Diyala Journal of Engineering Sciences

ISSN 1999-8716
Printed in Iraq

Vol. 06, No. 03, pp. 1-16, September 2013

KEY GENARATION FORIMAGE SCRAMBLING USING VOICEPRINT

Ahlam H. Shnain
College of Engineering, University of Baghdad
(Received: 20/9/2011; Accepted: 4/3/2012)

ABSTRACT:-This paper presents a new algorithm to scramble color image using voiceprint and linear predicative coding (LPC).

The speech signal pass through pre-processing stage which includes sampling and segmentation into many frames. All frames are windowed using rectangular window and fed to linear predicative predicator, the linear predicator is used to obtain the coefficient of the p^{th} order all-pole vocal tract and it predicts the current sample of the speech signal from linear combination of past samples. Levison Durbin (L-D) procedure is used for each speech frame to find Lp coefficients, reflection coefficients and predictor error.

For scrambling color image, key will be generated manually; by using the LPC coefficient, by ascending all the LPC coefficients and compare each coefficient with all pixels of the color image. When LPC coefficient is similar to the pixel, the pixel will be replaced by that coefficient. So that pixel will be send in random sequence and the color image will be scrambled by using voiceprint (LPC) coefficients. Descrambling will be done in reverse procedure.

Scrambling process is simulated using MATLAB version 7.06.324(R2008a). Many tests are done with different speech signals and color image, SNR, correlation will founded good results.

1- INTRODUCTION

The security of multimedia becomes more important, since data are transmitted over open networks. Typically, reliable security in storage and transmission n of digital speech, images and videos is needed in many real applications, such as play-TV, medical imaging systems, military image data bases as well as confidential video conferences.

Some consumer electronic devices, such as mobile phones, started to provide the function of saving and exchanging digital speech/music data, images and video clips the under the support of

multimedia message services over wireless networks, which is a regently demanding for multimedia security [1].

Secrecy is certainly important to the security or integrity of information transmission. Indeed, the need for secure communications is more profound than ever, recognizing that the conduct of much of commerce, business and personal matters is carried out today through many mediums [2].

2- CONSIDERATIONOF DESIGN SCRAMBLING SYSTEM

There are some considerations that must be taken into account when designing a scrambling system [3].

1. Bandwidth expansion
2. Transmission impairments
3. The residual intelligibility

Key space size is another consideration which represent the number of possible keys that can be used for provide sufficient level of security to scramble signal. If key have large number of elements is sufficiently large that increase key space, it will also not be possible for an interceptor to determine the correct key. If each key consist a few characters, then this limits the number of possible keys, hence the desirability of having a large number of characters per key.

Cryptography evaluates the security of system on the following four attributes: authentication, confidentiality, integrity and availability [4].

The term scrambling has been still used to describe the encryption process to protect voice communication.

3- SCRAMBLINGMETHODS

The scrambling methods are considered as important methods provide the communication systems with a specified degree of security, depending on the used technique to implement the scrambling method.

There are many traditional scrambling methods; some are used in signal dimension such as time or frequency domain scrambling, and others are used in more than one dimension method. To strengthen security, a two-dimensional scrambler is used. Image and speech scrambling are amongst the applications that have benefited most [5].

3.1 LPC Scrambling

It is a method of predicting a sample of a speech signal based on several previous samples. The LPC coefficients can be used to separate speech signal into two parts; the transform function (which contains the pitch and the sound) [6]. The nth sample in a sequence of speech sample may be predicted, it is represented by the weight sum of the previous samples.

$$\hat{s} = \sum_{k=1}^{p} a_k S(n-k) \quad \text{... (1)}$$

The number of samples p is referred as the order of the LPC; p is usually on the order of 10 to 12, which it can provide on accurate enough representation with a limited cost of computation. The weights on a_k (previous samples) are closer in order to minimize the square error between the real sample and its predicted value, thus, the error signal e(n), which is referred at as the LPC residual , would be as small as possible [7].

$$e(n) = S(n) - \hat{s}(n) = \sum_{k=1}^{p} a_k S(n-k) \quad \text{... (2)}$$

The particular source –filter model used in LPC is known as the linear predictive coding model. It has two key components; analysis or encoding and synthesis or decoding. The analysis part involves examining the speech signal and breaks it down into segments or blocks.

