International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 4, Issue 2, March-April 2015 **ISSN 2278-6856**

Modify Speech Cryptosystem Based on Shuffling Overlapping Blocks Technique

Dr. Hala B.Abdul Wahab[1], Sundus I. Mahdi[2]

[1] Asst.prof, University of Technology, Computer Sciences Department
Iraq/Baghdad

[2] Ph.D student University of Technology, Computer Sciences Department
Iraq/Baghdad

Abstract

A combination of high efficiency cryptosystem algorithms based on MOBS (Modified Overlapped Block Shuffling) and a HCS (Hybrid Chaotic System) are proposed to secure the transfer of an on-the-go audio signal (i.e. speech). As online voice-based communication is becoming increasingly more common, the need to protect these signals from an unauthorized third party becomes more significant. In natural speech, the values and positions for neighboring samples are highly correlated. The proposed algorithm breaks the correlation by using MOBS and encrypting with a HCS. First, the original speech signal is converted from a one dimensional into a two dimensional array. Then, it is divided into overlapped squared blocks followed by a subsequent permutation. Third, each permutated block is dynamically shuffled using Hénon and Arnold transformation. And finally a Hybrid Chaotic Map (Hénon and Arnold Cat map) is employed to generate a key matrix to encrypt the shuffled blocks, thus producing ciphered speech ready for transmission. Experimental results show that the cryptosystem can successfully encrypt/decrypt with symmetric keys. Experimental analyses like: Signal-to-Noise-Ratio (SNR), Segmental Signal-to-Noise-Ratio (segSNR), Correlation Coefficient Analysis (CCA), Log-Likelihood Ratio (LLR), Residual Deviation, key space and key-sensitivity reveal the effectiveness of the proposed technique for secure speech communication.

Keywords: Speech Encryption, Chaotic system, Arnold Chaotic map, Hénon system

1. INTRODUCTION

Advancements in wireless communications have shifted user reliance away from wired means. This shift has seen an enormous amount of sensitive voice data travel though open and shared networks. Voice-based communication has become more dominant in areas such as the military, VOIP, e-learning, teleconferencing, e-finance, news telecasting etc. These applications thrive on the careful protection of the transferred voice signals, and proper delivery to the concerned party [1]. Encryption is the key to securing transmissions over a vulnerable medium. Speech Encryption [2, 3] is done usually through scrambling, where the speech signal is converted into a meaningless signal. This has commonly been used in speech authentication to conceal secret speech [4], data hiding [5], and so on.

Scrambling is done according to an algorithm, and one of these algorithms is known as a chaotic map. Chaotic maps are nonlinear dynamic systems used to scramble data [6]. Chaos based encryption techniques are considered practical as these techniques provide a combination of speed, high security, complexity, reasonable computational overheads and computational power. Their properties include sensitive dependence on initial conditions and system parameters, pseudo-randomness, non-periodicity and topological transitivity. Most properties meet some requirements such as diffusion and mixing in the sense of cryptography [7]. Therefore, chaotic cryptosystems have more useful and practical applications.

Recently, a number of chaos-based encryption schemes used have been proposed. One of these algorithms, termed "Dynamic Total Shuffling" produces dynamic keys for each block in order to sustain speed and security in the encryption process [8]. Another algorithm divides an input image into overlapping blocks, shuffles image blocks to make the initial encryption, exploits a skew tent map and Arnold transform to generate mask matrices, then conducts exclusive "OR" operations between corresponding elements of each block and a random mask matrix [9]. Chaotic Pixel Shuffling (CPS) encrypts through an algorithm where pixels are scrambled through a chaotic map, while decryption follows a rearrangement of pixels back to their original positions [10]. Tang et al, exploited image encryption strategies using Arnold transform and random strategies [11]. It is achieved by dividing the image into random overlapping square blocks, generating random iterative numbers and random encryption order, and scrambling pixels of each block using Arnold transformation. This algorithm has no size limitation and thus is suitable for encrypting images of any size.

