Speech Encryption Technique Based on Bio-Chaotic Algorithm

Asst. Lecturer **Iman Qays Abduljaleel**

Basra University, Basra, Iraq.

Abstract

In today world of advancement, it is mandatory task to share, distribute and exchange the information like image, speech, text files throw public wired/wireless networks. Therefore, security gains more and more importance especially in those organizations where information is more critical and more important. Instead of using the traditional encryption techniques, Biometrics like speech uniquely identifies a person and a secure method for stream cipher, because Biometric characteristics are ever living and unstable in nature. In this paper wavelet packet transform used to decomposition each frame in the speech signal, then present anew algorithm used two steps: (1) addition of noise derived from three chaotic maps (Henon, Logistical, and Ikeda) to the decomposition signal. (2) Chosen bio-chaotic stream cipher which encrypted the speech signal to stored it into the databases to make it more secure by using a biometric key and a bio-chaotic function. In this paper present how to generate the bio-chaotic key by using any chosen frame (each frame is that of 256 sample long) to make it the security key. Chaotic function is used to make the algorithm more secure and make the process of the encryption and decryption more complex. Experimental result of the algorithm shows that the algorithm is faster, stronger and more secure. Use the matlab version of eighth in the different treatments stage.

Key words: Biometric, chaotic map, speech, wavelet packet transform, encryption.

1. Introduction

Speech is one of the most fundamental forms of human communications. Today, due to communications technology, we can sent and received any speech files throw the Internet, but notwithstanding its numerous benefits. To protect the content of digital Speech signal during communication, introduction of the specific encryption systems is usually a must.

Due to some inherent features of speech like high data redundancy, the encryption of speech is different from that of texts; therefore it is difficult to handle them by traditional encryption methods.

The idea of taking advantage of digital chaotic systems to construct cryptosystems has been extensively investigated and attracts more and more attention. Chaotic output signals, which present random statistical properties, are used for both confusion and diffusion operations in a cryptosystem [1].

Recently, some new speech encryption methods including chaotic cryptosystem [2] and encryption using circulant transformations [3] have also been developed.

Biometrics can be used to prevent unauthorized access to cellular phones, PCs, workstations, and computer networks. Recently, biometric based systems of personal identification are receiving considerable interest of research. Various types of biometric systems are being used for real-time identification; the most popular are based on face, iris and speech [4,5,6].

Speech signals change significantly from person to person, compared with the previously mentioned systems, the biometric feature of speech signals is extremely difficult to duplicate. Therefore, that kind of signals is appropriate as a sort of biometric tools for individual identification.

2. Related Concepts

2.1 Wavelet Packet Transform

The wavelet transform is actually a subset of a far more versatile transform, the wavelet packet transform [7], wavelet packet are particular linear combinations of wavelets. They form bases which retain many of the orthogonality, smoothness, and localization properties of their parents 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 tree [8].
In wavelet analysis (as see in figure(1)), 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 equal to 2^(2^n-1) different ways to encode the signal [9].

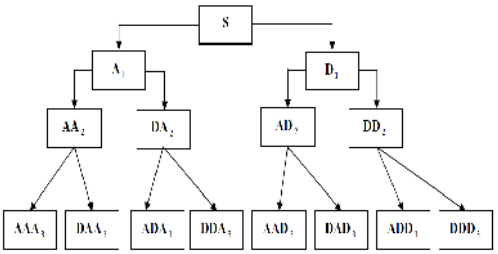

Figure (1) :WPT decomposition tree

2.2 Chaotic map

The chaos-based encryption has suggested a new and efficient way to deal with the intractable problem of fast and highly secure encryption. After Matthews proposed the chaotic encryption algorithm in 1989 [10]. Chaotic systems have many important properties, such as the sensitive dependence on initial conditions and system parameters, pseudorandom property, nonperiodicity and topological transitivity, etc. Most properties meet some requirements such as diffusion and mixing in the sense of cryptography [11]. Therefore, chaotic cryptosystems have more useful and practical applications.