Speech coder LPC tend to model two thing excitation and articulation. Excitation is the type of sound which is passed into the vocal tract and articulation is the transformation of the excitation signal into speech [6]. In the proposed algorithm the autocorrelation method is used and one of its solutions is called Durbin's recursive.

3.2 Durbin's recursive

It is a solution method for autocorrelation equations. From eqn. (3) by exploiting the Toeplitz nature of the matrix of coefficients, several efficient recursive procedures have been devised for solving this system of equations. The most efficient method is Durbin's recursive procedure which can be stated as follows [6].

$$E^{(0)} = R(0) \qquad \text{... (3)}$$

$$k_i = \left\{ R_i - \sum_{j=1}^{i-1} a_j^{(i-1)} R(i-j) \right\} \Big/ E(i-1) \qquad 1 \le i \le p \qquad \text{... (4)}$$

$$a_i^{i-1} = k_i \qquad \text{... (5)}$$

$$a_j^i = a_j^{(i-1)} - k_i a_{i-j} \qquad 1 \le j \le i-1 \qquad \text{... (6)}$$

$$E^{(i)} = R(1-k_i^2) E^{(i-1)} \qquad \text{... (7)}$$

Equations (4-7) are solved recursively for i=1, 2…p and the solution is given as

$$a_j = a_j^{(p)} \qquad 1 \le i \le p \qquad \text{... (8)}$$

The process of solving for predictor coefficients for a predictor of order p, the solutions for the predictor coefficients of all order less than p have also been obtained, i.e., $aj^{(i)}$ is the j_{th} predictor coefficients for predictor order [7].

There exist some properties in Durbin's recursive solution are [9]

- More efficient than Gaussian elimination.
- The parameters k_i are PARCOR's (the partial correlation coefficients).

4- KEY MANAGEMENT SYSTEM

Contemporary digital encryption schemes are based on two components; an algorithm that defines the general scheme to be used for protection of the data and a key that makes each instance of the encryption process unique. A major issue in the design of encryption products is how these keys are distributed to each authorized party. This issue is known as key management [10].

Key management can be achieved by physical distribution of keys in some form or other-written form for manual entry into the cryptographic device, electronic form with a corresponding electronic key fill capability or electronic distribution through devices "normal communication paths". In more advanced devices the key can be generated by one device as a part of establishing the connection and transmitted to the other device in some secure way. Alternatively, the public key can be used to achieve secure transfer.

Key exchange is more common than key agreement, but neither method has an overwhelming advantage [10].

A cryptographic key will normally consist of a number of characters which may be in various forms such as alphabetic, alphanumeric or numeric, including binary, octal, decimal and hexadecimal. To obtain a reasonable level of security, the number of possibilities for the complete set of keys must be sufficiently large that it will not be possible for an interceptor to determine in correct key simply by trying all possibilities. If each key consist of only a few characters, then, this limits the number of possible keys.

There are three major problems associated with keys:

- Key generation.
- Key distribution.
- Key management.

4.1 Key Generation

The problem which confronts the user is how to generate his key. It is undesirable to have a sequential method for generating keys, if the interceptor knew the sequential method and then discovered just one key, he would know then all. The most advantage scheme for obtaining keys is to generate them randomly.

4.2 Key Distribution

Once the keys have been generated they have to be distributed to the various receivers and transmitters throughout the systems. If the system is large, or if the key are to be changed frequently, then this is a non-trivial problem. In a secure communications network it is necessary to ensure that all communicators whom share the same key actually have that key in their possession at the appropriate time. More, no one else should have that key. This can be a sizeable logistics problem and if, for instance, it is performed manually, and then it might involve the use of a considerable number of staff.

Key distribution can be expensive, if, for instance, it involve a number of staff carrying keys from one location to another, then it is advisable to provide some means of ensuring that these staff is trustworthy. Furthermore, it may be necessary to provide them with a certain amount of physical protection. Even if the protection required is minimal, the cost of "checking" and protecting the couriers can be considerable.

4.3 Key Management

Key management means the process of keeping accounts on all the keys used in the system. Key management is a complicated procedure which includes, for instance, ensuring that there is a record of precisely which keys are at each terminal at any given moment, that all lists of keys are accounted for (in the sense that none of them is lost; in which case, of course, on would have to assume that the enemy had it) and that all used keys are successfully destroyed. Clearly this is not a trivial task. The user must specify a key management procedure which is compatible with the security level he requires. There is no point what over in deciding that you need a high level of security and failing to control the key management.