Merazka, introduces a speech encryption method based chaotic cat map algorithm [12], where a cat map is extended into a two-dimensional matrix and used to shuffle signals.

In this paper, the proposed cryptosystem for speech signal is based on (MOBS). A (HCS) Hénon chaotic and Cat chaotic systems are used to shuffle the positions of

samples of the overlapped blocks. The proposed cryptosystem provides a low correlation for the encrypted speech and high security features. HCS combines Hénon maps and Cat maps to shuffle overlapped blocks dynamically, i.e. each block receives different key shuffling, so as to fulfill the purpose of enhanced security. Also, HCS uses different mask keys for each block, so as to eliminate correlation between original and encrypted signals.

This paper is organized as follows:

- Section 1, a brief introduction.
- Section 2 presents a brief overview for chaotic system.
- Section 3 discusses a proposed cryptosystem.
- Section 4 discusses the experimental results and analysis.
- Section 5 presents concludes the findings and proposes a few ideas.

2. CHAOTIC SYSTEM

In this section, a brief overview of two chaotic maps which employed in proposed cryptosystem those are a Hénon chaotic system, and Arnold cat map.

2.1 Hénon Chaotic System

The Hénon map is a discrete-time dynamical system that exhibit chaotic behavior. The Hénon map takes a point (X_i, Y_i) in the plane and maps it to a new point. Nevertheless, the complete picture of all possible bifurcations under the change of the parameters G, H is far from completion. Where G = 1.4, H =0.3, the system is chaotic, subsequently this feature is very useful in image encryption [13, 14].

Hénon Chaotic is described as follows:

$$X_{i+1} = 1 - GX_i^2 + Y_i \qquad (1)$$

$$Y_{i+1} = HX_i \qquad (2)$$

The Hénon chaotic system is converted into one dimensional chaotic system [14], and described as follows:

$$X_{i+2} = 1 - GX_{i+1}^2 + HX_i \qquad (3)$$

2.2 Arnold Cat Map

Arnold cat map is a transformation map, named after the Russian mathematician Vladimir Arnold, who demonstrated its effects in the 1960s using an image of a cat, in matrix notation *Arnold cat map* described as follows [15]:

$$\begin{bmatrix} X_{n+1} \\ Y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & A \\ B & AB+1 \end{bmatrix} * \begin{bmatrix} X_n \\ Y_n \end{bmatrix} mod\ (N) \qquad (4)$$

Where X_n, Y_n is the sample's position in the N-by-N signal matrix so that the range for n is, $\{1, 2, 3, \dots, N\}$, X_{n+1}, Y_{n+1} is the transformed position after applying Arnold cat map, and A and B are two positive integers used as control parameters, which bring chaotic movement. X_{n+1}, Y_{n+1} value is changeable when the control parameters and signal matrix size is variable. Changeable parameters help having dynamic shuffling key to the blocks' samples as well as having dynamic mask key for encryption.

3. THE PROPOSED CRYPTOSYSTEM

The proposed cryptosystem is used for permutation and masking for the wave speech signal in the time domain. Each of the encryption and the decryption performed in a number of iterations which summarized as follows:

1. Convert input speech wave signal from 1D to 2D.
2. Divide signal 2D into overlapping square blocks. Overlapping often increases the amount of zero padding needed. Notice that in figure -1, padding zeros has been added to the right and bottom of the matrix.
3. Generate a key (Key1) by using Pseudo random number generator.

4. First Round

- Permutated the blocks, using permutated Key1.

6. Generate a key (Key2) using Hénon for controls parameters, and a mask key (Key3) using Hénon 1D and Arnold cat map for masking.

