Available online at: www.basra-science-journal.org

ISSN –1817 –2695

Speech Encryption Using Chaotic Map and Blowfish Algorithms

Maysaa abd ulkareem and Iman Qays Abduljaleel

Basra university / Science collage

Computer science department

emankais@yahoo.com

Received 4-10-2011 , Accepted 25-3-2013

Abstract

Recently emerged interest in the transfer of information, whether speech or image or text information . To maintain the confidentiality of such information we need to encrypt it.

In this paper, we used wavelet packet transform to transfer speech signal from time domain to frequency domain after that a new encryption algorithm is proposed by analyzing the principle of the chaotic encryption algorithm based on logistic map and blowfish encryption algorithm . Chaotic function is used to make the algorithm more secure and make the process of the encryption and decryption more complex. We used partial encryption technique for faster the encryption /decryption speed process. Moreover, the performance of the proposed algorithm is also estimated by used SNR,PSNR,NRMSE,RSE quantities. Experimental result of the algorithm shows that the algorithm is faster, stronger and more secure. Use the Matlab ver.8.a in the different treatments stage.

Keywords : Speech, Wavelet Packet, Encryption, Blowfish Algorithm, Logistic Map.

1. Introduction

Speech communications become more and more widely used . The importance of providing a high level of security is dramatically increasing. As such, a variety of speech encryption techniques have been introduced.

In general, there are four main categories of speech encryption: frequency-domain scrambling (e.g., the frequency inverter and the band splitter), time-domain scrambling (e.g., the time element scrambling), amplitude scrambling (also known as the masking technique that covers the speech signal by the linear addition of pseudorandom amplitudes), and two-dimensional scrambling that combines the frequency-domain scrambling with the time-domain scrambling. Besides, there are many speech encryption methods in the transform domain, e.g., fast Fourier

transform, discrete cosine transform and wavelet transform, etc. Recently, some new speech encryption methods including chaotic cryptosystem and encryption using circulate transformations have also been developed [1].

Wavelet Transform is one of the most powerful tools in digital signal processing. The digital signal components are decomposed into different decomposition levels using a wavelet transform. These decomposition levels contain a number of subbands, which consist of coefficients that describe the horizontal and vertical spatial frequency characteristics of the original digital signal component [2].

the aim of proposed algorithm is to encrypt speech signal using wavelet packet transform for splitting the raw signal then using chaos theory and blowfish algorithm to encryption this signal .The main structure of any speech encryption/decryption system describe in fig.1.

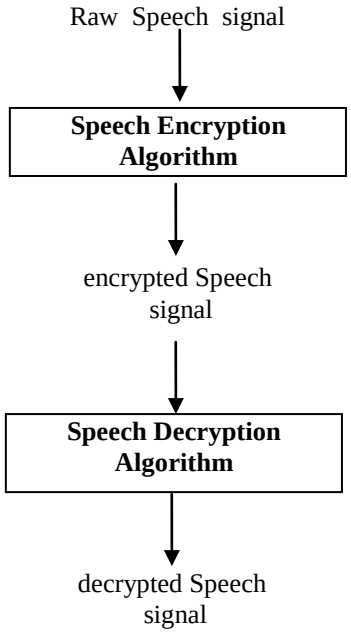

Fig.1 : Implementation of Encryption/Decryption Speech System

According to the differences between image , text and speech, recently there have been several innovative encryption techniques, some of them describe in [1,3, 4].

We describe below the most important principles uses in this paper :

2.Chaotic map

Chaos theory has been established since 1970s by many different research areas, such as physics, mathematics, engineering, and biology, etc..After that and Since 1990s, many researchers have noticed that there exists the close relationship between chaos and cryptography [5].

The security of stream cipher, which is known as one of the main cipher techniques, dependents completely on the quality of generated pseudo-stochastic sequences. Chaotic systems can produce the pseudo-random sequences with good randomness therefore, these systems are suitable to the stream cipher[6].