5- THE PROPOSED SCRAMBLINGSYSTEM

The computer simulation to construct the scrambling and descrambling techniques (sampling, segmentation…etc) .The proposed algorithm makes for general case to choose the segmentation length, prediction order and color images. The results are taken to different examples from the speech and image signals.

5.1The System Description

The scheme of the suggested key generated for scrambling color image using voiceprint are divided into several stages which consist:

5.1.1 Pre-processing Speech Signal

1- Load speech data (reading wave file).
2- Choose the segmentation length and prediction order.
3- Pre-processing speech signal (sampling, segmentation and framing).
4- LPC coefficients founded using L-D algorithm for each frame after windowing it using rectangular window to avoid overlap.
5- The resulting LPC coefficients is 2-D matrix will be converted into 1-D as a row matrix.
6- Sorting the 1-D row vector in a dc form.

Figure (1) shows the pre-processing of speech signal.

5.1.2 Pre-processing Color Image

The pre-processing is accomplished according to the following

1- Load the color image (read image (3D)).
2- Decompose the read image into R, G, and B components each of 2-D.
3- Resize each component into (256×256) pixel.
4- Co9nvert the decomposed component of R, G, and B into (1-D) as a row vector.

Figure (2) shows the Pre-processing of color image.

5.1.3 Key Generation

Key will be generated from LPC coefficient (before and after) sorting and each pixel of color image as follows:

1- LPC coefficients as row vector (1-D).
2- Sorting (1-D) row vector on descent form.
3- Color image pixels which represented by its component R, G, and B that converted into (1-D) row vector.
4- Each pixel of color image will replaced by LPC (1-D) sorting row vector such that p1→LPC1, p2→LPC2, and so on.
5- Return to LPC coefficient row vector (1-D) before sorting and given each coefficient its pixel number (according to step 4 above) equivalent it.
6- Key will be generated and pixel will be randomly transmitted. Figure (3) shows key generation.
7- (1-D) row vector that represent key will represent the scrambling of original image.

5.1.4 Numerical Example for Key Generation

Take any voice signal and do a pre-processing for this signal (sampling, segmentation, and framing), LPC analysis for each frame to find LPC coefficients, the resulting coefficients will be 2-D, and then convert it to 1-D row vector for example

Step 1: LPC 15 1 3 4 6 2 14 23 17

Then sorting (1-D) row vector in descending form, the sorting LPC coefficients will be

Step 2:↑ 1 2 3 4 6 14 15 17 23

Image will be converted from (2-D→ 1-D) row vector

Step 3: p1 p2 p3 p4 p5 p6 p7 p8 p9

Each pixel will take one LPC coefficient (sorting)

Step 4: 1 2 3 4 6 14 15 17 23

p1 p2 p3 p4 p5 p6 p7 p8 p9

Then return to LPC coefficients before sorting and each coefficient will take pixel will represent it from above step.

Step 5: LPC 15 1 3 4 6 2 14 23 17 Key generation

p7 p1 p3 p4 p5 p2 p6 p9 p8

At last image (pixel) will be transmitted in random sequence that later will be converted from 1-D row vector into 2-D matrix which represent scrambling image.

Hint

Resizing is very important for the purpose of mapping in all sections. Since the data must be converted to a suitable dimensional matrix before sorting for LPC coefficient also image 2-D must converted into 1-D for mapping LPC coefficient and image pixel. Figure (4) illustrate the main procedure of matrix resizing operations for both 1-D vector to 2-D matrix and 2-D matrix to 1-D vector.

6- ALGORITHMOF THESYSTEM

6.1 The Proposed Scrambling System

Speech signals are pre-processing (sampling, segmentation and framing) then LPC coefficients resulting from LPC analysis using L-D procedure. Figure (5) shows flow chart of scrambling color image using voiceprint.

6.2 The Proposed Descrambling algorithm

Descrambling process is very simple and easy. The (1-D) row vector of LPC coefficients after and before sorting will be used also scrambling image.

As in the scrambling process LPC coefficients are compared with LPC coefficients after sorting if there are equal, then reconstruction pixel will equal to scrambling pixel, then new (1-D) row vector is then converted into 2-D matrix to show the reconstruction image. Figure (6) shows the flow chart of descrambling process.