7. Second Round

- Generate a permutated key (Key4) using Arnold Cat map which employed Key2 as a new set of control parameter.
- permutated each block samples with a dynamic Key4.
- Generate a new mask key (Key6) using Arnold Cat map which employed Key2 as a new set of control parameter, then applied on Key3.
- Mask each blocks' samples with a dynamic mask Key6

8. Reshape signal 2D into 1D format

The decryption steps for the cryptosystem can be summarized as follow:

1. Reshape encrypted speech signal into 2D format.
2. Divide signal 2D into overlapping square blocks.
3. Generate Key2, Key6 using the same process above. Generate Inverse permutation (P^{-1}) for Key4.

4. First Round

- Mask each block samples with a dynamic mask Key6.
- Permute the outcome block samples with P^{-1} Key4

5. Generate Inverse permutation Key1

6. Second Round

- Permute the blocks with the P^{-1} of Key1.

7. Third Round

- Take off the padding zeros from the signal 2D.

8. Reshape the recovered signal into 1D, and listen.

Where (M, N) represent the width and the height for the input speech signal 2D, (R) represent the blocks' length of the squared overlapped block. a_x is the amount of the overlapping along x-axis, a_y is the amount of the overlapping along the y-axis. b_x, b_y are the number of the blocks along x-axis, and y-axis respectively. For example when 24-by-24 matrix includes blocks with size is 11-by-11 and the over lapping is 3- by-3; the padded matrix becomes a 27-by-27 matrix. The new boundaries of the signal, after padding has been added, are to accommodate the block size.

Now the blocks indexed from top to bottom and left to right as, $block_j, (j=1, 2, \ldots, N_{Blocks})$.

3.1 Permutation

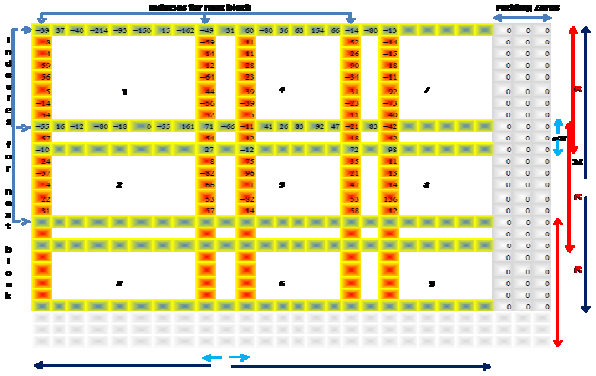

Figure 1 Structure of Overlapped Blocks

Includes generating a key to shuffle the blocks using pseudo-random number generation, the size of the key is the same as the number of the blocks (N_{Blocks}). Since our blocks are overlapped, so avoid overlapped blocks in the swapping between the blocks through the permutation. The speech data have strong correlations among adjacent samples. For speech security and secrecy, one has to disturb this correlation. To achieve this, a block based shuffling scheme is proposed using overlapped techniques.

3.2 Generated a Permutated Key2 and a Mask Key3 using HCS

One more permutation for the blocks' samples by using hybrid Hénon chaotic map and Arnold chaotic map to shuffle the addresses of the scrambled blocks. Each block's samples have a unique key to shuffle the samples. The output from Hénon (Key2) fed into Arnold Cat map (4), as a control parameter to generate new arrangements of Key4. A dynamic Key4 employed to produce a scrambled speech positions for each block to lower the residual intelligibility by disturbing the samples. With all the permutation for the speech signal in the time domain ,still the scrambled speech is not secure because any portion of the signal remain unscrambled will allow a hacker to listen and interpret the scrambled speech. In general, a speech cryptosystem cannot provide sufficient security against eavesdroppers during speech communication with scrambling only.

Mask key generation consist of two steps as the following:

Generating the mask key3 and a set of parameters (A and B) for the Arnold cat map are requisites for the encryption and decryption processes.

Step 1: Generation randomized mask key sized (R*R) by using (HCS): Adopted Hénon chaotic map to produce elements, the minimum iterations of Hénon map should be the same number for the total samples in the block. Since the first few iterations are quite close to each other, therefore the total number for Hénon iteration becomes R^2 +i. discarding the first i^{th} elements to achieve higher randomness, and take the rest to form a secret key using Arnolds cat map. Let *(Key3*) be the mask key and $Key3_{m,n}$ be the elements in the m rows and n column, where m=1,2,…,R and n=1,2,…,R.