Chaotic systems have many important properties, such as the sensitivity depends on initial conditions and system parameters, pseudorandom property, no periodicity and topological transitivity, etc. Most properties

meet some requirements such as diffusion and mixing in the sense of cryptography [7]. Therefore, it can provide a fast and secure means for data protection, which is crucial for multimedia data transmission over fast communication channels, such as the broadband internet communication.

As known Logistic map is defined as[8]:

$$x_{n+1} = \lambda * (x_n * (1 - x_n)) \quad \ldots(1)$$

where $0 < \lambda \leq 4$, n = 0,1,. . ..

The parameter λ and initial value x_0 may represent the key. The parameter λ can be divided into three segments, which can be examined by experiments on the following conditions:

x_0 = 0.3. When $0 < \lambda \leq 3$, the calculation results come to the same value after several iterations without any chaotic behavior[9]. When $3 < \lambda \leq 3.6$, the phase space concludes several points only, the system appears periodicity. While $3.6 < \lambda \leq 4$, it becomes a chaotic system with periodicity disappeared. So we can draw the following conclusions: (1) The Logistic map does not satisfy uniform distribution property. When $0 < \lambda \leq 3.6$ the points concentrate on several values and could not be used for encryption purpose.(2) Cryptosystems based on Logistic map has small key space and weak security [8,9].

3.Wavelet Packet Transform

The fundamental idea behind wavelets is to analyze the given signal according to scale. wavelet packets are particular linear combinations of wavelet [10]. They form the bases which retain many of the orthogonality, smoothness, and localization properties of their parent wavelets. The coefficients in the linear combinations are computed by a recursive algorithm making each newly computed wavelet packet coefficient sequence the root of its own analysis[11,12].

In wavelet analysis (as see in fig.2), a signal is split into an approximation and a detail. The approximation is then itself split into a second-level approximation and detail, and the process is repeated. For an n-level decomposition, there are n+1 possible ways to decompose or encode the signal. in wavelet packet analysis, the details as well as the approximations can be split. This yields a number equal to 2^(2^n-1) different ways to encode the signal [13].

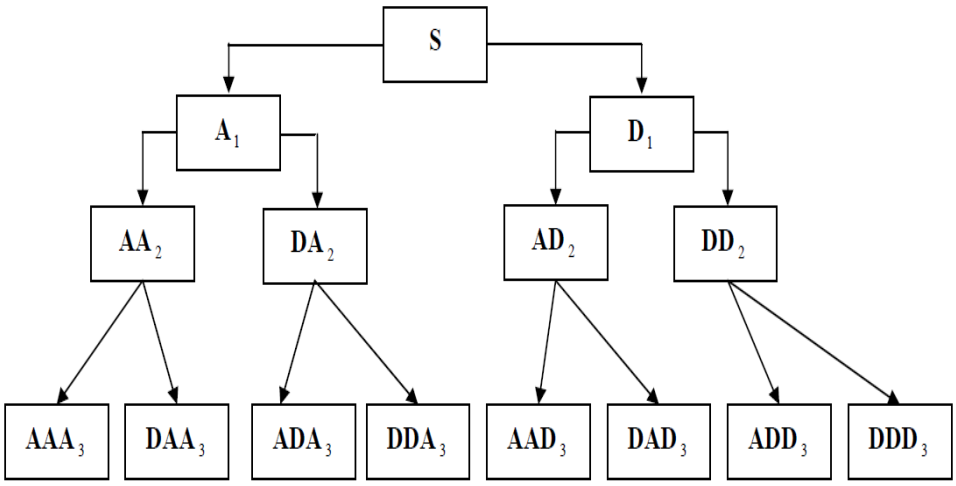

Fig.2 :WPT decomposition tree

4.Blowfish Algorithm

Blowfish is a symmetric block cipher that can be effectively used for encryption and safeguarding of data. It takes a variable-length key, from 32 bits to 448

bits, making it ideal for securing data. *Blowfish* was designed in 1993 by Bruce Schneider as a fast, free alternative to existing encryption algorithms. Data encryption occurs via a 16-round Feistel network. Each round consists of a key dependent permutation, and a key-and data-dependent substitution. All operations are XORs and additions on 32-bit words. The only additional operations are four indexed array data lookups per round[14].

