Speech Encryption using Fixed Point Chaos based Stream Cipher (FPC-SC)

Dr. Fadhil S. Hasan
Electrical Engineering Department, University of Mustansiriyah /Baghdad
Email: fadel_sahib@yahoo.com

Received on:2/3/2016 & Accepted on:22/6/2016

ABSTRACT

Fixed point chaos based stream cipher (FPC-SC) is presented in this paper to encrypt the speech signal. Fixed point chaos based pseudo random bit generator (FPC-PRBG) is used as key sequence in stream cipher system. Two chaotic Lorenz and Chen systems are combined to generate Gold FPC-PRBG. The results show that FPC-PRBG has good statistical randomness and encryption performance measure and can be used to produce high speech security level. FPC-PRBG is implemented using Xilinx system generator (XSG) with Xilinx Virtex 4 FPGA device, the system is accessed routed in this device with throughputs 818.64,7978.88 and 780.24 Mbits/sec for Lorenz, Chen and Gold FPC-PRBG respectively, where 40 bits fixed point operation are used.

Keywords: Speech Encryption, Stream Cipher, Fixed Point Chaotic-Pseudo Random Bit Generator, Statistical Randomness Test**,** Runge Kutto**,** Xilinx System Generator.

INTRODUCTION

To prevent unauthorized person from modification and listen through insecure speech channel, certain process are required to protect the speech signal when transmitted through this channel. The process that converts the intelligible speech signal into unintelligible one before transmitted through the channel is called encryption process [1]. There are two types of encryption techniques: analog or scrambling and digital speech encryption. In analog encryption the speech signal is scrambled or permutated either in time or in frequency domain or in both [2]. In digital speech encryption, the signal can be encrypted using digital cryptosystem such as stream ciphers [1,3]. Also encryption can be classified according to key distribution into public and secret key. In the first type, two different keys are used one for encryption which keeps public and the other for decryption which keeps secret. In the secret key encryption, single key is used for both encryption and decryption process [4].

Stream cipher is one type of secret key digital encryption technique in which the streaming data bits is encrypted by bitwise XORed with the stream bits of pseudo random bit generator (PRBG) [4]. It can be designed either as software stream cipher like RC4 [5] or hardware stream cipher like Grain-128 [6]. The main advantages of stream cipher system are more secure that analog encryption [7], faster than block cipher, has no error propagation like block and has high software efficiency [8,9].

PRBG must be designed with high quality of randomness and must be passing the most standards statistical randomness tests [10], Unpredictable with long period [11], low implementation cost and high throughput [12]. In the last years nonlinear dynamic system based chaos becomes more interesting for cryptosystem due to ergodicity, sensitivity to system parameters and initial

https://doi.org/10.30684/etj.34.11A.19
2412-0758/University of Technology-Iraq, Baghdad, Iraq

conditions, aperiodic and random behavior with unpredictable nature [2,13]. Chaos based speech encryption can be classified into analog like chaotic masking [1] and digital chaos like chaos based PRBG [11]. In the last years, different studies to generate Chaos based PRBG (CB-PRBG) were proposed: Addobbo et al. in [14] used one dimensional chaotic map to generate PRBG and enhanced it using efficient post processing technique in [15]. Vinod Patidar et al. proposed PRBG based on two logistic maps [16] and two standard maps [13]. Chen et al. in [12] used a digitalized modified logistic map (DMLM) to produce PRBG and then scrambled using linear feedback shift register (LFSR). Musheer Ahmed et al. [11] used Lorenz and Chen system to generate PRBG. They quantized the chaos signals with suitable pre-processing and then mixed with proposed mixer. After random bit generator, it then used as a key to encrypt speech signal using stream cipher system. Mohamed et al. [17] proposed a post processing technique to scrambled the selection bits of digitized different chaotic oscillators (Lorenz, Chen, Elwakil and Kennedy and Sprott) and check the proposed PRBG for image encryption. HanPing Hu et al. in [18] proposed new PRBG depends on Chen chaotic system where the samples of Chen were coded with suitable coding to generate random sequence.