7- PRACTICAL RESULTS

This section will present the practical results obtained by scrambling color image using voiceprint.

7.1 The Tested Speech Signal

The type of the digital speech in pulse code modulation (PCM) and the tested speech samples have 8bit/sample or 16bit/sample. The properties of test wave data are present in table (1).

7.2 The Tested Color Image

The format of image used in the proposed system of size (256×256) pixel. Table (2) gives brief information about images used.

7.3 Specifications of Test Algorithm

7.3.1 Error Rate algorithm

When the error ratio is lower than or equal 0.1, so that construction of the LPC is successful. Original image signal (O) and Descrambled image signal (D)

$$\therefore Error = |D(1) - O(1)| + |D(2) - O(2)| + ... + |D(N) - O(N)| \Big/ size\ of\ descrambled\ stream$$

7.3.2 Signal to Noise Ratio (SNR) Algorithm

If the SNR is greater than zero, so good process, otherwise bad signal

$$SNR = |D(1) - O(1)|^2 + |D(2) - O(2)|^2 + ... + |D(N) - O(N)|^2 \Big/ (D(1))^2 + (D(2))^2 + ... + (D(N))^2$$

7.3.3 Compressor Performance Algorithm

Compression ratio (CR), usually this is less than one.

CR = length of scramble image stream / length of original image stream.

7.4 Numerical Results

The tested speech signal and image signals are shown previously in table (1) and table (2). The results of scrambled and descrambled tests are shown in table (3)

7.5 Graphical Results

The speech signal, image signal, scrambled and descrambled signals are shown in fig. (7).

8- CONCLUSION

Several conclusions based on the results obtained from many tests. These conclusions are based on two different color images, with two different speech signals with different sampling frequency, prediction order of the LPC algorithm.

1- By using LPC (and the combined dimensional scrambling) the scrambling signal becomes more sufficient to transmit.
2- The combination between image and voice signal gives good result when scrambling image in voice but this combination between LPC of the voice signal and pixel of image gives better results comparing with the combination only.
3- From the results obtained the correlation between the original image and the scramble signal leads to good scrambling process.
4- The system delay time depends on many factors: number of input samples per frame, number of frame, and the sampling frequency.
5- The quality of the recovered signal depends on the used method, LPC and the predication order in the LPC is affected on the quality of the recovered signal.
6- From the compression advantage, it gives much higher degree of security, lower bit rate and small size (for storage memory and transmission line).
7- LPC techniques cause time delay and some loss in quality. But they are negligible in terms of cost as compared with the advantages in storage space saving, smaller bandwidth requirement, lower power consumption and small size production.
8- The procedure used in the proposed method is easy and requires simple computation.
9- When the voice signal size become large it will be good in scrambling image since the LPC coefficient will be more and that will more improve results.

9- REFERENCES

1- Li C., "Cryptanalysis of Some Multimedia Encryption schemes", M.Sc. thesis, University of Zhejian, 2005.
2- Haykin S., "communication systems", John Wiley and Sons, Inc., New York, 2001.
3- Kak S. C., "Overview of Analog Signal Encryption", IEEE Proc., Vol.13 Part F, pp.399-404, Augest1983.
4- LaithA.Abdul-Rahaim, Member, IEEE "Proposed Realization of Modified Scrambling Using 2D-DWT Based OFDM Transceivers", MASAUM Journal of Computing, Vol.1, Issue 2, September 2009.

5- Lyerl R., "Image Compression Using Balanced Multiwavelets", M.Sc. thesis, University of State and Virginia Polytechnic Institute, 2001.
6- Emad H. Salman, "Speech signal Scrambling", M.Sc. thesis, University of Baghdad, College of Engineering, Electrical Engineering Department, 2007.
7- Bradbury J., " Linear Predictive Coding", December, 2000.
8- Rabiner L.R., Schafer," Digital Processing of Speech Signal", Prentice Hall Inc., New Jersey, 1978.
9- Sproat R., "Speech Synthesis Methods, Introduction ; Linear Predictive Coding; the Klatt Synthesizer", 2000,
10- Wenbo M.," Modern Cryptography: Theory and Practice", Prentice Hall PTR, New Jersey, 2003.

Table (1): The tested speech samples.