4.1 Sub-Keys Generation :

Blowfish uses a large number of sub-keys. These keys must be pre-computed before any data encryption or decryption. The P-array consists of 18 32-bit sub- keys (P1, P2, … , P18) and there are four 32-bit S-boxes with 256 entries each[14,15] :
S1,0, S1,1, … , S1,255;
S2,0, S2,1, … , S2,255;
S3,0, S3,1, … , S3,255;
S4,0, S4,1, … , S4,255;

The sub-keys are calculated using the Blowfish algorithm. The exact method is as follows:
(1) Initialize first the P-array and then the four S-boxes, in order, with a fixed string. This
string consists of the hexadecimal digits of *pi* (less the initial 3). For example:
P1 = *0x243f6a88*
P2 = *0x85a308d3*
P3 = *0x13198a2e*
P4 = *0x03707344*

(2) XOR P1 with the first 32-bits of the key, XOR P2 with the second 32-bits of the key, and so on for all bits of the key (possibly up to P14). Repeatedly cycle through the key bits until the entire P-array has been XOR with key bits.
(3) Encrypt the all-zero string with the Blowfish algorithm, using the sub- keys described in steps (1) and (2).
(4) Replace P1 and P2 with the output of step (3).
(5) Encrypt the output of step (3) using the Blowfish algorithm with the modified sub-keys.
(6) Replace P3 and P4 with the output of step (5).
(7) Continue the process, replacing all entries of the P-array, and then all four S-boxes in order, with the output of the continuously-changing Blowfish algorithm.
In total, 521 iterations are required to generate all required sub-keys. Applications can store the sub- keys rather than execute this derivation process multiple Times.

4.2 Encryption/Decryption Process:

Blowfish is a Feistel network consisting of 16 rounds (see Fig.3). The input is a 64-bit data element, X. The steps of encryption are as follows[14,15]:
Divide X into two 32-bit halves: XL, XR
For I = 1 to 16
XL = XL XOR Pi
XR = F (XL) XOR XR
Swap XL and XR
Swap XL and XR (Undo the last swap)
XR = XR XOR P17
XL = XL XOR P18
Recombine XL and XR

Function F :
Divide XL into four eight-bit quarters: a, b, c, and d (a,b,c,d are statics size at 8 bits)

F (XL) = ((S1,a + S2,b mod 2^32) XOR S3,c) + S4,d mod 2^32

Decryption is exactly the same as encryption, except that P1, P2, … , P18 are use in the reverse order . The steps of decryption are as follows:
Divide X into two 32-bit halves: XL, XR
For I =18 down to 3
XL = XL XOR Pi
XR = F (XL) XOR XR
Swap XL and XR
Swap XL and XR (Undo the last swap)
XR = XR XOR P2
XL = XL XOR P1
Recombine XL and XR

In the proposal algorithm The input is 256 data element, so the blowfish divided its into two halves and start the blowfish algorithm.

