Speech Scrambler Based on Discrete Cosine Transform and Novel Seven-Dimension Hyper Chaotic System

Hayder Kadhim Zghair1, Sadiq A. Mehdi2, Sattar B. Sadkhan3
1 Department of Software Information Technology College, University of Babylon, Iraq
2 Department of Computer Science College of Education, Mustansiriyah University, Iraq
3 Department of Information networks Information Technology College University of Babylon, Iraq
hyderkadum8@gmail.com
sadiqmehdi71@uomustansiriyah.edu.iq
drengsattar@ieee.org

Abstract. Because of their inherent features related to cryptography, the hyperchaotic system has strong potential in security systems. In this paper, a new cryptography scheme for speech scrambling has been proposed which gives it more security level. Also, it introduced a novel seven dimensions (7D) nonlinear hyperchaotic system in third-order which has twelve positive parameters. A chaotic behavior for the proposed novel system is analyzed. The hyperchaotic system is demonstrated that beside it appropriates for speech scrambler. PRNG (Pseudo Random Number Generated) is created based on the proposed 7D hyperchaotic result. The proposed scheme depends on this novel hyperchaotic system as PRNG to generate a random keystream bit. The input speech signal in this work is first squeezed by discrete cosine transformation (DCT) to minimize the residual intelligibility (R.I.). Increasing the number of system parameters accomplished a high key space, therefore, improves the security to resist several cryptographic attacks. The scheme is measured using various tests like. Peak Signal-to-Noise Ratio (PSNR), Signal to noise ratio (SNR), percentage of Difference (P. Diff.), Segmental Signal to Noise Ratio Measure (SSNR), Crest factor measure (CF), Correlation coefficient Measure (R_C), root mean square measure (RMS), histogram, key sensitivity, spectrogram, and waveform. The results of simulation and comparison prove that the algorithm can achieve better performance in encryption that means the scheme is stronger and highly secure against various types of attacks than many recent similar audio encryption schemes. Simulated and implemented the result using Mathematica and MATLAB programs to simulation results, provided qualitatively, and figures.

Keywords. Seven-Dimension Hyperchaotic system, Bifurcation, Lyapunov Exponent, SDIC, Fractional Dimension, waveform analysis, security analysis, Speech Scrambler.

1. Introduction
Data safety for multimedia is a great challenge at the advanced open systems of communication that are endangered by various kinds of attacks. Encryption is the major tool to accomplish this safety. In comparison to other multimedia files (like image or text), speech files always possess larger size so that
traditional encryption schemes like AES, DES and RSA are inappropriate for the encryption of audio data because it consumes high power and requires a long computational time, so it cannot give a real-time communication. The establishment of new speech encryption systems with high speed and security has become a major interest in researchers working on a multimedia safety field [1-2]. In [3] recognition-based method for partly encryption telephonic speech was developed. In [4] two selective speech scrambled systems were introduced. In [5] authors suggested progressive speech encryption with a compression algorithm. almost all of the advanced encryption systems were based on two major concepts, diffusion & confusion, diffusion defined as plaintext statistics were completely dissolve in cipher statistics, while confusion defined as: is the relationship between the key and the ciphertext was as complex as possible. Chaos theory has been introduced as a source of diffusion and confusion in cryptography in [6].

Chaotic map possesses a dynamical behavior and it is highly sensitized to initial condition and control parameters. This proves that a remarkable change in the output will be produced by a very small change in the initial condition, this develops a more random system. Chaotic maps were applied in a lot of image encryption system. Speech segment permutation based on a baker chaotic map has been employed in speech encryption In [7], authors in [8] constructed two novel 7D of the chaotic system one of them is fourth-order, and another is six -order, it was obtained chaotic behavior through the system simulation with two positive Lyapunov exponents and it applied insecure communication to safety information between receiver and transmitter. Authors in [9] applied in 2D cellular automata in speech encryption and scrambling. In [10] authors developed a chaotic scrambled system for speech scrambler signals in transform domains. In [11] speech scrambler system dependent on off.line ica was developed. In [12] speech shuffling encryption system was established. In [13] combined chaotic mapping was employed in a speech encryption system. In [14] A speech encryption system having signal and double dimension chaotic systems that type of kind discrete-time was developed. In [15] authors transform and compressive sensing was employed in speech encryption. In [16] developed a random unified chaotic map as a pseudo-random number generated and were employed in wireless communication for speech scrambler. In [17] A speech encryption depends on the cosine transformation number were proposed. In [18] a speech encryption system applying confusion and diffusion depending on the multi-scroll chaotic system and signal time key were introduced. In [19] authors developed a strategy for speech encryption by using the Zaslavsky map as PRNG. In [20] A mixed chaos function was employed in speech encryption. In [21] A new technique dependent on-stream cipher for electric speech scrambled was developed. In [22] a speech encryption algorithm employing a modified rotation equation and substitution permutation architecture based on circle chaotic map was developed.

This work suggests an enhanced scheme of speech encryption based on a novel 7D hyperchaotic system that twelve positive parameters and eight-term cross-product to produce a strong chaotic sequence that has most of the randomness and dynamic complexity with DCT. This article is structured as follows: section two, the mathematical establishing of the novel 7D hyperchaotic system as PRNG and it has satisfactory performance, and then the system 7D is analyzed dynamically, in section three, the proposed algorithm, section four, national institute of standards and technology to test PRNG, section five, speech scrambler / de-scrambler algorithm, section six, security analysis and provides a comparative analysis of the scheme proposed, Finally, conclusions are discussed.