File Name	S1	S2
File type	Wave file	Wave file Window media player
File size byte	4.76MB	6.88MB
File format	PCM	PCM
	8KH	22KH
	16-bit mono	8-bit mono

Table (2): Brief information of the images used in the proposed system.

Image name	Size	Format
Img1 212	1.64MB	JPEG.(jpg)
Img2 waterfall	248KB	JPEG.(jpg)

Table (3): The results of scrambled and descrambled tests.

	Image signal	Voice signal	SNR	Error	CR
Scrambling	Image1	S1	-24.56	0.1394	0.4375
		S2	-28.5	0.0425	0.43813
	Image2	S1	-26.1	0.042357	0.43813
		S2	-25.05	0.13585	0.43751
Descrambling	Image1	S1	4.528	0.04717	0.43775
		S2	3.867	0.04255	0.43752
	Image2	S1	6.568	0.04365	0.4375
		S2	4.34	0.1394	0.43751

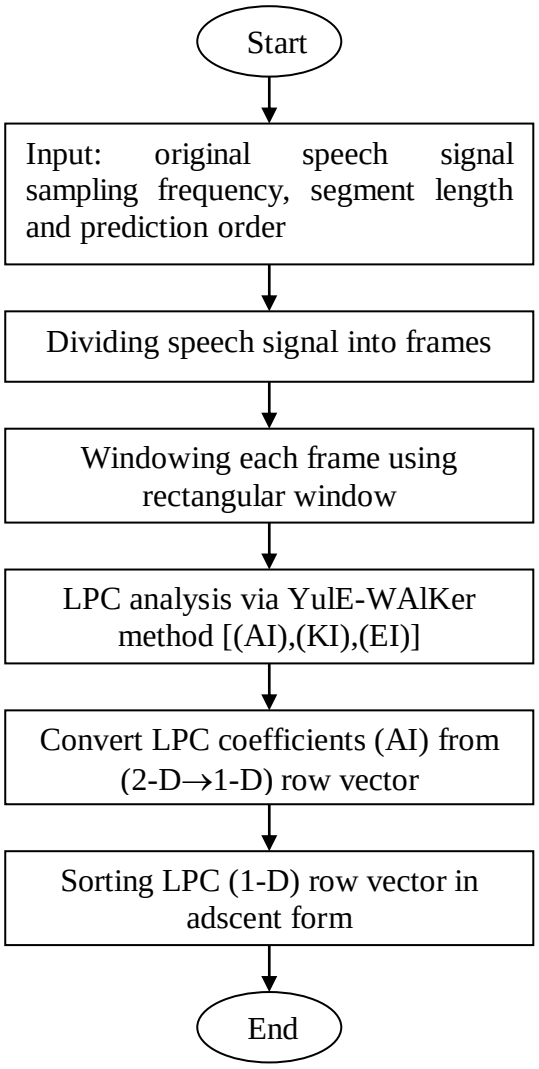

Fig. (1): Speech signal pre-processing

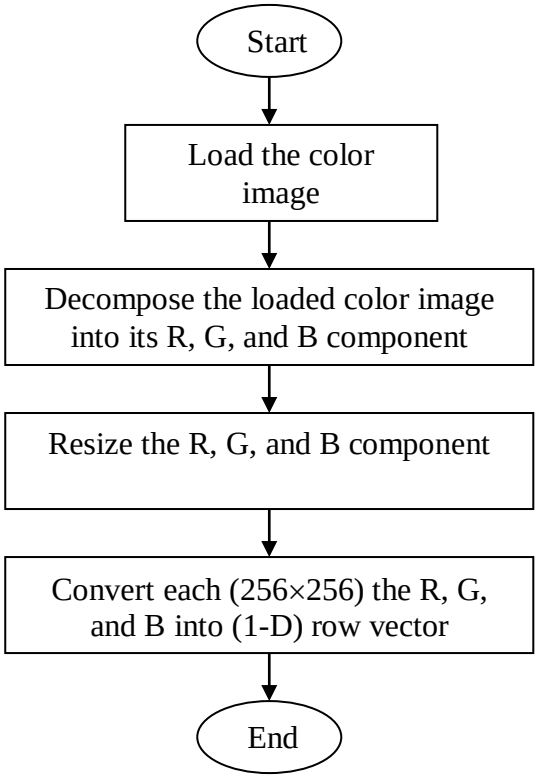

Fig. (2): Pre-processing of color image.

