y_i - E(y))}{\sqrt{(1/N_S)\sum_{i=1}^{N_s}(x_i - E(x))^2}\sqrt{(i/N_S)\sum_{i=1}^{N_s}(y_i - E(y))^2}}, \sigma_x,$$

$$\sigma_y \neq 0, \tag{22}$$

where $E(x)$ and $E(y)$ are mean and σ_x, σ_y are the standard deviation of the encrypted and decrypted speech signal. Scatter plot diagram is plotted for original and encrypted version, which is shown in Figures 4(a) and 4(b) respectively. It clearly shows that the encrypted version is scattered or randomized.

4.2. Signal to Noise Ratio (SNR). Signal to noise ratio is one of the straight forward methods to validate the performance of data encryption algorithm. SNR measures the noise content in the encrypted data signal. Cryptanalyst always try to increase the noise content in the encrypted signal so as to minimize the information content in the encrypted data [37]. Figure 5 displays the original and encrypted speech signal. It is clear

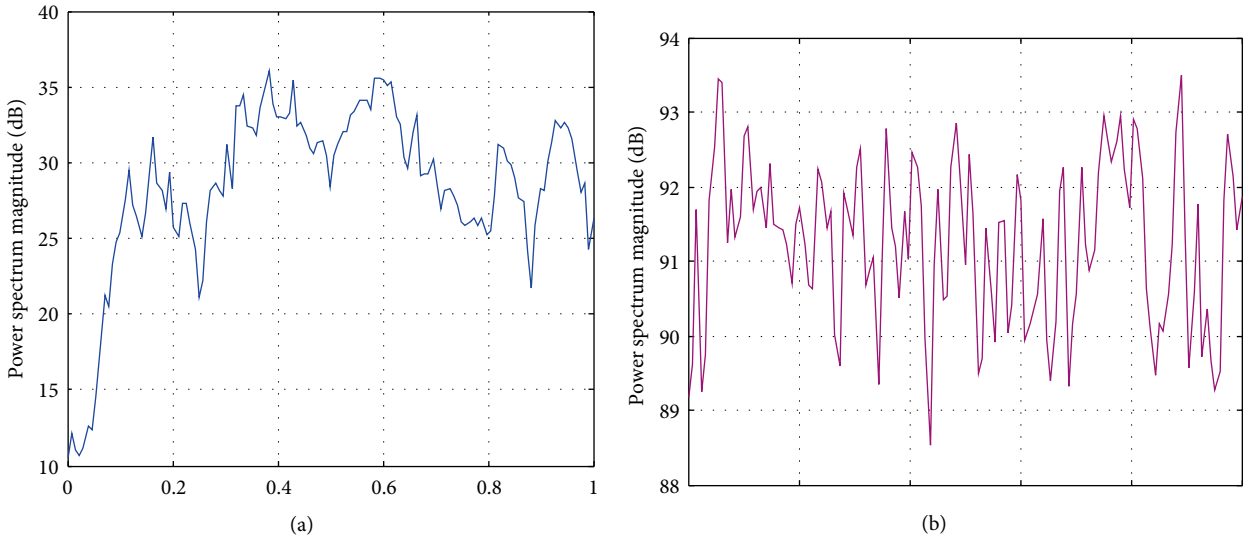

FIGURE 6: Power spectral density of (a) Original speech signal. (b) Encrypted speech signal.