2. The Mathematical establishing of the PROPOSED SYSTEM

The proposed novel 7D autonomous in the third-order hyperchaotic system with twelve positive parameters. It obtained a novel system by conducting several experiments to find the system parameters and initial conditions for the system (system statuses). This system was acquired the following:

\[
\begin{align*}
\frac{dx}{dt} &= -\sigma x + \rho y + \delta w - \eta v \\
\frac{dy}{dt} &= \Omega x - \Psi x z - \mu y
\end{align*}
\]

2
\[\begin{align*}
\frac{dz}{dt} &= -\phi z + xy + \eta v \\
\frac{dw}{dt} &= -w - \Omega yz - \phi vp \\
\frac{dv}{dt} &= yp + \beta xp - \eta z - v \\
\frac{du}{dt} &= -\omega u - \mu zwp + \Omega xp \\
\frac{dp}{dt} &= -\alpha p + x y + \eta v
\end{align*}\]

Wherever \(\sigma, \rho, \delta, \eta, \Omega, \Psi, \mu, \phi, \Omega, \beta, \omega, \text{ and } \alpha\) are positive system parameters and \(x, y, z, u, v, w, \text{ and } p\) belong to real called system statuses and. The novel seven-dimensional system (1) displays a chaotic and strange attractor, while system parameter values are elected as:

\[\begin{align*}
\sigma &= 14, \\
\rho &= 11, \\
\delta &= 0.4, \\
\eta &= 0.5, \\
\Omega &= 30, \\
\Psi &= 2.5, \\
\mu &= 5, \\
\phi &= 3, \\
\beta &= 2, \\
\omega &= 15, \\
\alpha &= 4 \text{ and } \alpha = 13
\end{align*}\]

The initial conditions as:

\[\begin{align*}
x(0) &= 0.1, \\
y(0) &= 0.5, \\
z(0) &= 3.5, \\
w(0) &= 0.6, \\
u(0) &= 0.4, \\
v(0) &= 0.1 \text{ and } p(0) = 0.6
\end{align*}\]

(3) Form (1) The strange attractor for proposed system in 3-D view is included in figure (1(a)) and in 2-D view is included in figures (1(b)).

![Figure 1. Chaotic attractors in a) 3-D view (y-x-v) b) 2-D View (x-y)](image-url)

The zero-one test to check used in deterministic dynamic systems to distinguish between chaotic dynamics and nonchaotic [23]. The K values obtained from the improved system where variables \((x, y, z, w, u, v, \text{ and } p)\) are achieved:

\[\begin{align*}
k_x &= 0.9901, \\
k_y &= 0.9797, \\
k_z &= 0.9811, \\
k_w &= 0.9614, \\
k_u &= 0.9497, \\
k_v &= 0.9597, \\
k_p &= 0.9712
\end{align*}\]

because all values \(K\) have been determined near one, we can say the proposed system is chaotic.

The Lyapunov exponent [24] for the proposed novel 7D system are:

\[\begin{align*}
L_1 &= 0.929593, \\
L_2 &= 0.327552, \\
L_3 &= 0.001271, \\
L_4 &= -1.214300, \\
L_5 &= -1.369635, \\
L_6 &= -1.381757, \\
L_7 &= -1.728070
\end{align*}\]

It can prove that the proposed system has chaotic features because the largest Lyapunov exponent is positive, since the \(L_1, L_2\) and \(L_3\) are three positive Lyapunov exponents and reminder four Lyapunov exponents are negative as figure (2), Therefore, the system is hyperchaotic. The fractal dimension [25] which determined through Lyapunov exponents for the proposed system by Kaplan-Yorke dimension is 

\[D_{KY} = 4.0322\]

This implies that the Lyapunov dimension is fractional. The proposed system has non-periodic orbits because of its fractal nature. Long-term unpredictability is one of the most important properties of a chaotic system because of the SDIC (sensitivity dependent on initial condition) solutions, two contrasting initial conditions, regardless of how close to each other will finally become impossible to predict. The initial values of the proposed system for the rigid line and dished line are chosen respectively as follows:

- \(x(0)=0.1, \ y(0)=0.5, \ z(0)=3.5, \ w(0)=0.6, \ u(0)=0.4, \ v(0)=0.1, \ p(0)=0.6\), while
- \(x(0)=0.1000001, \ y(0)=0.5, \ z(0)=3.5, \ w(0)=0.6, \ u(0)=0.4, v(0)=0.1, \ p(0)=0.6\), from fig.(2(b)) motions the proposed system beginning with very similar initial conditions, which implies this proposed system...
is extraordinarily (SDIC) sensitive to initial value prove that the trajectories evolution of the proposed system is a very (SDIC). the waveform of a chaotic system should be aperiodic. To demonstrate that the proposed system is chaotic It is obvious that from fig. (3 (c)) the waveforms are aperiodic. It can observe that the time-domain waveform has non-cyclical characteristics.

![Figure 2. Some dynamics properties for the proposed system](image)

### 3. THE PROPOSED ALGORITHM

The following algorithms are used to generate the PRNG from the proposed system.

1. Initialize the twelve secrets parameters and seven initial conditions of the proposed system to produce a secret key
2. Generate secret keys from the proposed novel 7D system
3. Truncate a sequence chaotic $F_i$ from the trajectory of $x_i, y_i, z_i, w_i, u_i, v_i$ and $p_i$
4. Convert them from real number $F_i$ of $x_i, y_i, z_i, w_i, u_i, v_i$ and $p_i$ into a 32-bit binary using the IEEE-754 -Standard.
5. Pick the last 16th digital number to obtain a binary string.