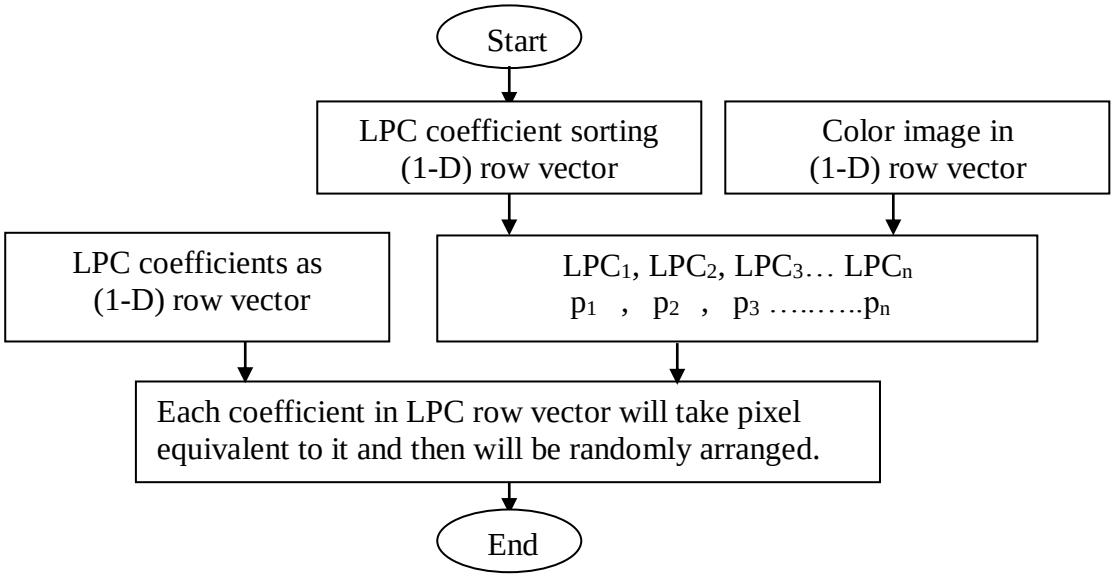

Fig. (3): Key generation.

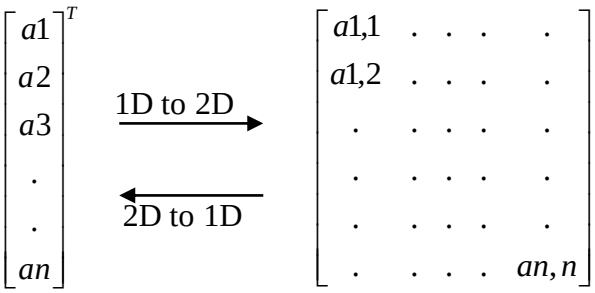

Fig. (4): Graphical illustration of matrix converter operations for both 1D vector to 2D matrix and 2D matrix to 1D vector.

