View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Elsevier - Publisher Connector

Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 93 (2016) 816 – 823

Procedia Computer Science

6th International Conference on Advances In Computing & Communications, ICACC 2016, 6-8 September 2016, Cochin, India

# A Novel Approach for Speech Encryption: Zaslavsky Map as Pseudo Random Number Generator

Farsana F J*[a], Gopakumar K[b]

[a]*Research scholar,LBS Centre for Science and Technology,Kerala University,Trivandrum, India*
[b]*Professor,TKMCollege of Engineering,Kollam,India*

## 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. This paper proposes a new cryptography technique for speech to increases the security of the data meant to be transferred on an insecure medium. The proposed scheme for speech encryption is based on Zaslavsky map and Cat map transform. In this work, the original speech signal is first compressed by discrete cosine transform (DCT) to reduce the residual intelligibility and then the plain data is hidden using random numbers generated using Zaslavsky map. The output data is then processed by Cat map to perplex the data samples so as to make the information unable to understand by an intruder. These two lower dimensional chaotic maps act together to make encryption in higher dimensional space which expands the key space and consequently enhances the security against brute force attack. The resulting system gives more complex dynamical properties proofed with good randomness and unpredictability. Various analyses such as signal to noise ratio (SNR), key space, correlation and brute force attack have been carried out. The analysis shows that the proposed algorithm is computationally simple and efficient compared to conventional higher dimensional chaotic maps. The signal obtained in the proposed technique after decryption at the recipient end is a replica of the original signal which was meant for encryption.

© 2016 Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license
(http://creativecommons.org/licenses/by-nc-nd/4.0/).
Peer-review under responsibility of the Organizing Committee of ICACC 2016

*Keywords:*Speech Encryption;Zaslavsky map;Cat transform;DCT; PRNG.

## 1. Introduction

Voiced based communication becomes prominent in several areas such as corporate and military sectors. Nowadays with the growing demand of information technology security is the major concern in these areas.Encryption is to safeguard the original data from unauthorized access or destruction.Cryptography is the study of information

* Farsana F J. Tel:91-9544288936; fax: +0-000-000-0000 .*E-mail address:*farsanafarooq@gmail.com

1877-0509 © 2016 Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license
(http://creativecommons.org/licenses/by-nc-nd/4.0/).
Peer-review under responsibility of the Organizing Committee of ICACC 2016
doi:10.1016/j.procs.2016.07.302

*E-mail address:*farsanafarooq@gmail.comsecurity like data integrity, authenticationbased on certain mathematical tool or well defined algorithm. Speech Encryption is filling the silent part of the message with noise signal in such a manner that its content can be rebuilt only by a legal recipient. Decryption is the method of reconstructing the original message from the encrypted message (also known as cipher-text).During the past two decades, many researchers had noticed the possibility of using chaos in cryptography. Chaotic functions have subtle nonlinear properties which put together them directly to cryptographical applications. Of special mentions in this conditions are sensitive dependence on initial conditions, topological mixing and deterministic pseudo randomness. Conventionaldigital encryption standards such as AES (Advanced Encryption standard) and DES (data encryption standard) can attain high degree of security[1]. But these encryption schemes experiences brute-force attacks due to lower key space. In real-time communication systems these techniques require long computational time and high computing power which may introduce latency. Also these encryption standards follow complex permutation process with small segment of data. These methods are seldom used in existing speech communication system due to the complexity of algorithms and the expansion in bandwidth of the encrypted data. In this contestchaos-based cryptography provideslow complexity and computationally secure speech encryption techniques[2].

Samah M.H.Alwahbani et al., introduced a method where Logistic map is used for diffusing the samples and one dimensional circle map for confusing the samples[3]. Transform domain cryptography based on two dimensional baker map is discussed by Moa[4]. Three dimensional Lorentz map as a pseudo random number generator is discussed by Rana Saad Mohammed et al.,[5]. Mohammed Salah Azzaz et al., proposed a hybrid Discrete Continuous system, which combines two dimensional Henon map and three dimensional Lorentz maps [6].