### 4. NIST test group

The random behavior of the novel hyperchaotic system is testes by the NIST test. For binary bits sequences, there is a requirement to measure the degree of randomization that generates chaotic keys for speech scrambling processes. This uses a statistical package that includes 15 different tests. It is called the National Standards and Technology Institute test (NIST Test)[26], for security, testing the chaotic scrambler generated bit sequences must pass the statistical tests. The NIST test consists of 15 tests, we take 12 test only, and the NIST test is widely used in the design of ciphers. To test the randomness of the binary sequence the NIST test has been used through calculation a (p-value) as follows:

1. If $p = 1$, that means excellent randomness of the sequences.
2. If $p = 0$, the sequences appear to be entirely non-random, the result in Table 1 has shown that the sequence from the novel system have twelve successfully passed the NIST test, therefore, the proposed algorithm has generated a sequence that possesses good arbitrary satisfying properties. The remaining three tests have been failed because of the insufficient numbers of cycles thus these tests are not applicable.

| No. | NIST-800-22 Tests | P-value (x) | P-value (y) | P-value (z) | P-value (w) | P-value (u) | P-value (v) | P-value (p) | Assessment |
|-----|------------------|------------|------------|------------|------------|------------|------------|------------|------------|
| 1   | Frequency (Monobit) Block | 0.7941 | 0.7600 | 0.3799 | 0.4527 | 0.8103 | 0.9746 | 0.7941 | ✓          |
| 2   | Frequency (m=128)   | 0.1038 | 0.5288 | 0.7326 | 0.0517 | 0.9914 | 0.1792 | 0.1038 | ✓          |
| 3   | Run               | 0.679 | 0.7309 | 0.2783 | 0.1799 | 0.9949 | 0.7268 | 0.2113 | ✓          |
5. SPEECH SCRAMBLER / De-scrambler Algorithm

In the following section, the proposed speech scrambler scheme consists of two stages that will be discussed. The proposed scheme's block diagram is shown below.

5.1. Speech Encryption Algorithm

The proposed algorithm (Symmetric Cipher) speech encryption with chaotic key as PRNG (pseudo-random number generated). Summarized the proposed encryption system as follows:

Step 1: (Original Speech)

Record and save the original analog speech signal or read the clear speech signal, reduce vector n*1 original data speech where n is the length of file speech. with sample rate Fs (Hz)= 8000, Number of channels= 1, Samples bit per = 16-bit integer.

Figure 3. shows a simplified block diagram of the proposed speech scrambler /Descrambler signal using the proposed chaotic system with orthogonal transformation (DCT)).
Step 2: (DCT)
Applying orthogonal Transformation DCT (discrete cosine transformation).
Step 3: (Convert 32-bit)
Convert Data in step 2 to a 32-bit binary by the suggesting method. These values are generated by speech after inserting the orthogonal transformation DCT. Then we separate an integral part from the fractional part and converting each part into 16 bits to become 32bit by letting n = 16; integer part, m = 16 fractions part. by using the following, where α any number
\[
\begin{align*}
\text{if}(\alpha < 0)
\quad & d2b = -1*(\text{fix}(\text{rem}(\alpha*\text{pow}(2, -(n-1):m),2))); \\
\text{else}
\quad & d2b = (\text{fix}(\text{rem}(\alpha*\text{pow}(2, -(n-1):m),2))); \\
\end{align*}
\]
end
Step 4: (Key Generation by a proposed Algorithms)
Input the parameters \(\sigma, \rho, \delta, \eta, \Omega, \Psi, \phi, \Omega, \beta, \omega, \mu\) and \(\alpha\). and the initial conditions \((x(0), y(0), z(0), w(0), u(0), v(0), p(0))\)generate seven sequences \(\{(x_i, y_i, z_i, w_i, u_i, v_i, p_i); i = 1, 2, \ldots, \text{time}\*\text{Fs}*2\}\) according to the proposed chaotic system (1). That means using the proposed algorithms above.
Step 5: (Mixing)
Fetch the last 16th digital number of the obtained binary string for the first key, then we take the last 16th of the second key. And mixing them with 16 bits from the first key to represent 32-bit binary form.
Step 6: (XOR)
Perform XOR operation between step 3 and step 5.
Step 7:
Convert 32-bit binary to double to gain on speech encryption signal
Step 8: (encryption speech)
Save and send encrypted speech.
The recipient and when the encrypted speech is received.
Firstly, Sharing the nineteen secret keys between the receiver and the sender so that they can be decrypted/sumbled the scrambled speech. The nineteen secret keys are:
The twelve system parameter values for the proposed 7D novel system: \(\sigma, \rho, \delta, \eta, \Omega, \Psi, \phi, \Omega, \beta, \omega, \mu\) and \(\alpha\).
The seven system status for the proposed 7D novel system: \(x(0), y(0), z(0), w(0), u(0), v(0)\) and \(p(0)\).
Secondly, Initialize the twelve secrets parameters and seven system status of the proposed system to produce the same secret key that is used by the receivers from the proposed system by using the same proposed algorithms. Convert them from real number \(F_i\) of \(x_i, y_i, z_i, w_i, u_i, v_i\) and \(p_i\) into a 32-bit binary using the IEEE-754 -Standard. Pick the last 16th digital number to obtain a binary string for the first key, then we take the last 16th of the second key, and connecting them with 16 bits from the first key to represent 32-bit binary form. Perform XOR operation between 32-bit binary form from the proposed system and 32-bit binary form from encryption speech by using step 3, convert 32-bit binary to double to gain on speech encryption signal, and applying inverse orthogonal Transformation (IDCT) transformed back to the clear speech.