Chaos Based Pseudo Random Bit Generator

Lorenz and Chen Chaotic System

Chaotic system of one dimensional has some drawback that it has low key space and no strong for adaptive parameter synchronous attack [11]. The higher dimensional chaotic system such as Lorenz [19] and Chen [11] can be used to increase the key space, complexity and enhanced the randomness of pseudo sequence. The differential equation of Lorenz system is described as:

$$\left.\begin{aligned}\dot{x}_1 &= \alpha_1(y_1 - x_1)\\ \dot{y}_1 &= \beta_1 x_1 - x_1 z_1 - y_1\\ \dot{z}_1 &= x_1 y_1 - \mu_1 z_1\end{aligned}\right\} \quad \dots (1)$$

where $(\alpha_1, \beta_1, \mu_1)$ are the positive parameters of Lorenz system and $(x_1(0),y_1(0),z_1(0))$ are the initial conditions. While the differential equation of Chen system is described as [11],[18]:

$$\left.\begin{aligned}\dot{x}_2 &= \alpha_2(y_2 - x_2)\\ \dot{y}_2 &= (\beta_2 - \alpha_2)y_2 - x_2 z_2 + \beta_2 y_2\\ \dot{z}_2 &= x_2 y_2 - \mu_2 z_2\end{aligned}\right\} \quad \dots (2)$$

where $(\alpha_2, \beta_2, \mu_2)$ are the positive parameters of Chen system and $(x_2(0),y_2(0),z_2(0))$ are the initial conditions. Lorenz and Chen exhibit chaotic behavior for the following parameters (16, 45.92, 4)[2] and (35, 28,3)[11], respectively. The three dimensional differential equations of Lorenz and Chen system can be solved using Runge-Kutta method with 4th order (RK4) [20]. RK4 can be summarized as:

Let the differential equation $\dot{x}\,(t)$ =f(*x,y,z*) with initial condition values $x(t_0)=x_0$, $y(t_0)=y_0$ and $z(t_0)=z_0$, then the approximate solution of $\dot{x}\,(t)$ using RK4 is given by:

$$x_{n+1} = x_n + \frac{h}{6}(K_1 + 2K_2 + 2K_3 + K_4), \quad t_{n+1} = t_n + h \quad \dots (3)$$

where x_{n+1} is the RK4 approximation of $x(t_{n+1})$, h is the interval size, and

$$\left.\begin{aligned}K_1 &= f(x_n, y_n, z_n)\\ K_2 &= f\left(x_n + \frac{h}{2}K_1, y_n + \frac{h}{2}K_1, z_n + \frac{h}{2}K_1\right)\\ K_3 &= f\left(x_n + \frac{h}{2}K_2, y_n + \frac{h}{2}K_2, z_n + \frac{h}{2}K_2\right)\\ K_4 &= f(x_n + hK_3, y_n + hK_3, z_n + hK_3)\end{aligned}\right\} \quad \dots (4)$$

RK4 has error per step (h^5) and total accumulated error (h^4).

Fixed Point Chaos Based Pseudo Random Bit Generator (Fpc-Prbg)

Figure (1) shows the block diagram of proposed fixed point chaos based pseudo random bit generator (FPC-PRBG). The differential equation of chaotic system (Lorenz or Chen system) can be solved using signed fixed point RK4 with WL bits word length, FL fractional length and IL integer length (WL=FL+IL)[21]. The initial condition $x(0)$,$y(0)$ and $z(0)$ are either $x_1(0)$, $y_1(0)$ and $z_1(0)$ for Lorenz system or $x_2(0)$, $y_2(0)$ and $z_2(0)$ for Chen system. The three dimension chaotic sequences x_{n+1}, y_{n+1} and z_{n+1} are the output of fixed point RK4 for the (n+1)th step each with 40 bits fixed point. To increase the randomness of each digital output sequence, the bits within each digit (WL bits) must be scrambled. Different approaches can be used for this purpose such as the studies in [15] and [17] that were used post processing technique and study in [12] that was used linear feedback shift register (LFSR). Here LFSR is used to scramble the output of fixed point chaotic system using RK4 because it is simple and efficient method. The scrambling strategy based on LFSR state that the WL bits (v_{n+1}), it is generated using LFSR [22], bit wise XORed with each of the three dimensional output sequence (x_{n+1}, y_{n+1} and z_{n+1}) according to the following equations:

$$\begin{aligned}\tilde{x}_{n+1} &= x_{n+1} \oplus v_{n+1}\\ \tilde{y}_{n+1} &= y_{n+1} \oplus v_{n+1}\\ \tilde{z}_{n+1} &= z_{n+1} \oplus v_{n+1}\end{aligned} \qquad \ldots(5)$$

where $\tilde{x}_{n+1}$, $\tilde{y}_{n+1}$ and $\tilde{z}_{n+1}$ are (n+1)th scrambled sequences. These scrambled sequences are feedback to the input of chaotic system to be initial value for the next sequences and so on. The scrambled sequences of 40 bits are passing through parallel to serial (P2S) to produce stream bits for each sequence. After that the three stream bits are multiplexed to produce the FPC-PRBG stream bits.

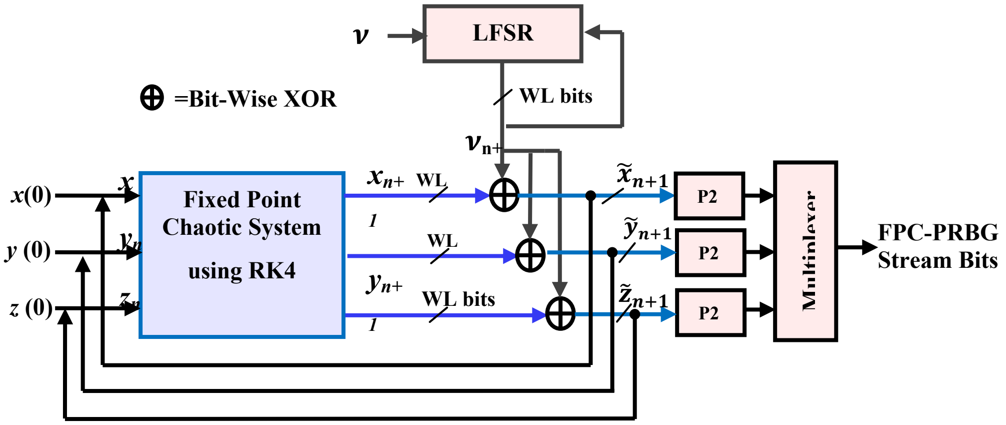


Figure (1) Block diagram of proposed fixed point chaos based pseudo random bit generator (FPC-PRBG)

To generate another family of FPC-PRBG, two or more different of FPC-PRBG can be combined by modulo-2 operation to enhance the security and statistical of the main generator. The idea of this combination is taken from Gold and Kasami sequences [23]. Gold FPC-PRBG is new code sequence that is combined two FPC-PRBGs based on Lorenz and Chen chaotic system respectively. Figure (2) shows the proposed Gold FPC-PRBG based on Lorenz and Chen chaotic system.

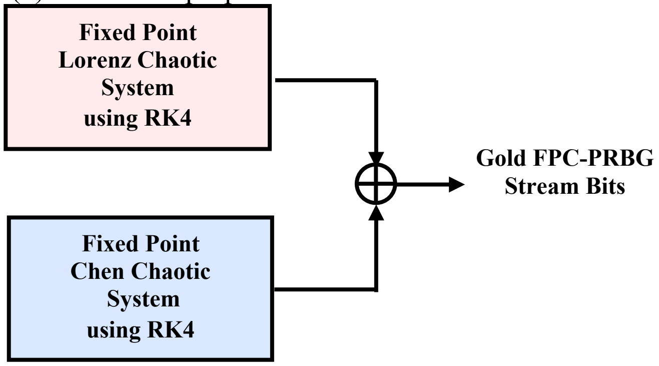

Fixed Point Lorenz Chaotic System using RK4
Fixed Point Chen Chaotic System using RK4
Gold FPC-PRBG Stream Bits

Figure (2) Block diagram of proposed Gold FBC-PRBGbased on Lorenz and Chen system.