In this paper we dealing with three types of chaotic map as describe below:

2.2.1 Logistic map

The one-dimensional logistic map is proposed by R. M. May [12]. It is one of the simplest nonlinear chaotic discrete systems that exhibit chaotic behavior, defined by the equation [10]:

$$X(k+1) = \lambda * (X(k)) * (1-X(k)) \quad \ldots(1)$$

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

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 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 [13].

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 [13,14].

2.2.2 Henon map

The Henon map is a 2-D iterated map with chaotic solutions proposed by M. Henon (1976) as a simplified model of the Poincare map for the Lorenz model [15]. The Henon map equation is given the following equation:

$$X(k+1) = 1 - a(X(k))^2 + b(Y(k))^2 \quad \ldots(2)$$

$$Y(k+1) = X(k) \quad \ldots(3)$$

Where *a* and *b* are (positive) bifurcation parameters, and *k*= 0,1,2,... The parameter *b* is a measure of the rate of area contraction, and the Henon map is the most general 2-D quadratic map with the property that the contraction is independent of *X* and *Y* [15].

2.2.3 Ikeda map

The Ikeda map is a two-dimensional map, being mathematically expressed as [16]:

$$X(k+1)=1+u(X(k)\cos[t(k)]-y(k)\sin[t(k)]) \quad \ldots(4)$$

$$Y(k+1)=u(X(k)\sin[t(k)]+Y(k)\cos[t(k)]) \quad \ldots(5)$$

Where *u* is a parameter, typically *u*=0.8 and t(k) defined by the equation:

$$t(k)=0.4-(6/(1+x^2(k)+y^2(k))) \quad \ldots(6)$$

3. Proposed Algorithm

Before start the encryption algorithm, we took a speech signal from .wav files. These files contain discrete signal value at a sampling frequency of 8 KHz for different peoples (Female and Male). Since the speech files used in this program are of different durations (between 2-8 seconds).

The proposed algorithm start by dividing the speech signal into blocks of the same size (256 samples) then using WP transformation to decomposition each block in it. After that used algorithm described below to encrypted each block in the speech signal. The basic steps of the algorithm are as follows:

For each block (256 samples) in speech signal Do:

- Using WP transform of mother wavelet db1 and scale level 2, and then put the WP transform coefficient in the vector M of 256 samples.

- A random block selected to create the initial condition for the secret key (B_Key) of 256 sample.

- To make the secret key (B_Key) secure and more stronger we add the logistic chaotic function describe in equation (1) to the secret key to find bio-chaotic key (bkkey).

- Generate a 256 sample Hénon noise signal by the relation describe in (2) and (3) by used a = 1.4 and b = 0.3, for canonical behavior which is chaotic and Put initial values as X(k)=Y(k) = 0.1.

- Generate a 256 sample Ikeda noise signal by the relation describe in (4) and (5) by used u = 0.9 for chaotic behavior and Put initial values as X(k)=Y(k)= 0.1.

- Generate a 256 sample Logistic noise signal by the relation describe in (1) by used X(0) = 0.3 and λ =0.35.

- Generate the noised speech signal by adding Henon (Hn) and Ikeda(Ikn) and Logistic noise (Ln) to each sample in vector M by using the equation:

$$Mn=M+((Hn+Ikn)/Ln) \quad \ldots(7)$$

Where Mn represent the noised speech signal.

- The bio-chaotic key (bkkey) and noised speech signal block (Mn) is then Xored in parallel to generate encrypted speech signal (EncB):

EncB = Mn(1) XOR bkkey(1) ,Mn(2) XOR bkkey(2), ..., Mn(256) XOR bkkey(256) ***…(8)***

- Used inverse WP to reconstructed encrypted speech signal and save it in wav file (i.e. .wav).
The main program used was matlab 8a, and this program describe in appendix (1).In figure (2-6) explain steps used to encrypted female speech signal. In figure (2) we shown the speech signal inputs in time domain after save it in file of type .wav.