6. Simulation Results
Applied several experiments to various speech with different sizes based on the proposed scheme have been performed, now, to measure the proposed algorithm performance, the experiment results for subjective tests are shown in figures [5],[6]. It is apparent from the figure that the scheme converts from clear speech into an encrypted speech like almost noise.
7. Results Discussion

The proposed scheme's security evaluation will be viewed using some performance measures, including key sensitivity and key space analysis.

7.1. Sensitivity and Key Space Analysis

Key space is the collection of all the speech encryption secret keys used. Two measurements can be used to assess it: The system parameters $\sigma, \rho, \delta, \eta, \Omega, \phi, \Omega, \Psi, \mu, \beta, \omega, \alpha$ and $\mu$ and the system status as $x(0), y(0), z(0), w(0), u(0), v(0)$ and $p(0)$. In this case, if computation precision is $10^{-14}$, the key space size can reach $10^{266} \approx 2^{880}$. So, the key space was much larger to avoid the attackers of brute-force exhaustion. Given in Table 2 compared this scheme based on the proposed novel 7D system and DCT with other schemes.

| Ref & Ours | Ref [32] | Ref [21] | Ref [33] | Ref [19] | Ref [29] | Ref [22] |
|------------|----------|----------|----------|----------|----------|----------|
| Size key space | $2^{880}$ | $2^{512}$ | $2^{512}$ | $2^{548}$ | $2^{477}$ | $2^{256}$ | $2^{149}$ |

To testing key sensitivity for the proposed novel seven dimensions just tiny, changes one value of parameter keys, and maintaining all the other parameters without changing during implement speech scrambling technique to recover the speech signal. The key sensitivity to proposed chaotic signals will be tested for the nineteen secret keys. The secret Keys of the proposed system are $\{x(0), y(0), z(0), w(0), u(0), v(0), p(0), \sigma, \rho, \delta, \eta, \Omega, \phi, \Omega, \Psi, \mu, \beta, \omega, \alpha\}$ three tests will be studied to show the sensitivity of key to the proposed chaotic system by using some statistical measurements, like percentage of Difference (P. Diff.), $R_C$, and SSNR, for guessing between the decrypted speech signals with different keys by little changes in $key_i, i = 1, 2, 3, ..., 19,$ and the speech decrypted by using the original key. Whenever they P. Diff. is large value and the SSNR and $R_C$ is small value it is means a large chaotic keys sensitivity of that used in the proposed system as shown in Table 3. From Figure 4: the key sensitivity analysis: experimental waveform ‘Claire’ results a) clear speech f) Speech encrypted with normal keys, (c-j) Speech Encrypted with change keys. This proves that the scheme proposed is very SDIC therefore it is robust against the statistical attack and the brute force attacks.

7.2. Histogram Analysis

Histogram analysis is an effective metric used to measure the consistency of the speech signal that is encrypted. Successful scheme encryption must encrypt the clear speech into a random like noise with a nearly flat deal of sample values. Hence statistical attacks can face it.

| Key name | Change key | $R_C$ | SSNR | P. Diff |
|----------|------------|-------|-------|---------|
| Key1     | $x(0) + 10^{-8}$ | 0.0049 | -30.1146 | 100%    |
| Key2     | $y(0) + 10^{-8}$ | -0.0018 | -30.1113 | 100%    |
| Key3     | $z(0) + 10^{-8}$ | 0.0252 | -30.1034 | 100%    |
| Key4     | $w(0) + 10^{-8}$ | 0.0112 | -30.1203 | 100%    |
| Key5     | $u(0) + 10^{-8}$ | 0.0137 | -30.1212 | 100%    |
| Key6     | $v(0) + 10^{-8}$ | 0.0106 | -30.1087 | 100%    |
| Key7     | $p(0) + 10^{-8}$ | 0.0149 | -30.1104 | 100%    |
| Key8     | $\sigma + 10^{-8}$ | 0.0031 | -30.1195 | 100%    |
| Key9     | $\rho + 10^{-8}$ | 0.031 | -30.1195 | 100%    |
| Key10    | $\delta + 10^{-8}$ | 0.00955 | -30.1159 | 100%    |
| Key11    | $\eta + 10^{-8}$ | 0.00953 | -30.1154 | 100%    |
| Key12    | $\Omega + 10^{-8}$ | 0.0127 | -30.1116 | 100%    |
| Key13    | $\Psi + 10^{-8}$ | 0.0015 | -30.1084 | 100%    |
| Key   | $\theta + 10^{-8}$ | $\mu + 10^{-8}$ | $\beta + 10^{-8}$ | $\omega + 10^{-8}$ | $\alpha + 10^{-8}$ |
|-------|--------------------|-----------------|-------------------|-------------------|-------------------|
| Key14 | 0.0087             | -0.0041         | -0.0161           | 0.0151            | 0.0041            |
| Key15 | -0.0118            | -0.0111         | -30.1186          | -30.1117          | -30.1123          |
| Key16 | 100%               | 100%            | 100%              | 100%              | 100%              |
| Key17 | 0.0094             | 0.0041          | -30.1123          | -30.1102          | -30.1123          |
| Key18 | 0.0151             | 0.0041          | -30.1123          | -30.1102          | -30.1123          |
| Key19 | 0.0041             | 0.0041          | -30.1121          | -30.1151          | -30.1121          |

**Figure 4.** The key sensitivity analysis: experimental waveform ‘Claire’ results a) original speech f) Speech encrypted with original keys (c-j) Speech Encrypted with (x(0) + 10^{-8}),(y(0) +10^{-8} ),(z(0) +10^{-8}),(w(0) +10^{-8}),(u(0) +10^{-8}),(v(0) +10^{-8}),(p(0) +10^{-8}),(\sigma +10^{-8} ), respectively.