In this paper we propose two dimensional deterministic dynamics Zaslavsky map basedPseudo Random Number Generator (PRNG)[7]. Confusion and diffusion are the two basic elements in any cryptographic algorithms. Confusion is the process of rearranging the data sample and it is achieved with Cat transform. Zaslavsky map is given to mask the data sample to form diffusion. In this algorithm encryption in higher dimension is possible by combining two lower dimensional maps such as Cat map and Zaslavsky map. Since the key space is dependent on initial conditions and system parameters, both Cat transform and Zaslavsky map together expands key space and total number of keys. So the new method assures high security against brute force attack. Here the encryption and decryption follows two level processes in lower dimensional space which makes the algorithm computationally simple.

The rest of the paper is organised as follows:Section 2 introduces Zaslavsky map based PRNG. Section 3 deals with proposed methodand section 4 analyze results.Comparison with Advanced Encryption Standard (AES) is discussed in section 5 followed by conclusion in section6.

## 2. Zaslavsky Map Based Pseudo Random Number Generator

The Zaslavsky Map is a discrete-time nonlinear dynamical system introduced by George M Zaslavsky in 1978[8]. It exhibits deterministic dynamic behaviour which is an integral part of the contemporary data encryption algorithms. Two key features of deterministic chaos are the noise-like time series (Pseudo Random Numbers) and the sensitive dependence on initial parameters. Chaotic map based pseudorandom bit generation schemes are important element in confusion of the data samples. In this paper we introduce speech encryption technique based on Zaslavsky map as pseudorandom bit generator. The analysis indicates that the proposed method is suitable for various cryptographic applications. Zaslavsky map is given by following mathematical equations:

$$y_{n+1} = mod(y_n + \nu(1 + \mu z_n) + \epsilon\nu\mu\cos(2\pi y_n), 1) \qquad (1)$$
$$z_{n+1} = e^{-r}\left(z_n + \cos\left(2\pi y_n\right)\right)$$

where $\mu = \frac{1-e^{-r}}{r}$

This map shows chaotic behaviour for the values

$$r = 3.0 \quad \nu = \frac{400}{3} \quad and\ \epsilon = 0.3$$

Before generating the random key streams initial conditions ($y_0$and $z_0$) and bit stream limit($N_s$) are determined. Zaslavskymap (1) is iterated for $N_s$ times. Key stream is generated through pre-processing the values as shown below

$x_i = mod\left(abs\left(integer(z_n * 10^9)\right), 2\right)$

Normalization of the key stream has been done as follows:

$$\bar{x} = \frac{x - x_{min}}{x_{max} - x_{min}} \qquad (2)$$

Where $x_{min}$is theminimum value of the generated key and $x_{max}$is the maximum value of the generated key stream. Normalized random key stream for the initial values $y_0 = 0.587201561347$ and $z_0 = -0.28432144902$ is generated for encryption process in this work.

## 3. Proposed Method

Original speech signal is converted in to cipher text by confusion and diffusion of the data samples with combined Zaslavsky map and Cat transform. The proposed algorithm is illustrated in Fig 1.At the sender part, key stream is generated using two dimensional Zaslavsky scheme. Initial conditions and system parameters of both maps are the key functionwhich is given as the input to the encryptionsystem. Before the encryption process the speech signal is converted to frequency domain by discrete cosine transform. Transform domain method like DCT is preferred over other methods since it has good energy compaction property also provide zero residual intelligibility. Speech scrambles are confused by XOR-ing each speech scrambles with the key stream of Zaslavsky map. Speech scrambles are rearranged or confused through Cat transform.