Step 2: each block has a unique Key6: Key2 fed into Arnold and applied on Key3 to produce a dynamic Key6. The values of the scrambled samples are changing while exclusive OR operation occurs between the scrambled samples and key6. Combination of shuffling the positions and changing the values of signal samples is introduced to shuffle the relationship between the cipher-speech signal and the original-speech signal. Secret key elements are generated with this formula.

```
y (j)=mod(floor(y(R+j)*2^15),(2^15)-1);
```

4. Experimental Results and Analysis

Several experiments are used to test the encryption for the proposed cryptosystem speech. Designed on MATLAB R2013a for a Windows 7 machine equipped with an Intel CORE i3 Processor, M370@2.40 GHz and 4.00GB of RAM.

The speech signal is encrypted with the proposed cryptosystem and the following results are noticed in Figure 2.Speech Signal Encryption where (a) represent the original speech signal and (b) shows the scramble speech and (c) demonstrate the encrypted speech signal.

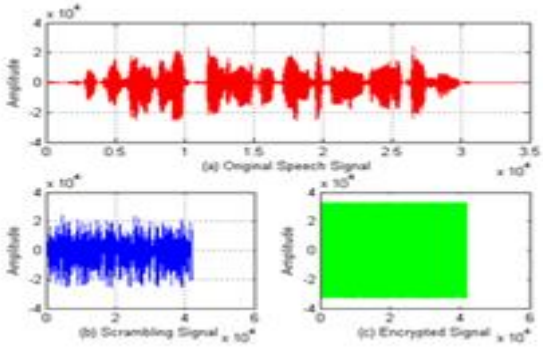

Figure 2 Speech Signal Encryption

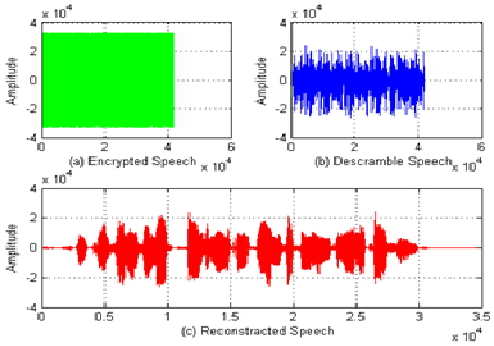

Figure 3 Reconstruct Speech Signal

It is evident that the encrypted speech is obviously similar to the white noise without any talk spurts and the original intonations have been removed, which indicates that no remaining intelligibility that helps the hacker at the communication channel. The decryption process starts from the encrypted speech as shown in Figure 3 and by applying the steps for decryption process, obtained the reconstructed speech.

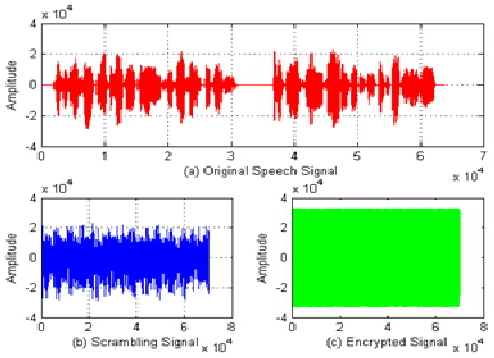

Figure 4 Speech Signal Encryption

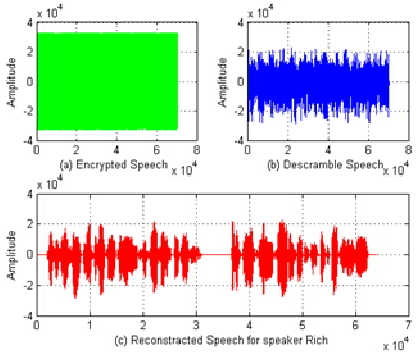

Figure 5 Reconstruct Speech Signal

Figure 4 and Figure 5 demonstrate another speech signal.