Shawn in fig(6[(G),(P),(Y)]) Histogram of clear speech while shown in fig(6[(G),(P),(Y)]). Histogram of speech encrypted.

7.3. SPECTROGRAM ANALYSIS

The spectrogram is used because it is a visual representation that enables us to see what happens all at once in time domain and frequency. It divides the speech into several chunks (in the time domain) and Fourier transforms its obtained plot of each chunk and shows them all in the same graph. Shown in fig.(6[(D),(M),(V)]). Spectrogram of clear speech while shown in fig(6[(E),(N),(W)]). Spectrogram of speech encrypted. It is clear that the difference between clear speech and Scrambler speech
7.4. Correlation Coefficient ($R_c$)
The correlation coefficient is an essential estimate (is a numerical measurement) of the correlation between the clear speech file and the scrambled speech file. The formula of the correlation coefficient of two clear speech and encrypted gives as follow:

\[ \text{corr}(x, y) = E(x - E(x))(y - E(y)) \]
\[ r_{xy} = \frac{\text{corr}(xy)}{\sqrt{\text{var}(x) \text{var}(y)}} \]
\[ \bar{y} = \frac{1}{n} \sum_{t=1}^{n} Y_t \]
\[ \bar{x} = \frac{1}{n} \sum_{t=1}^{n} X_t \]

by substituted $\text{corr}(x, y)$, $\text{var}(x)$ and $\text{var}(y)$ we get

\[ R_c = \frac{\sum_{t=1}^{n} (X_t - \bar{x})(Y_t - \bar{y})}{\sqrt{\sum_{t=1}^{n} (X_t - \bar{x})^2} \sqrt{\sum_{t=1}^{n} (Y_t - \bar{y})^2}} \]

Where $(X_i)$ clear speech sample, $(Y_i)$ scrambled speech sample, $(n)$ is the no. of speech samples [12].

The appropriate correlations are within the range of (–1 and 1), when $R=0$, so there is no correlation between clear and scrambled speech. An excellent speech scrambling has been produced when the correlated values are close to zero, therefore high security and low R.I. when $R=1$ then one variable will increase while the other will decrease (perfect negative correlations). When $R= +1$ then both variables will move in the same direction (perfect positive correlation), thus give us low security and high R.I. From Table [4], the $R_c$ between encrypted speech and clear speech file appears. From fig (5) the scatter plot between clear speech and encrypted speech files appears. Prove that from Table [4] the $R_c$ close to zero values that means reflects the randomness for scrambler speech and different two files.

7.5. PSNR Analysis:
Peak Signal-to-Noise Ratio (PSNR) [12]: Compute the mean square error for two vectors $X, Y$ by using the form:

\[ MSE = \frac{1}{n} \sum_{i=1}^{n} (X_i + Y_i)^2 \]

If $Y$ is an encrypted speech & $X$ is clear speech then the form $PSNR$ is

\[ PSNR = 10 \log_{10} \left( \frac{\text{max value}}{MSE} \right)^2 \]

The PSNR value is computed for the speech scrambler. It is clear that from Table [4] the PSNR is a small value that means that strong level noise in speech scrambler therefore good strength to attackers.

7.6. SSNR Analysis:
Spectral Segment Signal to Noise Ratio Measure [30] is formed:

\[ SSNR = 10 \log \left( \frac{\sum_{k=0}^{N/2-1} |X_k|^2}{\sum_{k=0}^{N/2-1} |X_k|^2 - |Y_k|^2} \right) \]

where, $X_k$ is the DFT of clear input speech, and $Y_k$ is DFT of the encrypted signal. This test provides an indicator of the encryption quality. This calculation is determined by taking DFT for them with a similar resolution between the clear signal and the encrypted signal. From Table [4] the proposed system has more negative SSNR. Therefore, it is better against attackers.

7.7. SNR Analysis:
Signal to noise ratio (SNR) [14]: for calculating the signal efficiency used SNR which the form:

\[ SNR = \frac{\sum_{i=1}^{n} x_i^2}{\sum_{i=1}^{n} y_i^2} \]

$n$ =number of the sample, where $x$ the clear speech & $y$ the encrypted speech. From Table [4] the proposed system has negative SNR. Therefore, it is better against attackers.