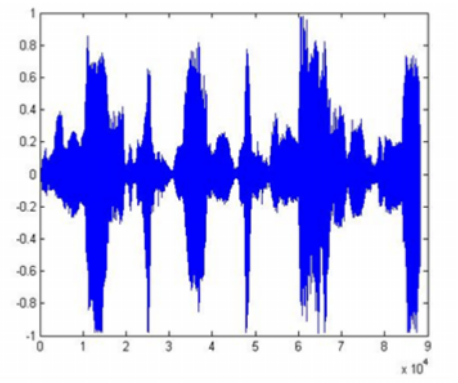

Figure (2) : Female speech signal *in time domain*

In figure (3,4,5) describe logistic , henon, ikeda signal of 256 sample. by used these three types of noised signal to add noise to the input signal.

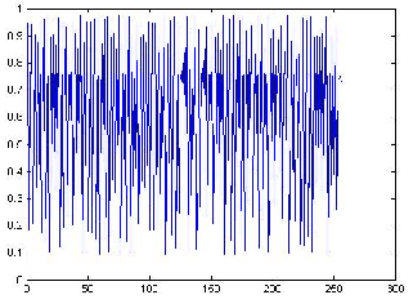

Figure (3) : Logistic noise signal saved in .wav file

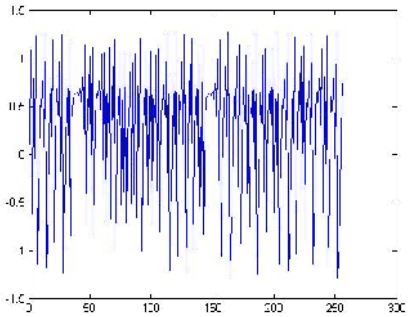

Figure (4) : Henon noise signal saved in .wav file

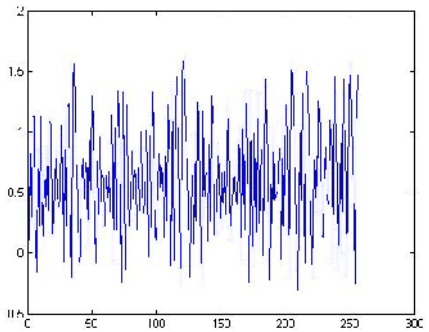

Figure (5) : Ikeda noise signal saved in .wav file

then we used bio-chaotic key to encrypted signal and reconstructed encryption speech signal uses inverse WP transform before save it in file (see figure(6)) .

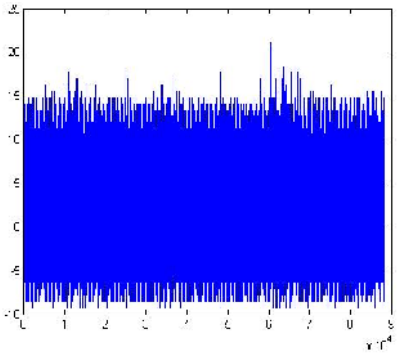

Figure (6) : encrypted speech signal

The decryption process of the used speech signal is carried on by the same way using the same key used for the encryption process but in the opposite direction by reading the encrypted blocks in the codec signal (each block contain 256 sample) and then used WP decomposition tree to restored ciphered speech signal block, then do the following :

1. **Read the initial values of Hénon and Ikeda and Logistic noise and generate respective noise signals.**
2. **The ciphered speech block is Xored with the bio-chaotic key to get the noised speech block back in its original form.**
3. **remove chaotic noises from the speech signal block to restore the WP coefficients block by using the following equation :**

$$DM=EncB-((Ln)/Hn+Ikn) \quad \textit{...(9)}$$

4. **Reconstructed speech signal using inverse WP transform at the same mother wavelet and same scale level used in encrypted stage to restored original speech signal block and then save each decrypted block into decrypted file (see figure (7).**