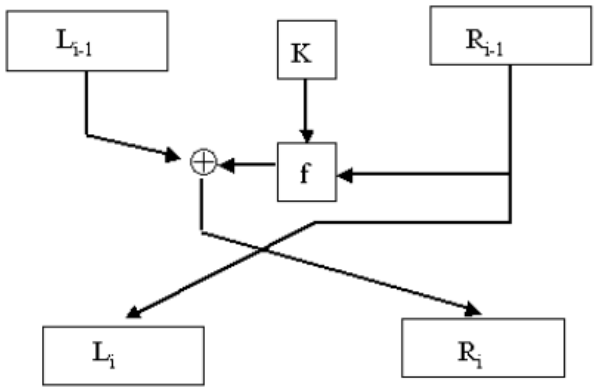

Fig.3 : Feistel Network

5. Measures Of Quality

A number of quantitative parameters can be used to evaluate the performance of the designed system, in term of both reconstructed signal quality after decrypting by using chaotic key and blowfish algorithm. The following parameters are compared: signal to Noise Ratio (SNR), Peak Signal to Noise Ratio (PSNR), Normalized Root Mean Square Error (NRMSE) and Retained Signal Energy (RSE) . the results obtained for the above quantities are calculated using the following formulas[16]:

a. Signal to Noise Ratio (SNR):

$$SNR = 10 * log \frac{\sigma_x^2}{\sigma_e^2} \qquad \text{...(2)}$$

Where σ2x is the mean square of the speech signal and σ2 e is the mean square difference between the original and reconstructed signals.

b. Peak Signal to Noise Ratio(PSNR):

$$PSNR = 10 * log \frac{(NX^2}{||x-r||^2)} \qquad \text{...(3)}$$

Where N is the length of the reconstructed signal, X is the maximum absolute square value of the signal x and ||x−r||2 is the energy of the difference between original and reconstructed signals.

c. Normalized Root Mean Square Error(NRMSE):

$$NRMSE = \sqrt{\frac{(x(n)-r(n))^2}{(x(n)-\mu_x(n))^2}} \qquad \text{...(4)}$$

Where X(n) is the speech signal, r(n) is the reconstructed signal, and μx(n) in the mean of the speech signal.

d. Retained Signal Energy(RSE):

$$RSE = 100 * \frac{||x(n)||2}{||r(n)||^2} \qquad \text{...(5)}$$

Where ||x(n)|| is the norm of the original signal and ||r(n)|| is the norm of the reconstructed one. The retained energy is equal to the L2−norm recovery performance.

6.Mathematical Description or Experimental

6.1 Encryption System Design:

Please submit the sample speech files to encryption it. The speech files are .wav files. These files contain discrete signal value at a sampling frequency of 8KHz for different people (Female and Male). Since the speech files used in this program are of different durations (between 2-10 seconds). In the start we divide speech signal into frames, each frames contain 256 values. Then we try to choose partial frames to encrypted it. To encrypted the chosen speech frames we use the following process :

1.decompose frame by using WPT with the db1 mother wavelet and 2 scale level to find decomposed frame coefficients (s) of the level 2, we have 256 (s) coefficients with i=1,2,3,…,256.

2.used chaotic logistic map and α=0.95 to generate chaotic key (x) :

$x(i+1) = \alpha\, x(i)(1-x(i))$

3.for each frame values (s) xored each value with the chaotic key by using the function as below to find the chaotic encrypted frame (cs) :

$$Cs(i) = \begin{cases} Xor(s(i), key1) & \text{if } x(i) > 0 \\ Xor(s(i), key2) & \text{if } x(i) < 0 \end{cases}$$

Where key1=133,key2=233,i=1,2,3,…,256.

4.extract each chaotic encrypted frame (cs) to two parts (left and right), each part contain 128 chaotic encrypted value, the left value named (csleft), and the right value named (csright).

5.With csleft,csright parts start the blowfish value.

6.connect the two parts right blowfish, left blowfish to make an encrypted frame with 256 value to written it in the encrypted speech signal file.

6.2 Decryption System Design

The decryption of the proposed method also consists of seven Stages. we start with read an encrypted speech signal file. divide the signal in the file into frames, each frames contain 256 values. Then we search about the frames have encrypted because we use partial encryption. To decrypted the chosen speech frames we use the following process :

1.split each frames value into two parts (right and left) : right blowfish, left blowfish ,each part have 128 values. then we send these parts to blowfish algorithm.