After the confusion and diffusion process, transformedencrypted speech signal is converted into time domain by inverse cosine transform. Encrypted voice is transmitted through channel after modulation. Retrieval of the original speech signal is carried out at receiver section. The encrypted voice is converted to transform domain by applying DCT prior to the diffusion process. Apply inverse discrete cosine transform to restore the original speech signal.Decryption process has the same structure as the encryption process. The Receiver should generate the same key stream to restore the original signal. Therefore the sender and receiver should be provided with same keys (initial values and control parameters)[9]. Various steps of encryption and decryption processes are explained as follows:

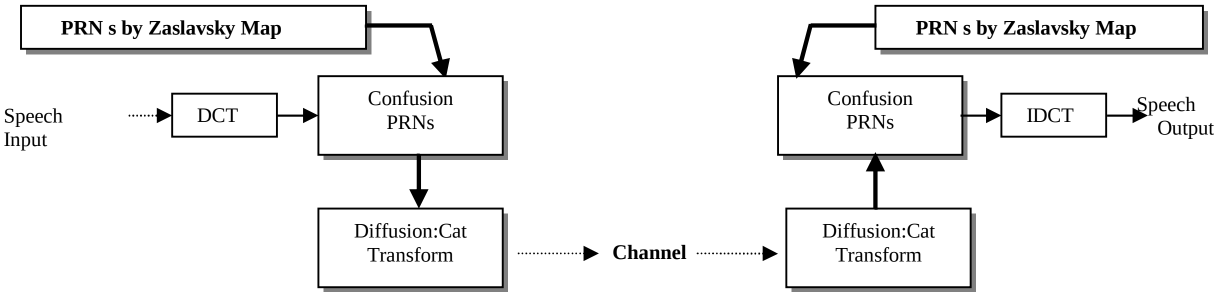

Fig.1. Block Diagram of Proposed Cryptosystem

### *3.1Encryption*

<u>Step 1</u>

Convert the input speech samples to frequency domain by applying discrete cosine transform. Transformed speech scrambles are then converted into its equivalent decimal values by using 16 bit quantization. The processed samples are divided into fixed block size, in which the block size is dependent on the random key size.

<u>Step 2</u>

XOR-ing the speech signal with normalized key generated by Zaslavsky map (section 2)

$$e_i = \bar{x} \oplus m_i$$

$m_i$ and$e_i$ are the original speech samples and encrypted samples respectively.

Step 3

After the first level encryption next level encryption is carried out by applying cat transform. Before applying Cat map-transform, the one dimensional data stream should be converted into two dimensional.

$$\begin{bmatrix} e_{\bar{x}} \\ e_{\bar{y}} \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} e_x \\ e_y \end{bmatrix} mod\ 1$$

Where $e_{\bar{x}}$ and $e_{\bar{y}}$ are the new position and $e_x$and $ey$ are original sample position. Cat transform can be iterated for required number of times. The cat transform parameters are chosen as a=b=c=1 and d=2.

Step 4

Take the inverse discrete cosine transform and transmit the speech sample through the channel after suitable modulation**.**

### *3.2 Decryption*

In this algorithm decryption follows the same procedure as encryption. Receiver section is also provided with the same keythat was used at the transmission side since the chaotic system is very much dependent on initial conditions and control parameters. Decryption process is as follows:

Step 1

Since the two levels encryption process is carried out in transformeddomain.DCT of the received data samples is taken.

Step 2

Apply cat transform to rearrange the data sample as follows

$$\begin{bmatrix} e_x \\ e_y \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} e_{\bar{x}} \\ e_{\bar{y}} \end{bmatrix} mod\ 1$$

Where $e_{\bar{x}}$ and $e_{\bar{y}}$ are the diffused position and $e_x$and $ey$ are rearranged sample position. Also a=b=c=1 and d=2. In this process the number of iterations is same as the receiver used in encryption process.

Step 3

Convert the two-dimensional map to one dimension before applying the ZaslavskyPseudo Random Numbers. Originalspeechsample is retrieved through XOR-ing the encrypted data sample with pseudo random numbers generated inreceiver section

$$m_i = \bar{x} \oplus e_i$$

Step 4

Take inverse cosine transform (IDCT) to get the original speech signal.