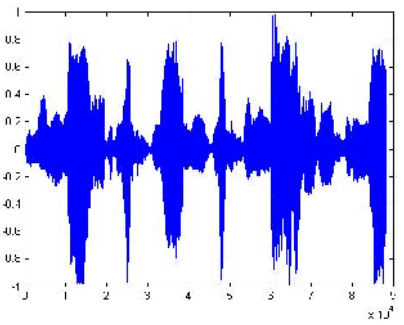

Figure (7) : decrypted female speech signal

4. 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 proposed algorithm. 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[17]:

a. Signal to Noise Ratio (SNR):

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

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):

$$PSNR = 10 * log\frac{(NX^2}{||x-r||^2)} \quad \text{...(11)}$$

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):

$$NRMSE = \sqrt{\frac{(x(n)-r(n))^2}{(x(n)-\mu_x(n))^2}} \quad \text{...(12)}$$

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):

$$RSE = 100 * \frac{||x(n)||2}{||r(n)||^2} \quad \text{...(13)}$$

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.

5. Experimental Results

In Table 1 explain some results of some speech signal for different male and female persons (s1,s2 explain male persons and s3,s4 explain female persons) recorded in natural room and without using any filtering technique and save then in .wav file.

File name	snr	psnr	rse	nrmse
S1	36.3416	58.4441	100.0232	0.0017
S2	36.2058	58.9064	100.0240	0.0015
S3	35.8886	58.8562	100.0258	0.0017
S4	36.0837	58.7604	100.0246	0.0020

Table (1): Experiment result for some input signal

The advantage of uses the proposed algorithms are:

1. Faster execution because of chosen a 256 samples for each encrypted block in each speech signal. We can chose a sample size max than 256 like 512 or 1024 samples but this mean we must used an input file of big size to guarantee segmentation the input file in blocks max than 3 blocks.

2. Uses three types of noised chaotic keys make it difficult to broken.

3. Uses wavelet packet make this proposed algorithm worked with time-frequency features instead of time domain features only.

4. Used biotic key make the chosen key for each file depended on chosen person speech signal.

6. Conclusion

This paper presents a new and novel idea for the encryption and decryption of the speech signals. The proposed algorithm called the Bio-Chaotic Algorithm takes a speech signal (male and female persons) after using WP to decomposition input speech and using three types of chaotic map to noised the speech signal decomposition generates the speech features or the binary bits pattern for the signal Experimental and statistical analysis of the algorithm shows that the algorithm is stronger and more secure. The test speech signal of .wav files. These files contain at a sampling frequency of 8KHz for different peoples (Female and Male) and different durations. By using PSNR,SNR,RSE and NRMSE can compared the quality of proposed algorithm in restore the real speech signal with all frequencies.

For future work we can suggestion to make the biotic key chosen more complex and we can used another chaotic key and a different transform like Fast Fourier or Curvelet transform.

7. References

[1] Abir Awad , Abdelhakim Saadane, "**Efficient Chaotic Permutations for Image Encryption Algorithms**", Proceedings of the World Congress on Engineering, Vol I, ISBN: 978-988-17012-9-9, London, U.K.

[2] K. Li, Y. C. Soh, and Z. G. Li, "**Chaotic cryptosystem with high sensitivity to parameter mismatch,"** *IEEE Trans. Circuits Syst. I, Fundam.*

Theory Appl., vol. 50, no. 4, pp. 579–583, Apr. 2003.

[3] G. Manjunath and G. V. Anand, **"Speech encryption using circulant transformations,"** *Proc. IEEE Int. Conf. Multimedia and Expo*, vol. 1, pp. 553–556, 2002.

[4] Albert Bodo, **"Method for producing a digital signature with aid of a biometric feature",** German patent DE 42 43 908 A1, 1994.

[5] Colin Soutar, Danny Roberge, Alex Stoianov, Rene Gilroy, and B.V.K. Vijaya Kumar, **"Biometric Encryption™ using image processing",** *Proc. SPIE* 3314, pp. 178-188, 1998.

[6] Colin Soutar, Danny Roberge, Alex Stoianov, Rene Gilroy, and B.V.K. Vijaya Kumar, **"Biometric Encryption™ - Enrollment and Verification Procedures",** *Proc. SPIE* 3386, pp. 24-35, 1998.