4.1 Statistical Analyses

The different types of ciphers signal can be analyze statistically [16] by using.

4.1.1 Signal-to-Noise-Ratio

It is one of the widely used as objective measurement to measure the distortions level of speech cryptography.

$$SNR = 10 * log10 \frac{\sum_{i=1}^{L} x^2(i)}{\sum_{i=1}^{L}[x(i)-y(i)]^2} (dB) \qquad (5)$$

Where x (i) is the original speech and y (i) is the encrypted Where S is the samples number in the block, Nblocks is the number of the blocks in the speech signal where the length of the signal is (L=SNblocks)

4.1.2 Segmental signal-to-Noise-Ratio

The lower segSNR value indicates a higher level of noise in the encrypted file, which making them more resistance to attack

Where S is the samples number in the block, Nblocks is the number of the blocks in the speech signal where the length of the signal is (L=SNblocks).

$$\text{segSNR.} = \frac{10}{N_{blocks}} \sum_{i=1}^{N_{blocks}} log10 \frac{\sum_{i=SN_{blocks}}^{SN_{blocks}+S-1} x^2(i)}{\sum_{i=SN_{blocks}}^{SN_{blocks}+S-1}[x(i)-y(i)]^2} (\text{dB}) \qquad (6)$$

The lower segSNR value indicates a higher level of noise in the encrypted file, which making them more resistance to attack.

4.1.3 Correlation Coefficient Analysis

When the correlation coefficient equal to zero, it means the original signal and the encrypted signal are totally different, so the successful of the encryption process means smaller value of CCA, and the CCA equal to one if they are highly depended as the original and reconstructed speech.

L is the number of the samples.

$$CCA = \frac{cov(x,y)}{\sigma_x \sigma_y} = \frac{\sum_{i=1}^{L}(x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^{L}(x_i - E(x))^2}\sqrt{\sum_{i=1}^{L}(y_i - E(y))^2}} \qquad (7)$$

$$where\ E(x) = \frac{1}{L}\sum_{i=1}^{L} x_i \qquad (8)$$

Table 1 shows the cryptosystem achieves a very low (near to zero) correlation between similar blocks in the original speech and the encrypted speech that gives a good indication for encrypted algorithm.
Lower correlation indicates less similarity between them, which provide more resistance to attacks.
On the other hand, the cryptosystem shows a high (close to one) correlation between original and the reconstructed speech, which provide a high quality for the decryption process as demonstrate in table 2.

4.1.4 A log-Likelihood Ratio (LLR)

It is a distance measure that can be directly calculated from the LPC vector of the clean and distorted speech. LLR measure can be calculated as follows:

$$d_{LLR}(a_d, a_c) = \log\left(\frac{a_d R_c a_d^T}{a_c R_c a_c^T}\right) \qquad (9)$$

Where a_c is the LPC vector for the original speech, a_d is the LPC vector for the synthesized speech, a^T is the transpose of a, and R_c is the auto-correlation matrix for the clean speech.

Table 1: Result of Residual Intelligibility for Encryption Process

Bock Size 25*25 Samples				
Encryption File Name	SNRe	segSNR	rxy	LLR
Mike	-11.7794	-14.5452	-2.30E-03	1.8708
Rich	-11.2823	-13.7147	1.60E-04	2.0878
Keym	-13.3816	-14.3917	-5.64E-04	3.8622
Smm	-13.07	-20.968	-7.42E-04	3.0642

Table 2: Results of Reconstructed Speech Quality

Bock Size 25*25 Samples				
Decryption File Name	SNRe	segSNR	rxy	LLR
Mike	63.069	91.9052	1.00E+00	6.13E-06
Rich	1.1928	17.159	9.99E-01	0.000402
Keym	1.6506	17.241	1.00E+00	3.01E-05
Smm	0.8497	11.8525	1.00E+00	0.0479

4.2 Key Space and Key Sensitivity

One of the important criteria for the performance of the cryptosystem is having a large key space and should be very sensitive to the key value.