## **4. Resultsand Discussion**

In this work we mainly focused on the quality of encrypted and decrypted signal.Various experimental analyses areused to validate the efficiency ofthe proposed speech cryptosystem. It is modeled by MATLAB R2013.For the testspeech files of male and female voice with sampling frequency of 8000samples/second for a duration of 2sec istaken. Fig. 2 shows original, encrypted and decrypted male voice signals.Various analysis are given below:

### *4.1 Key Space*

Key space of the secure encryption system should be large enough to resist different cryptographic attack[10]. Total number of different keys is dependent on key space. Control parameters and all initial conditions determine the key space. $\boldsymbol{y\ (0), z\ (0), \epsilon, r,\ \upsilon}$are initial conditions and system parameters of the Zaslavsky map and $\boldsymbol{a,b,c}$, and $\boldsymbol{d}$ are the system parameters of cat map transform[11]. In this method, signal floating point precision of **$10^{-16}$** is used for secret keys $\boldsymbol{y\ (0), z\ (0), \epsilon, r,\ \upsilon, a,b,c,d}$.Therefore the key space achieved in this scheme is $(10^{16})^9=2^{477}$which is large enough to resist the brute force attack.

### *4.2Signals to Noise Ratio*

Cryptanalyst always strive to minimise the signal to noise signal ratio. Noise performance is the key parameter to measures the information content in the encrypted data. Here the encrypted data is similar to white noise and hence the noise level in the encrypted data is more than that in original speech signal.Combined Zaslavsky and cat transform based algorithm gives better negative signal to noise ratio. It can be calculated as follows:

$$SNR = 10 * log10 \frac{\sum_{i=1}^{N_S} {x_i}^2}{\sum_{i=1}^{N_S} (x_i - y_i)^2} \tag{3}$$

where$x_i$and $y_i$ are the samples of plain and encrypted samples.

### *4.3 Correlation*

Correlation coefficient analysis is statistical measure which indicates the quality of any cryptosystem. This analysis gives the correlation between two or more variables in the original signal and the encrypted signal. If the correlation coefficient is zero, it shows weakest relationship between the original and encrypted signal. The proposed algorithm gives correlation values closer to zero, which validates the excellence of cryptographic process. Correlation can be calculated as follows

$$r_{xy} = \frac{cov(x,y)}{\sigma_x \sigma_y} = \frac{\frac{1}{N_S}\sum_{i=1}^{N_S}\left(x_i - E(x)\right)\left(y_i - E(y)\right)}{\sqrt{\frac{1}{N_S}\sum_{i=1}^{N_S}\left(x_i - E(x)\right)^2}\sqrt{\frac{i}{N_S}\sum_{i=1}^{N_S}(y_i - E(y))^2}} \tag{4}$$

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

$$E(y) = \frac{1}{N_S}\sum_{i=1}^{N_S} y_i$$

In this work five sample files are analysed for correlation and signal to noise ratio. Table 1 shows the various results and it indicates that the proposed method is reliable.

Table 1. SNR and Correlation for various speech files

| Sample files | SNR | Correlation |
|---|---|---|
| A | -22.45dB | 0.000569 |
| B | -23.89dB | 0.000819 |
| C | -21.89dB | 0.000456 |
| D | -24.32dB | 0.000289 |
| E | -22.89dB | 0.000635 |