2.When we received a decrypted two parts from the blowfish algorithm: Ldcrblowfish, Rdcrblowfish, we odd them into one group to make a decrypted frame (dcs) of 256 value.

3. Remove the chaotic keys from the frame value (dcs) by used the function below to restart the signal ds :

$$Ds(i) = \begin{cases} Xor(Dcs(i), key1) & \text{if } x(i) > 0 \\ Xor(Dc(i), key2) & \text{if } x(i) < 0 \end{cases}$$

4.the restored frame (ds) pass throw IWPT to restored the decrypted frame ds of 256 value to written it in the decrypted speech signal file.

7. Results and Discussion

We describe in fig.4.a the speech signals we have to encrypted it after we choose frames between 100-200 to encrypted it by using the algorithm describe above to have an encrypted signal files (see fig.4.b). Then we try to decrypted it by used the decrypted algorithm describe above to restore the speech signal files(see fig.4.c).

The results obtained to measures of quality the encryption algorithm are describe in the table (1,2) for some speech signal file for the same partial encryption and same durations(2 seconds in table (1)) and (4 seconds in table(2)) .

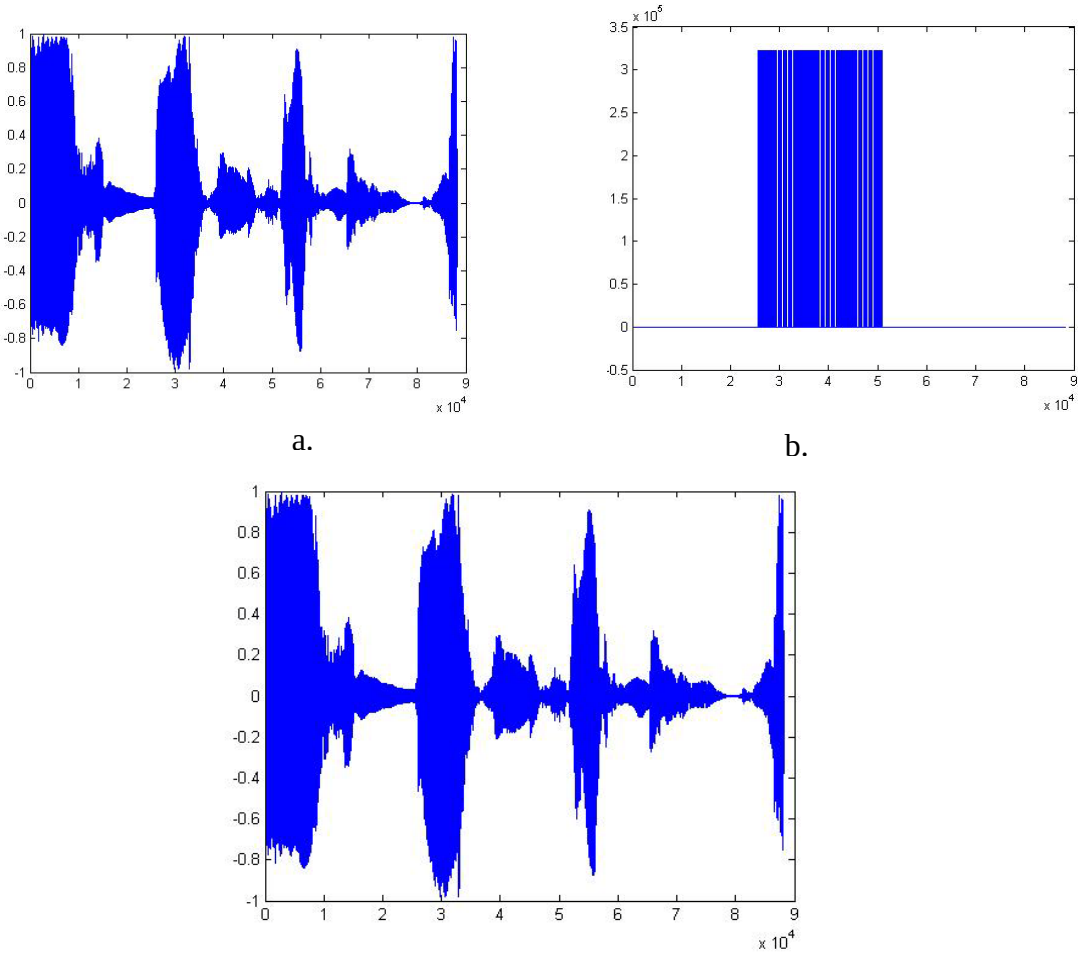

Fig.4 : a. Input Speech Signal, b. Encrypted speech signal, c. decrypted speech signal

Table (1): measures quality of the proposal algorithm for speech signal duration 2 seconds

File name	SNR	PSNR	NRMSE	RSE
s1.wav	32.0365	59.3899	0.0013	100.0620
S2.wav	33.7464	59.7989	0.0012	100.0422
S3.wav	32.8270	59.9148	0.0013	100.0522
S4.wav	33.1516	59.7252	0.0016	100.0484

Table (2): measures quality of the proposal algorithm for speech signal duration 4 seconds

File name	SNR	PSNR	NRMSE	RSE
s1.wav	34.6212	62.8398	0.0009	100.0345
S2.wav	29.4942	58.810	0.0047	100.1125
S3.wav	32.7943	58.1832	0.0023	100.0526
S4.wav	32.2212	59.4964	0.0015	100.0600

8.Conclusion

The human voice is a complex signal and furthermore is the human ear and brain very well trained to understand this signal and has even the ability to cover some losses, which makes it very hard to adulterate a signal with just scramble frequencies so it is not understandable anymore.