4.2.1 Key space

A good encryption scheme should resist most kinds of known attacks, and the key space should be large enough to make brute-force attacks infeasible. In the proposed scheme, the partition pattern is determined by the combination of R, ax, and ay. The correct pattern is almost impossible to guess, so the random partition is an efficient technique. The keys Key1, Key2, Key3, Key4, Key6, the parameters G and H, the initial values x0 and y0 for the Hénon map, and extra parameter A, B of the Arnold cat map, are used as secret keys. The key space is large enough to resist all kinds of brute-force attacks.

4.2.2 Key sensitivity

A good encryption algorithm should be very sensitive to any change in the keys. Any slight changes in the key should result in totally different reconstructed speech at the receiver end as in Figure 6.

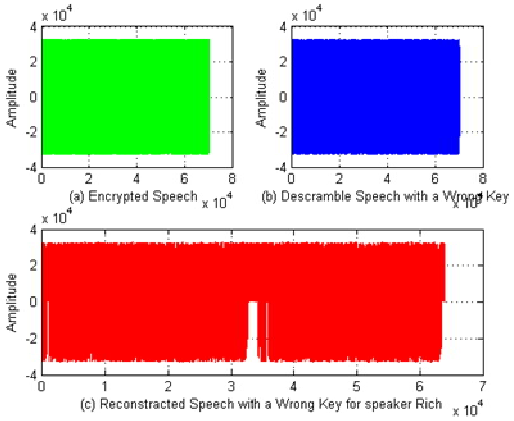

Figure 6 Reconstruct the Speech with a Wrong Key

The above figure has shown by changing the Control parameter from G=1.40000, to G=1.40001 for a Hénon. A completely different reconstructed speech obtained, it's like a noise and can notice that from Table 3 and Table 4 which demonstrate the decryption process with a wrong key.

Results of decryption with a wrong keys show that r is not almost 1and the SNR and segSNR is not positive, which prove the key sensitive

Table 3: Decryption with a wrong Key2

Bock Size 25*25 Samples				
Decryption with Wrong Key2	SNRe	segSNR	rxy	LLR
Mike	-0.8545	-14.8875	-7.70E-03	1.4587
Rich	-0.9741	-14.3109	9.02E-02	1.0788
Keym	-0.627	-14.7844	-4.71E-02	2.2672
Smm	-1.0367	-20.2357	-2.02E-02	2.2594

Table 4: Decryption with a wrong Key3

Bock Size 25*25 Samples				
Decryption with Wrong Key3	SNRe	segSNR	rxy	LLR
Mike	-0.9113	-13.4261	7.90E-01	0.6456
Rich	-1.0358	-13.0588	6.38E-01	0.3989
Keym	-0.6845	-13.5157	7.76E-01	0.9942
Smm	-1.1191	-18.9786	6.72E-01	2.2246

5. CONCLUSION

The purpose here was to evaluate the encryption strength and practical usability of "dynamic keys", that are characteristic of the MOBS system.

Statistical analysis was used to assess the quality of the encrypted and recovered speech. In one hand, it showed that the low correlation coefficient of encrypted speech is

near to the ideal value of 0 and the SNR, segSNR are very low while LLR measure is high which means no residual intelligibility and the encrypted speech are very noisy. This algorithm completely removes the residual intelligibility of the encrypted speech and it is not vulnerable to attack, the obtained values clearly signify the importance of this algorithm in the application of speech encryption.

In the other hand, it demonstrate the high correlations (near to 1), and the SNR, segSNR are increased for the decrypted speech while the LLR is decreased that indicates very good quality of the reconstructed speech signals.

It was concluded that the cryptosystem has shown good results in terms of SNR, segSNR, CCA, LLR. It provided good scrambling as well as good encryption of a speech signal. Security system tests have found it to be robust against statistical attacks and resisted to all type of brute-force attacks.