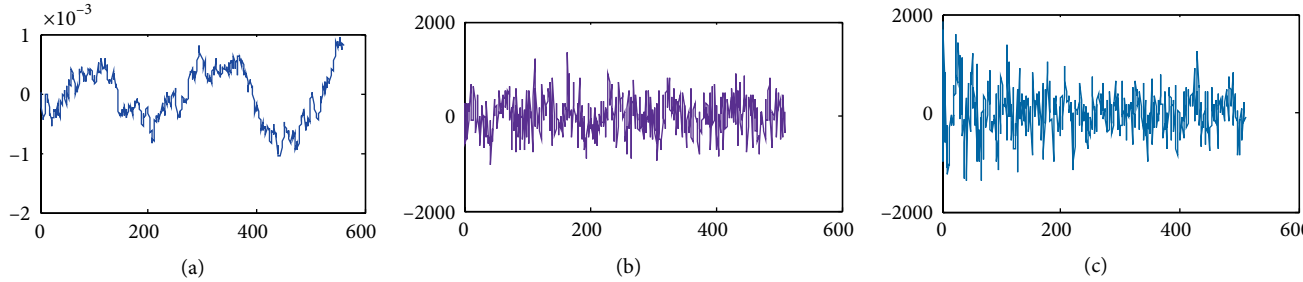

FIGURE 7: Key sensitivity on encryption process (a) original speech signal (b) encrypted speech signal for key $x_0 = 0.413$, $y_0 = -0.931$, $z_0 = 0.465$, $w_0 = 0$ (c) encrypted speech signal for $x_0 = 0.913$, $y_0 = -0.131$, $z_0 = 0$, $w_0 = 0.825$.

that encrypted speech signal contains more noise content that in original speech signal. The SNR values of encrypted audio files are calculated based on the following equation (23) and it is given in Table 4.

$$SNR = 10 * \log 10 \frac{\sum_{i=1}^{N_s} x_i^2}{\sum_{i=1}^{N_s} (x_i - y_i)^2}. \tag{23}$$

4.3. Percent Residual Deviation (PRD). Percentage Residual Deviation is another statistical tool to measure the variation of the encrypted speech signal from original signal. PRD can be calculated for the given plain audio signal x_i and encrypted signal y_i as follows:

$$\emptyset = 100 \times \sqrt{\frac{\sum_{i=1}^{n} (x_i - y_i)^2}{\sum_{i=1}^{n} x_i^2}}. \tag{24}$$

The calculated values of the percent residual deviation for various original and encrypted speech signals are given in Table 4. It can be seen that the encrypted signal is highly deviated from its original signal.

4.4. Spectral Entropy. Spectral entropy measures the randomness in both encrypted and original speech signal. Its measurement is based on the assumption that the spectrum of meaningful speech segment is correlated than the noisy signal. The spectral measurement compares the entropy where the amplitude component of the power spectrum is taken as a probability parameter in entropy calculation. The amount of information can be calculated as the negative of entropy or the negative logarithm of probability. Thus, meaningful speech segments shows low entropy since it contains organized data samples. However the encrypted speech signals have high entropy and large spectral peaks similar to noisy signal. The entropy E_i can be measured as follows:

$$E_i = \sum_n PSD_n(f_i) \log\left(PSD_n(f_i)\right); i = 1, 2, 3 \ldots \ldots, n, \tag{25}$$

where PSD_n is the normalized power spectrum and f_i is the frequency of the signal. Irregularities of amplitude in original and encrypted signals are shown in Figure 6.

4.5. Keyspace and Key Sensitivity Analysis. The secret rotation angles θ_i and initial conditions and system parameter (x_0, y_0, z_0, w_0, c) of the hyperchaotic system determine the keyspace. In the recommended algorithm, floating point accuracy of $10^{-16}$is used for the key components. Therefore the keyspace achieved in this scheme is $\theta_i \times \left(10^{-16}\right)^5 = \theta_i \times 2^{224}$