Stream ciphers are an important class of encryption algorithms. They encrypt individual characters (usually binary digits) of a plaintext message one at a time, using an encryption transformation which varies with time.

The experimental results have shown that the combination technique resulted in a lower correlation, a higher entropy value, and a more uniform histogram, compared with using the Blowfish algorithm alone, resulting in an enhancement to the security level of the encrypted images. This implies a high similarity and a good quality of the retrieved image compared to the original one. Another feature of the combination technique is its generality; it can be applied with any other traditional algorithm to enhance its performance. relies on the apparent difficulty of solving the computational problems such as Motivated by the fact that the security of many cryptosystems.

We find it faster because we used partial encryption, so we can encrypted and decrypted any speech file faster then we encrypted all the speech file. In all experiments, the attacker cannot obtain the original speech signal unless he knows the encryption key. So, the proposed methods have good security since the key space is very large.

9. References

[1] Qiu-Hua Lin, Fu-Liang Yin, Tie-Min Mei, and Hualou Liang,"A Blind Source Separation Based
Method for Speech Encryption", IEEE Transactions On Circuits and Systems_I: Regular Papers,
vol. 53, no. 6, pp. 1320,(2006).

[2] Purat.m and Noll.p, “Audio Coding with a Dynamic Wavelet Packet Decomposition Based on
Frequency-Varying Modulated Lapped Transforms,” *Proc. IEEE Intern. Conf. Acoust., Speech,*
and Sig. Processing (ICASSP), Vol. 2, pp. 1021,(1996).

[3] Anil Kumar.v, Abhijit Mitra and Mahadeva Prasanna S.R “On the Effectivity of Different Pseudo-
Noise and Orthogonal Sequences for Speech Encryption from Correlation Properties ",
International Journal of Information and Communication Engineering , 4:6,(2008).

[4] Tin Lai Win, and Nant Christina Kyaw,” speech Encryption and Decryption Using Linear
Feedback Shift Register (LFSR) ", World Academy of Science, Engineering and Technology ,
Vol. 48 , pp.462,(2008).