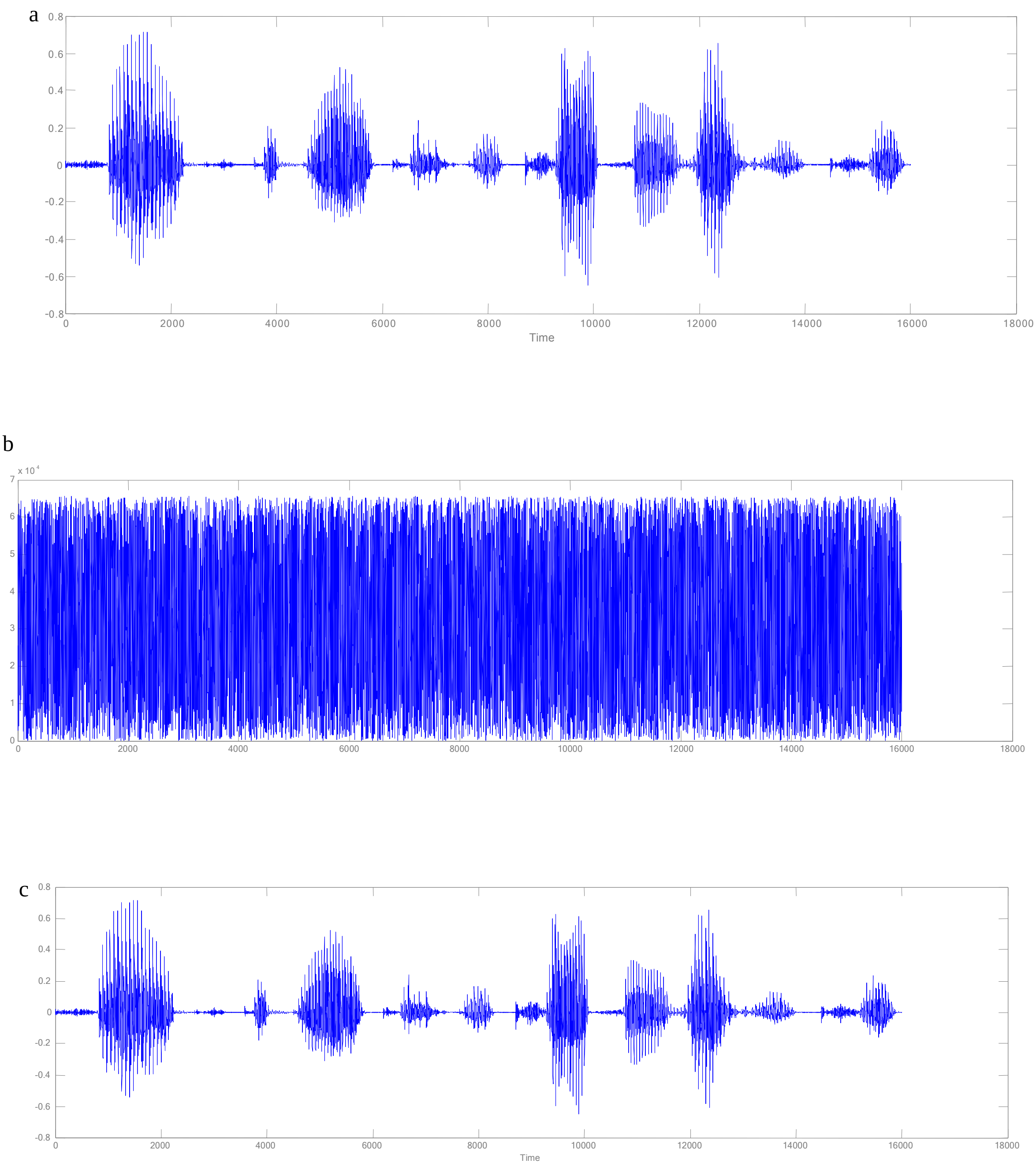
a
0.8
0.6
0.4
0.2
0
-0.2
-0.4
-0.6
-0.8
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
Time
b
x 10^4
7
6
5
4
3
2
1
0
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
c
0.8
0.6
0.4
0.2
0
-0.2
-0.4
-0.6
-0.8
0
2000
4000
6000
8000
10000
12000
14000
16000
18000
Time

Fig. 2. (a) original voice (b) encrypted voice (c)decrypted voice

## 5. Comparison with Advanced Encryption Standard (AES)

AES is the most prominent method [12] existing today. Various performance measures such as key length, number of possible keys, signal to noise ratio, correlation have been discussed. Table 2 shows the comparison between performance measures of proposed method and AES. Key space for the proposed method is found to be 477 bits which is much larger than existing AES scheme. Larger key space is a measure of better encryption. High negative value of SNR obtained in this method shows that signal power is lower than noise power which makes it difficult to detect. Correlation is another measure followed in encryption techniques. Correlation value obtained in our scheme is nearer to zero which shows that original signal and encrypted signals are totally uncorrelated. It can be concluded that the proposed method over rides existing method in most of the performance measures.