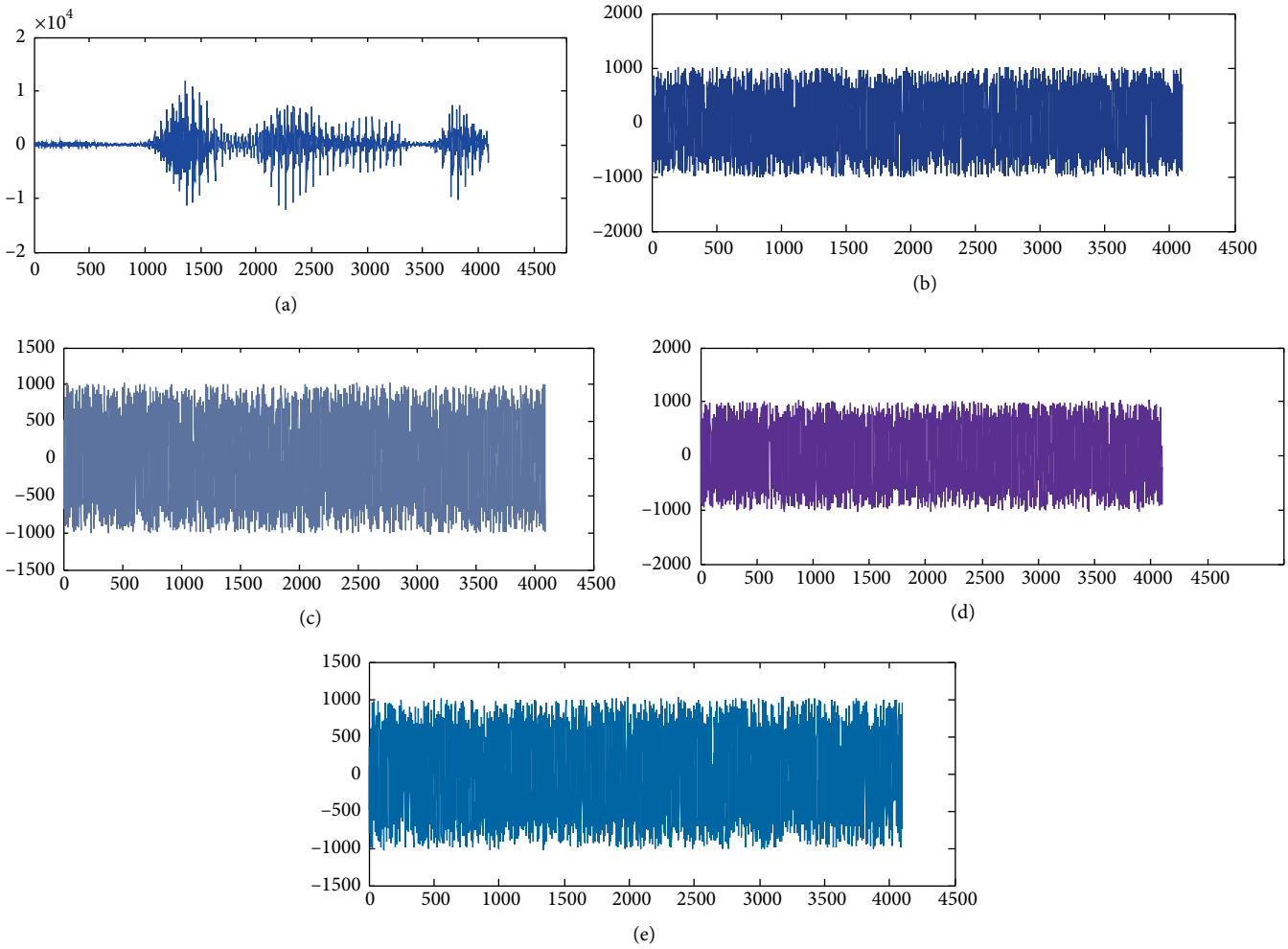

FIGURE 8: Key sensitivity on decryption process (a) decrypted signal with correct key, decrypted signal with incorrect key (b) $x_0 + 10^{-15}$ (c) $y_0 + 10^{-15}$ (d) $z_0 + 10^{-15}$ (e) $w_0 + 10^{-15}$.

TABLE 5: Quality metrics comparison of encryption scheme with other methods.

Method	Key length	keyspace	r_{xy}	NPCR	UACI
AES	128,192,256	$2^{128}, 2^{192}, 2^{256}$	0.009700	99.60327	33.4218
Ref [22]	>264	$>2^{624}$	0.00022	99.6399	33.8085
Ref [23]	744	2^{744}	0.00121	99.6317	33.6781
Ref [26]	$>2^{107}$	2^{107}	0.00321	99.6317	33.6782
[pro:meth]	$>2^{212}$	$> 2^{2^{212}}$	0.000136	99.6320	33.6823

in classical computation. But in the quantum domain the keyspace exist as the superposition of $2^{2^{224}}$ quantum states, which is large enough to break various cryptographic attacks.

Key sensitivity is the essential quality for any good data encryption algorithm, which make sure that the security level of the algorithm against the brute-force attack. It means that a small variation for any key parameters bring an apparent change in both encrypted and decrypted speech signal. The effect of variation in keyparameter on encryption process is verified by encrypting the signal with slightly different initial conditions. The simulation result shows that the slight variation in keyparameter will result completely different encrypted signal. Figure 7 shows the encrypted signals with two different initial conditions. To evaluate the key sensitivity of decrypted signal, encrypt the speech file with one fixed secret key then decryption is performed with slightly different keys. The resulting speech files decrypted with wrong keys apparently looks different and reveals no information.