7.8. RMS & CF Values:
The value of the root mean square (RMS) [29] is calculated by the average value of clear speech amplitude rate has the form:

\[ RMS = \sqrt{\frac{|A|^2}{N}} \]

A waveform parameter that is defined is the Crest factor (CF) the ratio between the effective value and the peak values has Form:

\[ CF = 20 \log_{10} \left( \frac{|V_{\text{peak}}|}{V_{\text{RMS}}} \right) \]

from the Table[4], CF & RMS computed for encrypted speech. It clear that CF & RMS are close to (0.00001325, 0.99999), respectively, the relationship between the clear speech and the encrypted speech files is not statistical.
Table 4. $R_C$, SNR, PSNR, SSNR, RMS, and CF between clear and encrypted speech files.

| Speech files | $R_C$  | SNR     | PSNR   | SSNR    | RMS      | CF       |
|--------------|--------|---------|--------|---------|----------|----------|
| Claire       | 0.001906 | -27.9940 | 0.0038  | -39.2984 | 0.99998  | -0.000133 |
| Mike         | 0.000204  | -28.7314 | 0.0043  | -34.5831 | 0.99998  | -0.0001321|
| Charles      | 0.002489  | -27.7471 | 0.00805 | -36.8101 | 0.99999  | 0.0001325 |
| Lauren       | 0.0004579 | -28.4280 | -0.0046 | -39.5601 | 0.99998  | 0.0001352 |
| Rich         | 0.00837317 | -29.5849 | -0.012419 | -32.3723 | 0.99998  | -0.0013421|
| Ray          | 0.0033318 | -26.0598 | -0.0046801 | -42.2938 | 0.99998  | -0.0001322 |

8. SPEED PERFORMANCE

An important factor to consider when analyzing the efficiency of a cryptosystem is its speed. Accordingly, run the proposed algorithm implemented in MATLAB 2019 b under Windows 10, using a laptop with Intel(R) Core (TM) i7 @2.53GHz CPU and 6 GB RAM. Used 5 speech tested files. To computational speed of the proposed novel system with DCT. It takes approximately between 0.21 – 0.99 s to scrambler $IKB$ of a sample. If the length audio file increase then this time increases. The computational speed is summarized in Table [5].

Table 5. Time analysis

| Speech files | Size (KB) | Total (S) | Speed (S/KB) |
|--------------|-----------|-----------|--------------|
| Claire       | 32 KB     | 13.0916   | 0.4091       |
| Mike         | 48 KB     | 21.544    | 0.4488       |
| Charles      | 64 KB     | 30.6883   | 0.4795       |
| Lauren       | 80 KB     | 48.7133   | 0.6089       |
| Rich         | 128 KB    | 116.0516  | 0.9067       |

9. COMPARATIVE STUDY

The abilities of the proposed system in this paper with another scheme. The most popular security measure including having been used for efficiency (Key Space), (SNR), (SSNR), (PSNR), (CF), (RMS) and ($R_C$) have been used for efficiency comparison. Table [6] display this comparison with another scheme, from this outcome, it has been found that the proposed system has the smallest value of correlation coefficient $R_C$ between the clear speech and its corresponding scrambled files one that reflects the smallest similarity among them. It is obvious that the proposed system has the greatest key space comparing to other systems with an amount of $2^{880}$, also it has a powerful strength to attacks. The proposed system has the lowest PSNR value and more negative value of SSNR and the compared to other systems, also the system has the highest values of RMS and the smallest CF therefore the best one against different attacks.

10. CONCLUSION

In this paper, proposed a new cryptography scheme for speech scrambling which gives it more security level. Also, it introduced a novel seven dimensions (7D) nonlinear hyperchaotic system in third-order which has twelve positive parameters. A chaotic behavior for the proposed novel system is analyzed. It has three positive Lyapunov exponents therefore the system is hyperchaotic and the Lyapunov
dimension is fractional. The proposed system has non-periodic orbits because of its fractal nature, and prove that the trajectories evolution of the proposed system is a very (SDIC). The hyperchaotic system is demonstrated that beside it appropriates for speech scrambler. PRNG (Pseudo Random Number Generated) is created based on the proposed 7D hyperchaotic result. The proposed scheme depends on this novel hyperchaotic system as PRNG to generate a random keystream bit. The input speech signal in this work is first squeezed by discrete cosine transformation (DCT) to minimize the residual intelligibility (R.I.). Increasing the number of system parameters accomplished a high key space, therefore, improves the security to resist several cryptographic attacks. The scheme is measured using various tests. Peak Signal-to-Noise Ratio (PSNR), Signal to noise ratio (SNR), percentage of Difference (P. Diff.) , Segmental Signal to Noise Ratio Measure (SSNR), root mean square measure(RMS), Correlation coefficient Measure ($R_C$), Crest factor measure (CF), histogram, spectrogram, key sensitivity, waveform, and key space. The results of simulation and comparison prove that the algorithm can achieve better performance in encryption that means the scheme is stronger and highly secure against various types of attacks than many recent similar audio encryption schemes.