Speech Encryption Using Fixed Point Chaos Based Stream Cipher (Fpc-Sc)

Figure (3) shows the proposed block diagram of speech encryption and decryption process using fixed point chaos based stream cipher (FPC-SC) system. The speech signal in the first is recorded with pulse code modulation (PCM) system of 8 KHz sampling frequency and 16 resolution bits for each sample. Pre-processing functions is process to convert the sampled speech signal (s) into positive normalized value ($\breve{S}$) between 0 and (2^{16}-1) according to the following equation [3]:

$$\breve{S} = fix\left(\left(2^{16}-1\right) * \left(\frac{\mathrm{S-Min}}{\mathrm{Max-Min}}\right)\right) \qquad \ldots(6)$$

where *fix*(.) is Matlab function that rounds the element to the nearest integer toward zero. Min and Max are the maximum and minimum value of t e signal (S) respectively. The block P2S is parallel to serial function to convert the 16 bits for each sample into stream bits (B_i) and then XORed with the key stream bits (κ_i), that is generated using FPC-PRBG, to produce ciphering bits (C_i).

$$C_i = B_i \oplus \kappa_i \qquad \ldots(7)$$

The initial key of FPC-PRBG system represents the parameters $(\alpha_1, \beta_1, \mu_1)$ for Lorenz system and $(\alpha_2, \beta_2, \mu_2)$ for Chen system. At the decryption side the ciphering bit is XORed with the identical key stream bits generated in the encryption side and synchronized with it to produce the decryption ith bit ($\widetilde{B_\imath}$).

$$\widetilde{B}_i = C_i \oplus \kappa_i \qquad \ldots(8)$$

After the serial to parallel function, the conversion process is considered to recover the original speech signal. Conversion function is designed in reverse fashion to that of pre-processing function at encryption side.

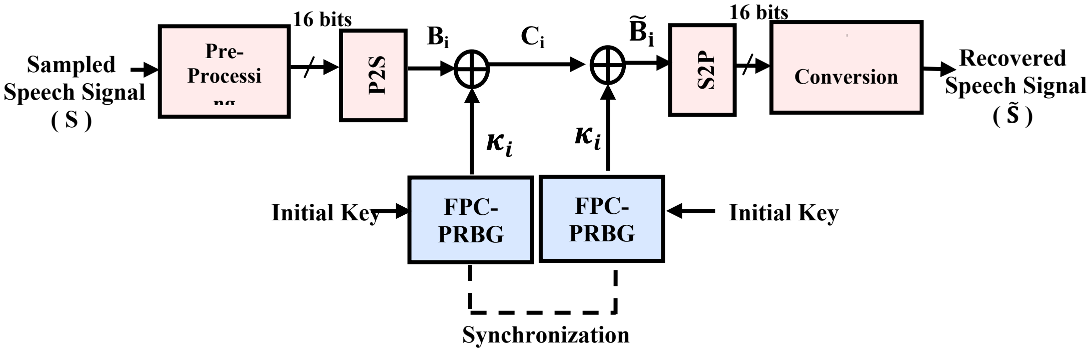


Figure (3) Block diagram of speech encryption system using FPC-SC.

Statistical Tests for Randomness

The main tests that are applied to test the statistical randomness of the proposed FPC-PRBG sequence are frequency, frequency within block, runs, serial, discrete Fourier transform(DFT), cumulative sum, and auto-correlation test. The brief descriptions for each test are summarized below.

Frequency (Monobit) Test:

The test purpose is to check whether the number of zeros and ones in the tested bits sequence are the same in approximately. It is determined as [10]:

$$\mathrm{P_{value}} = \mathrm{erfc}\left(\frac{\left|\sum_{i=1}^{L}(2\kappa_i-1)\right|}{\sqrt{2L}}\right) \qquad \ldots(9)$$

where κ_i are the bits sequence as generated by FPC-PRBG.