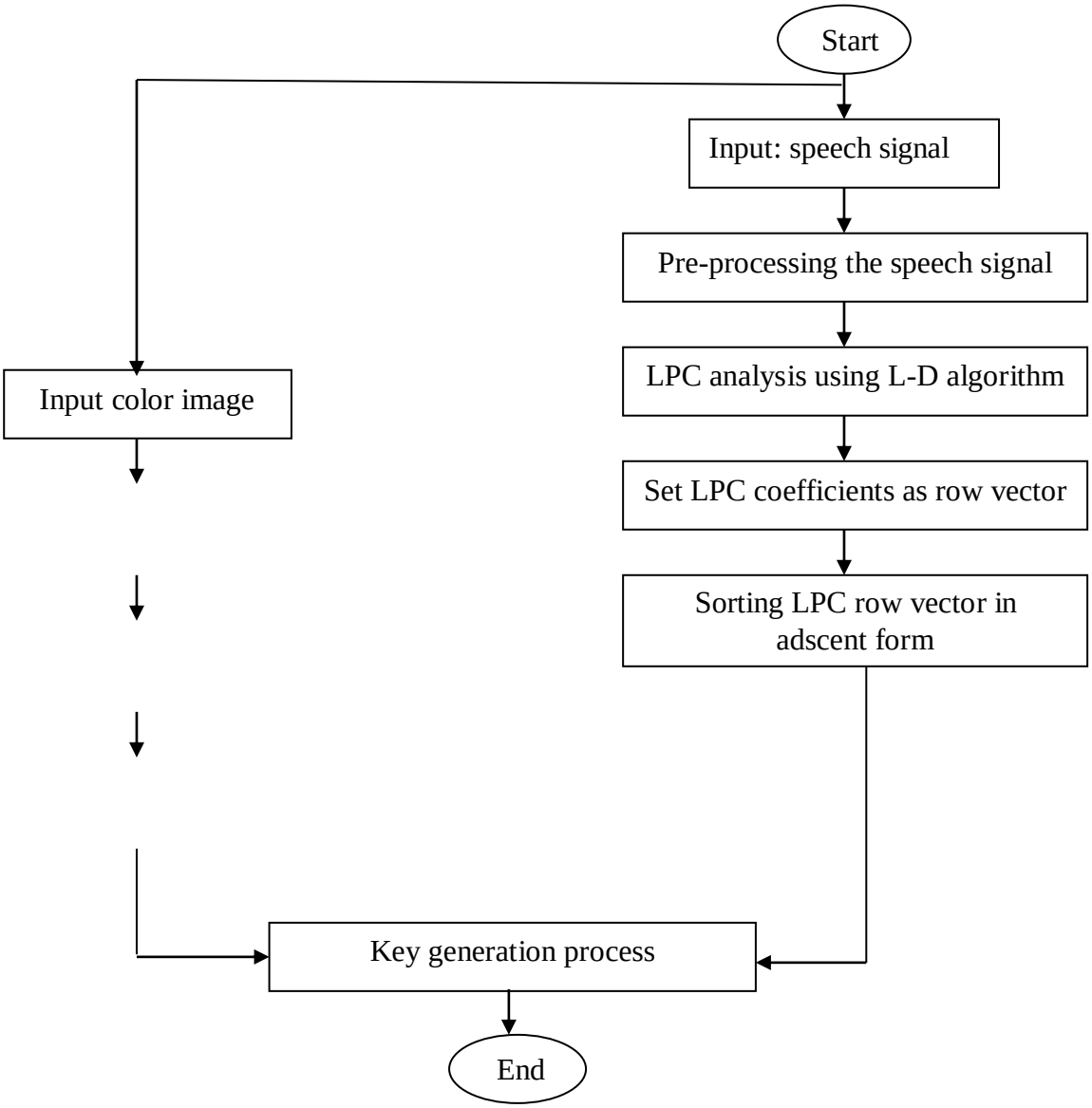

Fig. (5) The proposed scrambling system.