Table 2. Comparison between performance measures of proposed method and AES

| Parameters | AES | Proposed method |
|---|---|---|
| Key length | 128,192 or 256 bit | 477 bits |
| Possible Keys | $2^{128,}2^{192}$ or $2^{256}$ | $2^{477}$ |
| SNR | -1.4dB | -23.89dB |
| Correlation | 0.0097 | 0.000236 |

## 6. Conclusion

In this paper, a novel approach for speech encryption scheme based on combined Zaslavsky and Cat transform based four dimensional encryption system is proposed. The proposed chaotic map posses large number of total keys which makes the system safe from brute force attack. Because of above reason, two level encryption processes is sufficient to successfully encrypt the speech scrambles. Therefore the algorithm is computationally simple and highly secure. The experimental results demonstrate that proposed system gives large key space, good correlation and SNR.Performance analysis of proposed method with AES shows that combined Zaslavsky and cat transform based encryption algorithm is better compared with existing advanced encryption standard algorithm

## References

1. D. Ambika and V. Radha,“Secure speech Review” International Journal of Engineering Research and application (IJERA),Vol.2 Issue5 pp.1044-1049 2012.

2. Gonzalo Alvarez, Shujun Li,“Some basic cryptographic requirement for chaos based cryptosystems”, International Journal of Bifurcation and Chaos, 2006.

3.Samah M.H.Alwahbani and Eihab B.M.Bashier, “Speech scrambling based on chaotic maps and one time pad”,Proceedings of IEEE International Conference on computing electrical and electronics engineering,2013.

4.E.Mosa, Nagy.W.Messiha and O.Zahran,“Chaotic encryption of speech signals in transform domain”, Proceedings of IEEE International Conference on computing electrical and electronics engineering, 2010.

5.Sattar B Sadkhan, Rana Saad Mohammed, “A proposed voice encryption based on Random Lorenz map with DCT permutation", International Journal of Advancement in Computing Technology, Vol .7, No3 2015

6. Mohamed Salah Azzaz, Camel Tanougast, Said sadoudi, Ahmed Bouridane, “synchronized hybrid chaotic generators: Application to real time wireless speech encryption”Numerical simulations. Vol 18, issue 8 August 2013, PP 2035–2047,

7.Borislav Stoyanov and Krasimir Kordov “Novel Zaslavsky Map BasedPseudorandom Bit Generation Scheme”Applied Mathematical Sciences, Vol. 8, 2014, no. 178, 8883 – 8887

8.G.M. Zaslavskii (1978). "The Simplest case of a strange attractor". *Phys. Lett. A* **69** (3): 145–147.

9.Xianyong Wu,Zhi-Hong Guan “ A Novel digital Watermark algorithm based on chaotic maps”,physics Letters A 365(2007) 403-406

10.S. Li; X. Mou and Y. Cai, "Pseudo-Random Bit Generator Based on Couple Chaotic Systems and its Applications in Stream Cipher Cryptography", Proc. LNCS, Vol. 2247, PP: 316-329, Springer-Verlag, Berlin, 2001 INDOCRYPT 2001.

11.Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani “New Comparative Study betweenDES, 3DES and AESwithin Nine Factors”.Journal of Computing,Volume 2, Issue 3, March 2010, ISSN 2151-9617.

12.Jawad Ahmad and Fawad Ahmed, “Efficiency Analysis and Security Evaluation ofImage Encryption Schemes”.International Journal of Video & Image Processing and Network SecurityIJVIPNS-IJENS Vol: 12 No: 04