Figure 8(a) shows the decrypted speech signal with correct key. Figures 8(b)–8(e) show the decrypted signal with slight variations in the initial conditions.

4.6. UACI and NSCR Analysis. In data encryption process, resistace to differential attacks is generally analyzed through NSCR (number of samples change rate) and UACI (unified average changing intensity) tests. In this analyysis two different speech segments are encrypted with same keystreams,where the original speech segments are differed by one sample space [38]. Then the encrypted speeech segments are compared by the number of sample change rate (NSCR) and the unified average changing intensity (UACI). Both these prameters can be expressed as follows:

$$\begin{aligned} \text{NSCR} &= \sum_i \frac{D_i}{N} \times 100\% \; i = 1, 2 \ldots . N, \\ \text{UACI} &= \frac{1}{N}\left[\frac{\sum_i x_i - x_i'}{65535}\right], \end{aligned} \tag{26}$$

where

$$d_i = \begin{cases} 1, & x_i \neq x_i', \\ 0, & \text{otherwise}, \end{cases} \tag{27}$$

c_i and c_i' denotes the the audio samles at i^{th} position of the encrypted speech samples and N corresponds to the length of the speech segments.The upper-bound for NSCR and UACI are 100% and 33.3% respectively. For a secure encryption scheme these parameters should be close to the upper bound ideal values.

4.7. Computational Complexity. In quantum computation, computational complexity is evaluated by the number of quantum gates employed in encryption process. In the proposed algorithm fundamental quantum gates such as C-NOT gate and Hadamard gates are utilized. Since the computational complexity of the quantum computation is parallel, complexity of the entire encryption process could be obtained by the quantum sub-operations like C_{k_1}(C-NOT operator) and H_{K_2}(Hadamard operator). Assume that the input speech samples are encoded in quantum domain and each sample spaces are in a superposition of $2^n \times 1$ quantum states. In Controlled-NOT operation, $(1/2^n)\sum_{i=0}^{2^n-1} \otimes_{j=0}^{j=n} \left|\psi_{m_i} \otimes C_{k_1}\right\rangle$ each qubit is acted upon by C_{k_1} when z_i^j=1. Quantum XOR operator or bit flip operator C_{k_1} is realized by n-CNOT gate. In these operations each n-CNOT gate can be realized by $4n - 8$ Toffoli gates and each Toffoli gate is equivalent to six Control-not gates. Therefore total elementary gates involved in quantum XOR operation is $24n - 48$. Thus, the computational complexity of the first phase of encryption with C-NOT operator is $O(n)$. The Hadamard gate operation on n qubit system is $H^n = \left(1/\sqrt{2^n}\right)\sum_{i,j\{0,1\}}(-1)^{ij}$. The Hadamard gate can be realized by $XZ^{1/2}$. Pauli X and Pauli Z gates can be decomposed to single Toffoli gate with appropriate control signal. Therefore the basic elementary operation involved in Hadamard gate is $6n + 6n$. In the second phase of encryption process the computational complexity of Hadamard operator H_{K_2} can be approximated to $O(n)$. Since both the operations scales linearly with input n, the computational complexity of entire process is $O(n)$. Comparing with classical speech encryption algorithm, the classical XOR operation could be realized with 2^{2n} XOR operations. Therefore the computational complexity of classical encryption algorithm corresponding to its quantum version is $O(2^n)$.

5. Comparison with Existing Works

The proposed algorithm is compared with existing algorithms in both quantum and classical domain. Various quality metrices such as key length, keyspace NPCR, UACI and correlation coefficient between original and encrypted signals are analysed and tabulated in Table 5.

The size of the proposed method's key space is greater than 2^{224} (Section 4.5). It is clear from the simulation results (Figure 4) that the encrypted speech signal contains more noise content that in the original speech signal. Correlation coefficient (CC) evaluated is almost zero (Table 4) for the proposed algorithm. A standard Encryption Algorithm (AES), a fast colour image encryption algorithm based by hyperchaotic system [22], an algorithm based on hyperchaotic system and S boxes in the form of permutation–substitution network [23], and a colour image encryption based on quantum chaotic system [26] are taken for comparison.