[7] M. A. Cody, **"The wavelet packet transform",** Dr. Dobb's Journal, Vol. 19, pp. 44-46,50-54, 1994.

[8] V. Wickerhauser, **"Adapted wavelet analysis from theory to software",** AK peters, pp. 213-214,237,273-274,387, Boston, 1994.

[9] M. Misiti, Y. Misiti, G. Oppenheim and J. Poggi, **Matlab Wavelet Tool Box***,* The Math Works Inc., 2000.

[10] Haojiang Gao, Yisheng Zhang, Shuyun Liang, Dequn Li,**" A new chaotic algorithm for image encryption ",** Chaos, Solitons and Fractals 29 ,pp. 393–399,2006.

[11] Zhang LH, Liao XF, Wang XB. **An image encryption approach based on chaotic maps. Chaos**, Solitons & Fractals 2005;24:759–65.

[12] R. M. May, "Simple mathematical model with very complicated dynamics." Nature, vol. 261, pp. 459-467, 1976.

[13] M. Shamsher Alam, 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. 46-50,2009.

[14] Shubo Liu, Jing Sun, Zhengquan Xu, **"An Improved Image Encryption Algorithm based on Chaotic System",** Journal of Computers, Vol. 4, No. 11, pp. 1091-1100, 2009.

[15] M. Henon, **"A two-dimensional mapping with a strange attractor",** Commun. Math. Phys., vol. 50, pp. 69-77, 1976.

[16] Aline Souza de Paula and Marcelo Amorim Savi, **"A Multiparameter Chaos Control Method Applied to Maps",** Brazilian Journal of Physics, vol. 38, no. 4, December, 2008.

[17] L.R. Litwin, **"Speech Coding with Wavelets"**,. *IEEE Potentials*, Vol.17, No.2, pp. 38-41,1998.

تقنية لتشفير الكلام بالاعتماد على خوارزمية bio-chaotic

م.م. إيمان قيس عبد الجليل

جامعة البصرة - كلية العلوم

المستخلص

في عالمنا المتطور اليوم, نلاحظ حاجة للتواصل بين البشر من خلال إرسال واستلام المعلومات سواء كانت صورية أو نصية أو صوتية بواسطة شبكات سلكية\ لاسلكية. لذلك نقل هذه المعلومات تحتاج إلى أمنية تتزايد بتزايد أهمية المعلومات المنقولة. وبدلا من استعمال التقنيات التقليدية في التشفير برز الاهتمام بالخصائص البايلوجية للشخص فمثلا لكل إنسان صوت يميزه عن الأخر وذلك يفرض صفة أمنية إذا ما اعتمد كمفتاح تشفيري سري.

استخدمنا في هذا البحث التحويل المويجي Wavelet Packet لتحليل كل مقطع من مقاطع الصوت المدخل, ثم قدمنا طريقة جديدة للتشفير اعتمدت على مرحلتين هما : (1) إضافة ضوضاء لكل مقطع صوتي محلل علما إن هذه الضوضاء قد اشتقت من ثلاثة أنواع من خرائط chaotic وهي (Henon, Logstic, Ikeda) . (2) اختيار مفتاح تشفير bio-chaotic لتشفير الصوت المدخل وإضفاء أمنية لطريقة التشفير المستخدمة بالاعتماد على الخصائص البايلوجية للصوت البشري ودالة bio-chaotic.

وبواسطة هذه الورقة بينا كيفية توليد مفتاح التشفير bio-chaotic من خلال اختيار مقطع صوتي ضمن الصوت المدخل (كل مقطع عبارة عن 256 قيمة) لجعله المفتاح السري. استخدام دالة chaotic تجعل من الطريقة المقترحة في التشفير وفك التشفير أكثر تعقيد وهذا يبين مدى صعوبة كسر مفتاح التشفير. والنتائج التي حصلنا عليها من استخدم هذه الطريقة بينت قوة وسرعة وصعوبة اختراقها. وقد تم استخدام برنامج matlab في كل مراحل المعالجة.