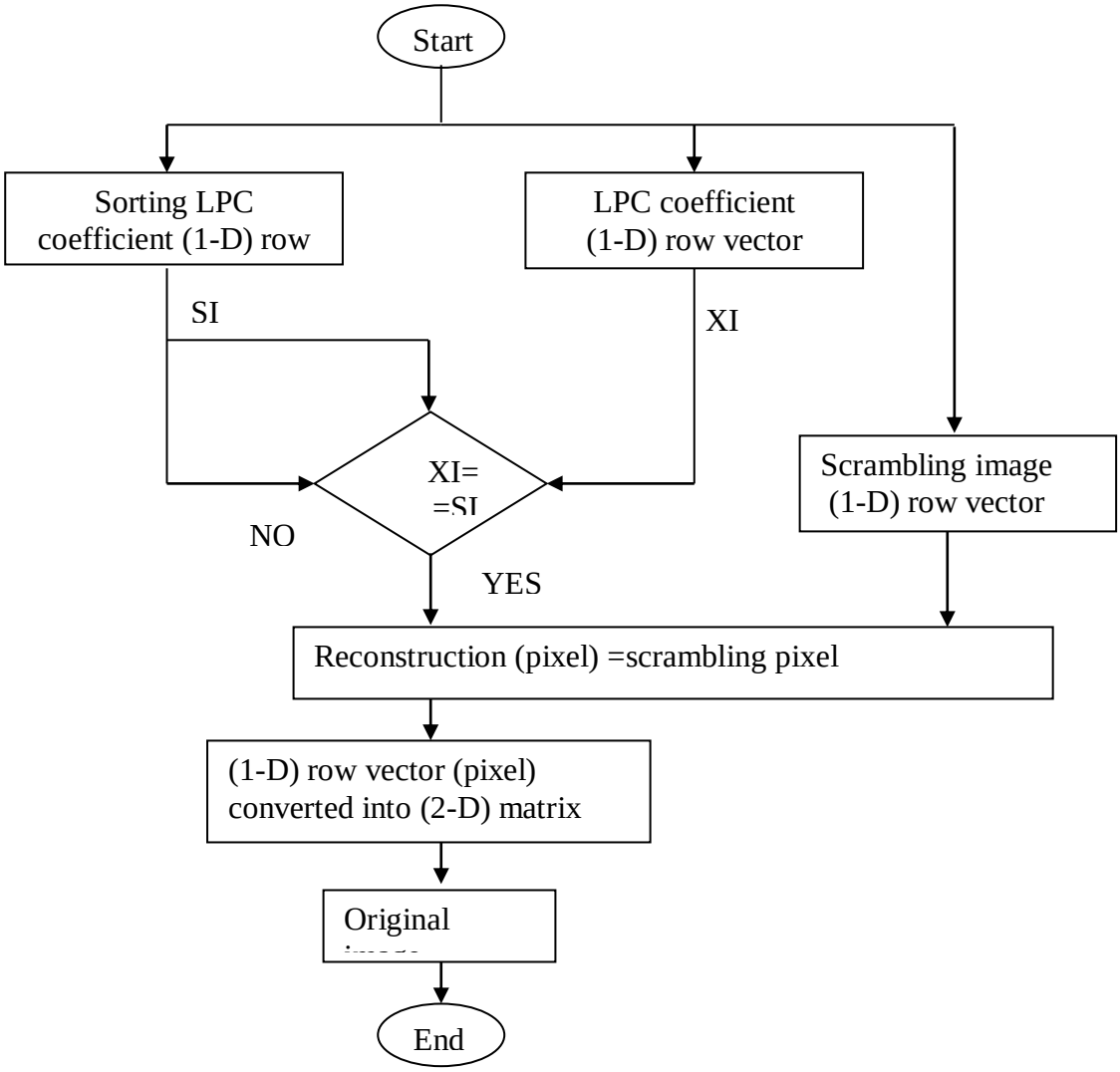

Fig. (6): Descrambling process flow chart.

توليد مفتاح لبعثرة الصورة الملونة باستخدام الاشارة الكلامية

احلام حنون شنين
جامعة بغداد/ كلية الهندسة

الخلاصة

البحث الحالي يقدم منظومة امنة مستندة على طريقة بعثرة الصورة الملونة باستخدام معاملات الرمز الخطي التنبؤي (LPC) للاشارة الكلامية. الاشارة الكلامية التي استخدمت تم تسجيلها في ظروف مختلفة ومن ثم تمريرها الى مرحلة المعالجة الاولية والتي تتضمن مرحلتين (sampling) و (segmentation) لتقسيمها الى اطارات. كل اطار تتم معاملته مع نافذة مستطيلة ومن ثم تمرر الى المرمز الخطي التنبؤي (باستخدام نموذج التنبؤ الارتدادي الغير تلقائي) لايجاد معاملات التنبؤ الخطي للنماذج التي استخدمت. وقد استخدمت خوارزمية (L–D) لحساب معاملات التنبؤ الخطي. اما بعثرة الصورة الملونة فقد تم بأخذ معاملات المرمز الخطي التنبؤي وترتيبها ترتيب تصاعدي ومقارنتها مع كل (pixel) في الصورة الملونة فاذا تشابه وتساوى (pixel) مع احد معاملات المرمز الخطي التنبؤي فيتم استبدال قيمة ال (pixel) مع ذلك المعامل وبهذا فقد تم توليد مفتاح بعثرة الصورة الملونة باستخدام معاملات (LPC) للاشارة الكلامية. تم اجراء عدة اختبارات بأخذ صورتين ملونتين واشارتين كلامية لكل صورة وتم قياس (SNR) وقياس نسبة التشابه بين الصورة الاصلية والصورة المبعثرة.

كل القياسات تمت باستخدام لغة MATLAB version 7.06.324 (R2008a) ونظام تشغيل Windows vista وحاسبة متنقلة شخصية.