6. Conclusion

In this paper, a new classical data encryption algorithm in quantum domain is proposed. The basic idea behind the security of the proposed algorithm lies in protecting the classical information in the form of nonorthogonal quantum states. Furthermore the Controlled NOT operation and Hadamard operation in quantum domain extends the security of the proposed algorithm. The introduction of modified hyperchaotic *Lù*-system into quantum speech encryption algorithm increases the number of keys and improved the key sensitivity. Various simulations and numerical analysis have been carried on classical computer to evaluate the performance of the algorithm. The simulation results demonstrated that the proposed approach is an excellent choice for classical data encryption in quantum domain.

Data Availability

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

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

[1] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *Journal of Cryptology*, vol. 5, no. 1, pp. 3–28, 1992.

[2] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 1, pp. 802–803, 1982.

[3] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," vol. 175, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, pp. 175–179, IEEE, Bangalore, 1984.

[4] R. P. Feynman, "Simulating physics with computers," *International Journal of Theoretical Physics*, vol. 21, no. 6/7, pp. 467–488, 1982.

[5] G. Beach, C. Lomont, and C. Cohen, "Quantum image processing (quip)," in *IEEE 32nd Applied Imagery Pattern Recognition Workshop Proceedings*, pp. 39–44, IEEE, Washington, DC, USA, 2003.

[6] M. A. Nielson and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, 2000.

[7] V. Vlatko, B. Adriano, and E. Artur, "Quantum network for elementary arithmetic operation," *Physical Review A*, vol. 54, no. 1, pp. 147–153, 1996.

[8] A. Klappenecker and M. Roetteler, "Discrete cosine transforms on quantum computers," in *IEEER8-EURASIP Symposium on Image and Signal Processing and Analysis (ISPA 01)*, pp. 464–468, IEEE, Pula, Croatia, 2001.

[9] C. Tseng and T. Hwang, "Quantum circuit design of 8×8 discrete cosine transforms using its fast computation flow graph," in *IEEE International Symposium on Circuits and Systems*, pp. 828–831, IEEE, Kobe, Japan, 2005.

[10] A. Fijany and C. P. Williams, "Quantum wavelet transform: fast algorithm and complete circuits," in *Proceedings of International Conference on Quantum Computing Quantum Communications*, ACM, pp. 10–33, London, 1997.

[11] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *International Journal of Chaos and Bifurcation*, vol. 16, no. 08, pp. 2129–2151, 2006.

[12] O. S. Faragallah, "An enhanced chaotic key-based RC5 block cipher adapted to image encryption," *International Journal of Electronics*, vol. 99, no. 7, pp. 925–943, 2011.

[13] Z. Liu, T. Xia, and J. Wang, "image encryption technology based on fractional two-dimensional triangle function combination discrete chaotic map coupled with menezes-vanstone elliptic curve cryptosystem," *Discrete Dynamics in Nature and Society*, vol. 2018, Article ID 4585083, 24 pages, 2018.

[14] M. Amin and A.A. Abd El-Latif, "Efficient modified RC5 based on chaos adapted to image encryption," *Journal of Electronic Imaging*, vol. 19, no. 1, p. 013012, 2010.

[15] T. Gopalakrihnan and S. Ramakrishnan, "Chaotic image encryption with hash keying as key generator," *IETE Journal of Research*, vol. 63, no. 2, pp. 172–187, 2016.

[16] F. J. Farsana and K. Gopakumar, "A novel approach for speech encryption: Zaslavsky map as pseudo random number generator," vol. 93, in *Proceedings of International Conference on Advances in Computing and Communications (ICACC)*, pp. 816–823, 2016.

[17] S. J. Sheela, K. V. Suresh, and D. Tandur, "A novel audio cryptosystem using chaotic maps and DNA encoding," *Journal of Computer Networks and Communications*, vol. 2017, Article ID 2721910, 12 pages, 2017.

[18] M. Khan, T. Shah, H. Mahmood, M. A. Gondal, and I. Hussain, "A novel technique for the construction of strong S-boxes based on chaotic Lorenz systems," *Nonlinear Dynamics*, vol. 70, no. 3, pp. 2303–2311, 2012.

[19] M. Khan and Z. Asghar, "A novel construction of substitution box for image encryption applications with Gingerbreadman chaotic map and S8 permutation," *Neural Computing and Applications*, vol. 29, no. 4, pp. 993–999, 2018.