[5] Shubo Liu, Jing Sun, Zhengquan Xu, “An Improved Image Encryption Algorithm based on
Chaotic System", Journal of Computers, Vol. 4, No. 11, pp. 1091,(2009).

[6] Geisel.T, Fairen.v, “Statistical Properties of Chaos in Logistic Map", *Phys. Lett. A*, Vol. 105, pp.
263, (1984).

[7] Baptista M.S, “Cryptography with chaos *“,Phys. Lett. A*, Vol. 240, pp. 50, (1998).

[8] Haojiang Gao, Yisheng Zhang, Shuyun Liang, and Dequn Li, “A new chaotic algorithm for image
encryption ", Chaos Solitons and Fractals 29 ,pp. 393,(2006).

[9] Shamsher Alam .M, Musheer Ahmad, "A New Algorithm of Encryption and Decryption of
Images Using Chaotic Mapping", International Journal on Computer Science and Engineering,
Vol.2(1), pp. 46,(2009).
[10] Walker J. S., "A Primer on Wavelets and Their Scientific Applications", Second Edition,
Chapman & Hall/CRC (2008).
[11] Gerhards R. H.,"Sound Analysis, Modification, and Resynthesis With Wavelet Packets", Ms.c.
Thesis, School Of Engineering Science, Simon Fraser University, (2002).
[12] Iman Q. Abduljaleel,"study of analysis techniques used in automatic Arabic syllable recognition systems", Msc. Thesis, Basra University, Iraq,(2005).
[13] Misiti.M , Misiti.Y, G. Oppenheim and J. Poggi, *Matlab Wavelet Tool Box*, The Math Works
Inc., 2000.
[14] Schneier.B, "The Blowfish Encryption Algorithm – One Year Later," Dr. Dobb's Journal,
September (1995).
[15] Bani Younes M. A. M. , "An Approach To Enhance Image Encryption Using Blockbased
Transformation Algorithm", PHD. Thesis, UNIVERSITI SAINS MALAYSIA,(2009).
[16] Litwin , L.R. "Speech Coding with Wavelets", *IEEE Potentials*, Vol.17, No.2, pp. 38,(1998).

تشفير الكلام باستخدام مفاتيح chaotic map وخوارزمية blowfish

ميساء عبد الكريم و ايمان قيس
جامعة البصرة / كلية العلوم
قسم علوم الحاسبات

الخلاصة :

في الآونة الأخيرة برز الاهتمام في آلية نقل البيانات, سواء كانت بيانات نصية أو صورية أو صوتية. ومن اجل الحفاظ على موثوقية هذه البيانات بعيدة عن أيدي العابثين استدعى الأمر تشفيرها.

في هذا البحث تم استخدام التحويل المويجي Wavelet Packet Transform(WPT) لتحويل الإشارة الصوتية المدخلة من المدى الزمني إلى المدى الترددي. بعد ذلك تم استخدام خوارزمية جديدة تعتمد على مبدأ خوارزمية خرائط logistic chaotic map وخوارزمية blowfish لتشفير البيانات الصوتية المدخلة. استخدام مفاتيح chaotic يجعل الخوارزمية أكثر أمنا وعملية التشفيرافك التشفير أكثر تعقيدا. و اجل ضمان سرعة التشفير\ فك التشفير وكفاءة العمل تم اعتماد التشفير الجزئي من خلال اختيار كل محددة ضمن نطاق الملف الصوتي المدخل. إضافة إلى ذلك اعتمدنا في قياس كفاءة الخوارزمية على استعادة الملف الصوتي المدخل مع الحفاظ على جميع الترددات التي يحتويها من خلال استخدام معاملات SNR, PSNR, NRMSE, RSE .

النتائج التي حصلنا عليها تبين إن الخوارزمية المقترحة تمتاز بالسرعة وكفاءة التشفير وفك التشفير إضافة إلى صعوبة كسرها. وقد تم استخدام برنامج MATLAB بنسخته الثامنة لتنفيذ كافة مراحل المعالجة.