Table 6. Comparative study

| Systems          | Key Space | $R_C$  | SNR | SSNR | PSNR | CF   | RMS   |
|------------------|-----------|--------|-----|------|------|------|-------|
| Ref [12]         | -         | 0.0263 | -   | -    | 4.536| -    | -     |
| Ref [13]         | $2 \times 10^{28}$ | 0.0282 | -  | -    | -    | -    | -     |
| Ref [14]         | $2^{128}$ | 0.0014 | -1.47 | -   | -    | -    | -     |
| Ref [17]         | $2^{256}$ | 0.0021 | -   | -    | 4.8  | -    | -     |
| Ref [18]         | $2^{128}$ | 0.00035 | -   | -    | 4.426| 4.8  | -     |
| Ref [19]         | $2^{447}$ | 0.00023 | -23.89 | -   | -    | -    | -     |
| Ref [20]         | $2^{144}$ | 0.0092 | -   | -    | -    | -    | -     |
| Ref [27]         | $2^{512}$ | -0.0011 | -10.63 | -  | 47.98 | -    | -     |
| Ref [28]         | -         | 0.0119 | 34.71 | -   | 62.31 | 4.8  | -     |
| Ref [22]         | $2^{149}$ | -0.00038 | -16.06 | -  | 4.39  | -    | -     |
| Ref [29]         | $2^{256}$ | 0.00207 | -   | -    | 4.8  | 0.6  | -     |
| AES              | $2^{256}$ | 0.0097 | -1.4 | -   | -    | -    | -     |
| Triple DES       | $2^{168}$ | 0.1704 | -0.25 | -   | -    | -    | -     |
| Ref [30]         | -         | -     | -2.62555 | -2.45871 | -   | -     |
| Ref [31]         | -         | -     | -35.0224 | -38.0201 | -   | -     |
| Ref [3]          | -         | -     | -2.62555 | -2.56744 | -   | -     |
| Ref [10]         | -         | -     | -23.1549 | -   | -    | -    | -     |
| Ref [11]         | -         | -     | -13.07 | -20.968 | -   | -     |
| ours             | $2^{880}$ | 0.000204 | -29.5849 | -42.2957 | 0.004306 | 0.0001325 | 0.99999 |
Figure 6. Simulation result: clear speech [(A),(J),(S)], encryption speech [(B),(K),(T)], recovered speech [(C),(L),(U)], Histogram clear speech [(G),(P),(Y)], Histogram encryption speech [(H),(Q),(Z)], Histogram recovered speech [(I),(R),(XZ)], spectrogram clear speech [(D),(M),(V)], spectrogram encryption speech [(E),(N),(W)], spectrogram recovered speech [(F),(O),(X)].
References

[1] Rijmen, Vincent, and Joan Daemen. "Advanced encryption standard." Proceedings of Federal Information Processing Standards Publications, National Institute of Standards and Technology (2001): 19-22.

[2] RIVEST, RONALD L., ADI SHAMIR, AND LEONARD ADLEMAN. "A METHOD FOR OBTAINING DIGITAL SIGNATURES AND PUBLIC-KEY CRYPTOSYSTEMS." COMMUNICATIONS OF THE ACM 21.2 (1978): 120-126.

[3] SERVETTI, ANTONIO, AND JUAN CARLOS DE MARTIN. "PERCEPTION-BASED PARTIAL ENCRYPTION OF COMPRESSED SPEECH." IEEE TRANSACTIONS ON SPEECH AND AUDIO PROCESSING 10.8 (2002): 637-643.

[4] SERVETTI, ANTONIO, CRISTIANO TESTA, AND JUAN CARLOS DE MARTIN. "FREQUENCY-SELECTIVE PARTIAL ENCRYPTION OF COMPRESSED AUDIO." 2003 IEEE INTERNATIONAL CONFERENCE ON ACOUSTICS, SPEECH, AND SIGNAL PROCESSING, 2003. PROCEEDINGS,(ICASSP'03).,. VOL. 5. IEEE, 2003.

[5] YAN, WEI-QI, WEI-GANG FU, AND MOHAN S. KANKANHALLI. "PROGRESSIVE AUDIO SCRAMBLING IN THE COMPRESSED DOMAIN." IEEE TRANSACTIONS ON MULTIMEDIA 10.6 (2008): 960-968.

[6] ALVAREZ, GONZALO, AND SHUJUN LI. "SOME BASIC CRYPTOGRAPHIC REQUIREMENTS FOR CHAOS-BASED CRYPTOSYSTEMS." INTERNATIONAL JOURNAL OF BIFURCATION AND CHAOS 16.08 (2006): 2129-2151.

[7] Mosa, Emad, et al. "Chaotic encryption of speech signals." International Journal of Speech Technology 14.4 (2011): 285.

[8] S.N.Lagmire, M.Amghar, and N.Sbiti, “ Hyperchaos Based Cryptography: New Seven Dimensional to Secure Communications ”, Circulation in Computer Science, vol.2, No.2, pp(20-30), 2017.

[9] Madain, Alia, et al. "Audio scrambling technique based on cellular automata." Multimedia tools and applications 71.3 (2014): 1803-1822.

[10] Mosa, Emad, Nagy W. Messiha, and Osama Zahran. "Chaotic encryption of speech signals in transform domains." 2009 International Conference on Computer Engineering & Systems. IEEE, 2009.

[11] Tamimi, Abdelfatah A., and Ayman M. Abdalla. "An audio shuffle-encryption algorithm." The world congress on engineering and computer science. 2014.

[12] ABBAS, NIDAA A., AND SATTAR B. SADKHan. "A PROPOSED VOICE ENCRYPTION SYSTEM BASED ON OFF-LINE ICA ALGORITHM." JOURNAL OF UNIVERSITY OF BABYLON 22.7 (2014): 1917-1923.

[13] LI, RUISHAN DU YANG. "APPLICATION OF COMPOUND CHAOTIC MAPPING IN VOICE ENCRYPTION ALGORITHM." INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND NETWORK SECURITY (IJCNS) 14.8 (2014): 44.

[14] AKGÜL, AKIF, SEZGIN KAÇAR, AND İHSAN PEHLİVAN. "AN AUDIO DATA ENCRYPTION WITH SINGLE AND DOUBLE DIMENSION DISCRETE-TIME CHAOTIC SYSTEMS." TOJSAT 5.3 (2015): 14-23.