[20] X. Wang, Ü. Çavuşoğlu, S. Kacar et al., "S-box based image encryption application using a chaotic system without equilibrium," *Applied Sciences*, vol. 9, no. 4, p. 781, 2019.

[21] H. Zhu, C. Zhao, and X. Zhang, "A novel image encryption–compression scheme using hyper-chaos and Chinese remainder theorem," *Signal Processing: Image Communication*, vol. 28, no. 6, pp. 670–680, 2013.

[22] B. Norouz and S. Mirzakuchaki, "A fast color image encryption algorithm based on hyper-chaotic system," *Nonlinear Dynamics*, vol. 78, no. 2, pp. 995–1015, 2014.

[23] Y. Liu, X. Tong, and J. Ma, "Image encryption algorithm based on hyperchaotic system and dynamic S-box," *Multimed Tools and Applications*, vol. 75, no. 12, pp. 7739–7759, 2016.

[24] L. J. Sheu, "A speech encryption using fractional chaotic systems," *Nonlinear Dynamics*, vol. 63, no. 6/7, pp. 103–108, 2011.

[25] G. Vidal, M. S. Baptista, and H. Mancini, "Fundamentals of a classical chaos-based cryptosystem with some quantum cryptography features," *International Journal of Bifurcation and Chaos*, vol. 22, no. 10, p. 1250243, 2012.

[26] A. A. Abd El-Latif, L. Li, N. Wang, Q. Han, and X. Niu, "A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces," *Signal Processing*, vol. 93, no. 11, pp. 2986–3000, 2013.

[27] N. Jiang, W. Y. Wu, and L. Wang, "The quantum realization of Arnold and Fibonacci image scrambling," *Quantum Information Processing*, vol. 13, no. 5, pp. 1223–1236, 2014.

[28] N. R. Zhou, T. X. Hua, L. H. Gong, D. J. Pei, and Q. H. Liao, "Quantum image encryption based on generalized Arnold transform and double random- phase encoding," *Quantum Information Processing*, vol. 14, no. 4, pp. 1193–1213, 2015.

[29] A. Akhshani, A. Akhavan, and S. C. Lim, "An image encryption scheme based on quantum logistic map," *Communication in Nonlinear Science and Numerical simulations*, vol. 17, pp. 4653–4661, 2012.

[30] H. R. Liang, X. Y. Tao, and N. R. Zhou, "Quantum image encryption based on generalized affine transform and logistic map," *Quantum Information Processing*, vol. 15, no. 7, pp. 2701–2724, 2016.

[31] L. H. Gong, X. H. He, S. Cheng, T. X. Hua, and N. R. Zhou, "Quantum image encryption algorithm based on quantum image XOR operations," *International Journal of Theoretical Physics*, vol. 55, no. 7, pp. 3234–3250, 2016.

[32] L. Li, B. Abd-El-Atty, A.A. Abd El-Latif, and A. Ghoneim, "Quantum color image encryption based on multiple discrete chaotic systems," in *Proceedings of the Federated Conference on Computer Science and Information Systems*, pp. 555–529, IEEE, Prague, Czech Republic, 2017.

[33] M. H. Al Hasani and K. A. Al Naimee, "Impact security enhancement in chaotic quantum cryptography," *Optics & Laser Technology*, vol. 119, p. 105575, 2019.

[34] G. l de Oliveira and R. v Ramos, "Quantum-chaotic cryptography," *Quantum Information Processing*, vol. 17, no. 3, 2018.

[35] P. Zhou and F. Yang, "Hyperchaos, chaos and horseshoe in a 4D nonlinear system with an infinite number of equilibrium points," *Nonlinear Dynamics*, vol. 76, no. 1, pp. 473–480, 2014.

[36] R. Taylor, "Interpretation of the correlation coefficient: a basic review," *Journal of Diagnostic Medical Sonography*, vol. 6, no. 1, pp. 35–39, 1990.

[37] B. T. Bosworth, W. R. Bernecky, J. D. Nickila, B. Adal, and G. D. Carter, "Estimating signal-to-noise ratio (SNR)," *IEEE Journal of Oceanic Engineering*, vol. 33, no. 4, pp. 414–418, 2008.

[38] Y. Wu, J.P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," *Cyber Journals: Multidisciplinary Journals in Science and Technology Journal of Selected Areas in Telecommunications (JSAT)*, vol. 1, no. 2, pp. 31–38, 2011.