References

[1] Zhaopin Su, Guofu Zhang and Jianguo Jiang (2012). Multimedia Security: A Survey of Chaos-Based Encryption Technology, Multimedia - A Multidisciplinary Approach to Complex Issues, Dr. Ioannis Karydis (Ed.), ISBN: 978-953-51-0216-8. http://www.intechopen.com/books/multimedia-a-Multidisciplinary-approach-to-complex-issues/multimedia-security-a-survey-of-chaos-based-encryption-technology

[2] E. Mosa, Nagy.W. Messiha, and O.Zahran ,"Chaotic encryption of speech signals in transform domains". International conference on computer engineering &systems; 2009. p. 300–5, 14–16. doi:http://dx.doi.org/10.1109/ICCES.2009.5383252.

[3] M. Ashtiyani, P. Moradi Birgani , S. S. Karimi Madahi, "Speech Signal Encryption Using Chaotic Symmetric Cryptography" . J. Basic. Appl. Sci. Res., 2(2)1678-1684, 2012© 2012, TextRoad Publication

[4] Rupa Patel , Urmila Shrawankar. SECURITY ISSUES IN SPEECH WATERMARKING FOR INFORMATION TRANSMISSION. AMOC2011

[5] Dora M. Ballesteros L, Juan M. Moreno A. "Real-time, speech-in-speech hiding scheme based on least significant bit substitution and adaptive key" Computers and Electrical Engineering 39 (2013) 1192–1203.

[6] Zhenwei Shang Honge Ren Jian Zhang, "A Block Location Scrambling Algorithm of Digital Image Based on Arnold Transformation", in Proc 9th International Conference for Young Computer Scientists 2008, pp 2942-2947

[7] Narendra K. Pareek, Vinod Patidar , Krishan K. Sud, Diffusion–substitution based gray image encryption scheme, Digital Signal Processing 23 (2013) 894–901 www.elsevier.com/locate/dsp

[8] Hala Bahjat, PhD and May A. Salih, "Dynamic Shuffling for Speed Image Encryption" International Journal of Computer Applications (0975 – 8887) Volume 89 – No.7, March 2014

[9] Zhenjun Tang & Xianquan Zhang &Weiwei Lan "Efficient image encryption with block shuffling and chaotic map" #Springer Science+Business Media New York 2014

[10] Manjunath Prasad and K.L.Sudha," Chaos Image Encryption using Pixel shuffling" D.C. Wyld, et al. (Eds): CCSEA 2011, CS & IT 02, pp. 169–179, 2011.© CS & IT-CSCP 2011 DOI: 10.5121/csit.2011.1217

[11] Zhenjun Tang and Xianquan Zhang," Secure Image Encryption without Size Limitation Using Arnold Transform and Random Strategies", JOURNAL OF MULTIMEDIA, VOL. 6, NO. 2, APRIL 2011

[12] Fatiha Merazka, "Efficient speech encryption using chaotic cat map for code-excited linear prediction (CELP) based coders in packet networks" Proceedings of Meetings on Acoustics Volume 19, 2013, http://acousticalsociety.org/

[13] Osama Abu M Zaid, Nawal A El-fishawy, E M Nigm and Osama S Faragallah, "A Proposed Encryption Scheme based on Henon Chaotic System (PESH) for Image Security," International Journal of Computer Applications, USA, Vol. 61, No. 5, 2013, pp. 29-39.

[14] M, Sonls, "Once more on Henon map: analysis of bifurations," Chaos, Sotilons Fractals, Vol. 7, No. 12, 1996, pp. 2215-2234.

[15] Xin Ma,Chong Fu, Wei-min Lei, Shuo Li," A Novel Chaos-based Image Encryption Scheme with an Improved Permutation Process" International Journal of Advancements in Computing Technology Volume 3, Number 5, June 2011

[16] Kondo, K. "Subjective Quality Measurement of Speech, its Evaluation, Estimation and Application" Springer