[15] AUGUSTINE, NISHANTH, SUDHISH N. GEORGE, AND DEEPTHI P. PATTATHIL. "AN AUDIO ENCRYPTION TECHNIQUE THROUGH COMPRESSIVE SENSING AND ARNOLD TRANSFORM." INTERNATIONAL JOURNAL OF TRUST MANAGEMENT IN COMPUTING AND COMMUNICATIONS 3.1 (2015): 74-92.

[16] Sadkhan, Sattar B., and Rana Saad Mohammed. "Proposed random unified chaotic map as PRBG for voice encryption in wireless communication." Procedia computer science 65 (2015): 314-323.

[17] LIMA, JULIANO B., AND ERONIDES F. DA SILVA NETO. "AUDIo ENCRYPTION BASED ON THE COSINE NUMBER TRANSFORM." MULTIMEDIA TOOLS AND APPLICATIONS 75.14 (2016): 8403-8418.
[18] LIU, HONGJUN, ABDURAHMAN KADIR, AND YANLING LI. "AUDIO ENCRYPTION SCHEME BY CONFLATION AND DIFFUSION BASED ON MULTI-SCROLL CHAOTIC SYSTEM AND ONE-TIME KEYS." OPTIK 127.19 (2016): 7431-7438.

[19] FARSANA, F. J., AND K. GOPAKUMAR. "A NOVEL APPROACH FOR SPEECH ENCRYPTION: ZASŁAVSKY MAP AS PSEUDO RANDOM NUMBER GENERATOR." PROCEDIA COMPUTER SCIENCE 93 (2016): 816-823.

[20] GHASEMZADEH, ARDALAN, AND ELHAM ESMAILI. "A NOVEL METHOD IN AUDIO MESSAGE ENCRYPTION BASED ON A MIXTURE OF CHAOS FUNCTION." INTERNATIONAL JOURNAL OF SPEECH TECHNOLOGY 20.4 (2017): 829-837.

[21] KALPANA, MUTHUSAMY, KURU RATNAVELU, AND PAGAVATHI BALASUBRAMANIAM. "AN AUDIO ENCRYPTION BASED ON SYNCHRONIZATION OF ROBUST BAM FCNNS WITH TIME DELAYS."MULTIMEDIA TOOLS AND APPLICATIONS 78.5 (2019): 5969-5988.

[22] Kordov, Krasimir. "A novel audio encryption algorithm with permutation-substitution architecture." Electronics 8.5 (2019): 530.

[23] MEHDI, SADIQ A., AND RAGEED HUSSEIN AL-HASHEMY. "A NEW ALGORITHM BASED ON MAGIC SQUARE AND A NOVEL CHAOTIC SYSTEM FOR IMAGE ENCRYPTION." JOURNAL OF INTELLIGENT SYSTEMS (2019).

[24] WOLF, ALAN, ET AL. "DETERMINING LYAPUNOV EXPONENTS FROM A TIME SERIES." PHYSICA D: NONLINEAR PHENOMENA 16.3 (1985): 285-317.

[25] MEHDI, SADIQ A., AND HAYDER A. QASIM. "ANALYSIS OF A NEW HYPER CHAOTIC SYSTEM WITH SIX CROSS-PRODUCT NONLINEARITIES TERMS." AM. J. ENG. RES 6 (2017): 248-252.

[26] Diaz, Cathleen. Concept for an Algorithm Testing and Evaluation Program at NIST. US Department of Commerce, National Institute of Standards and Technology, 1994.

[27] BELMEGUENAI, AISSA, ET AL. "A NOVEL APPROACH BASED ON STREAM CIPHER FOR SELECTIVE SPEECH ENCRYPTION." INTERNATIONAL JOURNAL OF SPEECH TECHNOLOGY 20.3 (2017): 685-698.

[28] SATISHAMURTHI, P., AND S. RAMAKRISHNAN. "SPEECH ENCRYPTION USING CHAOTIC SHIFT KEYING FOR SECURED SPEECH COMMUNICATION." EURASIP JOURNAL ON AUDIO, SPEECH, AND MUSIC PROCESSING 2017.1 (2017): 1-11.

[29] NASKAR, PRABIR KUMAR, ET AL. "DNA ENCODING AND CHANNEL SHUFFLING FOR SECURED ENCRYPTION OF AUDIO DATA." MULTIMEDIA TOOLS AND APPLICATIONS 78.17 (2019): 25019-25042.

[30] AL-SAAD, SAAD N. "A SPEECH SCRAMBLER ALGORITHM BASED ON CHAOTIC SYSTEM." AL-MUSTANSIRIYAH JOURNAL OF SCIENCE 24.5 (2013): 357-372.

[31] IMRAN, OMAR A., ET AL. "IMPLEMENTATION OF EL-GAMAL ALGORITHM FOR SPEECH SIGNALS ENCRYPTION AND DECRYPTION." PROCEDIA COMPUTER SCIENCE 167 (2020): 1028-1037.

[32] KATE, HAMIDREZA KAKAEI, JAFAR RAZMARA, AND AYAZ ISAZADEH. "A NOVEL FAST AND SECURE APPROACH FOR VOICE ENCRYPTION BASED ON DNA COMPUTING." 3D RESEARCH 9.2 (2018): 17.

[33] F. J. FARSANA, V. R. DEVI, AND K. GOPAKUMAR, "AN AUDIO ENCRYPTION SCHEME BASED ON FAST WALSH HADAMARD TRANSFORM AND MIXED CHAOTIC KEYSTREAMS." APPL. COMPUT. INFORM., TO BE PUBLISHED, DOI: 10.1016/J.ACI.2019.10.001.