Appendix(1)

Encrypted Proposed algorithm using MATLAB

```
[y,fs,nbit] = wavread('e:\soundquran\female01.wav'); %%% chosen file
siz = wavread('e:\soundquran\femal01.wav','size'); % determine the size of file
% calculate the number of blocks in input speech signal
Block=1;
i=1;
while i<(siz(1,1))
   j=1;     nnn=i+255;
   for k=i:nnn
      stream(block,j)=y(k);
      j=j+1;
   end
   block=block+1;
   i=i+255+1;
end
block=block-1;
 % generate three types of chaotic key
x0=0.95; a=3.9;
xx0=double(0); xx1=double(0); xx2=double(0);
yy1=double(0); yy2=double(0); xx0(1)=x0;
%% generate logistic chaotic key
for ii=2:256
  xx0(ii)=a*xx0(ii-1)*(1-xx0(ii-1));
end
% generate hanon  key
```

```
a=1.4; b=0.3;
xx1(1)=0.1; yy1(1)=0.1;
for ii=2:256
  xx1(ii)= yy1(ii-1)+1-a*(xx1(ii-1)^2);
  yy1(ii)= b* xx1(ii-1);
end
% generate ikleda key
u=0.9; b=0.3; xx2(1)=0.1; yy2(1)=0.1;
for ii=2:256
  t(ii-1)= 0.4 -(6/(1+xx2(ii-1)^2+yy2(ii-1)^2));
  xx2(ii)= 1+u*( (xx2(ii-1)*cos(t(ii-1)))- (yy2(ii-1)*sin(t(ii-1))));
  yy2(ii)= u*(xx2(ii-1)*sin(t(ii-1))+ yy2(ii-1)*cos(t(ii-1)));
end
%%% execute the proposed algorithm in each block of speech signal
for i=1:block
   for kk=1:256
     x_bit(kk)=stream(i,kk);
   end
   wpt = wpdec(x_bit,2,'db1'); %execute wavelet packet transform
   new_x = read(wpt,'allcfs');
   if i= = chosed_ block    % used bio-key by chosen secure block number
     key_stream=new_x;
     if key_stream(1)>0.5
       yy0(1)=0;
     else
       yy0(1)=1;
     end
     for ii=2:256
```

```
        if key_stream(ii)>0.5
          yy0(ii)=0;
        else
          yy0(ii)=1;
        end
      end
    end
end
key1=133; % secure key1
key2=233; % secure key2
kkn=1;
for i=1:block
    for kk=1:256
      x_bit(kk)=stream(i,kk); %#ok<AGROW>
    end
    wpt = wpdec(x_bit,2,'db1');
    new_x = read(wpt,'allcfs');
    new_stream(i,:)=new_x(:);

    for ii=1:256%%% number of vale the new_x
       dyoooo(ii)=((new_x(ii)+ xx1(ii)+xx2(ii))/xx0(ii));
       y_new(ii)= fix(abs(((new_x(ii)+ xx1(ii)+xx2(ii))/xx0(ii))*10^3));
    end
    %%%% second level encryption
    %%% xor key with block
    kk=1;
    for u1=1:256
       if yy0(kk)= =0
```

```
        y_new2(u1)=bitxor(key1,uint32(y_new(u1)));
      else
        y_new2(u1)=bitxor(key2,uint32(y_new(u1)));
      end
    end
    for u1=1:256
      inc_y(u1)=y_new2(u1)/10^3;
    end
    T1 = cfs2wpt('db1',256,[3 4 5 6]',2,inc_y);
    inc_xreal = wprec(T1); %%% encrypted block
    for cont=1:256
      incrvoice2(kkn)=inc_xreal(cont);
      kkn=kkn+1;
    end
end
wavwrite(incrvoice,44100,16,'e:\soundquran\incvoice.wav');  %saved  encrypted
signal
```