L is the length of bits sequence.

| . | is absolute value.

erfc is complementary error function which described as [10]:

$$\mathrm{erfc(r)}=\frac{2}{\sqrt{\pi}}\int_{r}^{\infty} e^{-u^2}\,du \qquad \ldots(10)$$

Frequency Test within a Block

The test purpose is to check whether the frequency of ones in a $\mathcal{M}$ bit block of the tested sequence bits κ_i (i=1,..,L) is approximately $\mathcal{M}/2$. It is determined as [10]:

$$\mathrm{P_{value}} = \mathrm{gammainc}\left(2\mathcal{M}\sum_{i=1}^{\aleph}\left(\frac{\sum_{j=1}^{\mathcal{M}}\kappa_{(i-1)\mathcal{M}+j}}{\mathcal{M}}-\frac{1}{2}\right)^2, \frac{\aleph}{2}\right) \qquad \ldots(11)$$

where $\aleph = fix(\frac{L}{\mathcal{M}})$ is number of block, each block has length $\mathcal{M}\ bits$.

igame is the incomplete gamma function that is defined as [10]:

$$\mathrm{gamminc(r,a)}=\frac{1}{\Gamma(a)}\int_0^r e^{-t}t^{a-1}\,dt \text{ ,and} \qquad \ldots(12)$$

$\Gamma(a)$ is gamma function and it is given by:

$$\Gamma(a) =\int_0^{\infty} t^{a-1}e^{-t}\,dt \qquad \ldots(13)$$

Runs Test

The test purpose is to check whether the number of runs of zeros and ones of various lengths is random sequence expectation. It is determined as [10]:

$$\mathrm{P_{value}} = \mathrm{erfc}\left(\frac{\left|\sum_{i=1}^{L-1}\varphi(i)+1-2L\gamma(1-\gamma)\right|}{2\sqrt{2L}\,\gamma(1-\gamma)}\right) \qquad \ldots(14)$$

$$\text{where } \varphi(i) = \begin{cases}0 & \text{if } \kappa_i = \kappa_{i+1}\\ 1 & \text{else where}\end{cases} \text{ and } \gamma = \frac{\sum_j \kappa_j}{L} \qquad \ldots(15)$$

Serial Test

The test purpose is to check that the number of transition bits of binary sections (00, 01, 10, 11) in the sequence of length L are occurred in the same frequency. It is determined as [24]:

$$\mathrm{P_{value}} = \mathrm{erfc}\left(\frac{4}{L-1}\sum_{i=0}^{1}\sum_{j=0}^{1}N_{ij}^2-\frac{2}{L}\sum_{i=0}^{1}N_i^2+1\right) \qquad \ldots(16)$$

where N_{00},N_{01}, N_{10} and N_{11} are the frequency of the section (00), (01), (10) and (11) respectively. N_0 and N_1 are the frequency of zeros and ones respectively.

Discrete Fourier Transform (DFT) Test

The test purpose is to detect the repetitive patterns are near for each other in the tested sequence. Let H_ℓ is a complex variable that is DFT of the sequence (2 κ_i-1) (i=0,..,L-1 and ℓ=0,..,L/2-1) and is given by:

$$\mathrm{H}_\ell = \sum_{\mathrm{i}=0}^{\mathrm{L}-1}(2\kappa_{\mathrm{i}} - 1)e^{-\mathrm{j}\frac{2\pi\ell\mathrm{i}}{\mathrm{L}}} \qquad \ldots(17)$$

The 95% peak height threshold value T is defined as:

$$\mathrm{T}=\sqrt{\left(\log\frac{1}{0.05}\right)\mathrm{L}} \qquad \ldots(18)$$

Then the DFT test is determined as [10]:

$$\mathrm{P}_{\mathrm{value}} = \mathrm{erfc}\,\left(\frac{(\Omega_1-\Omega_0)}{\sqrt{\mathrm{L}(0.95)(0.05)/2}}\right) \qquad \ldots(19)$$

where $\Omega_0 = \frac{0.95\mathrm{L}}{2}$ is the expected theoretical (95%) number of peaks that are less than T, and Ω_1 is the number of peaks in $|\mathrm{H}_\ell|$ that are less than T.

Cumulative Sums Test

The test purpose is to check whether the cumulative sum of the partial tested sequence is large or small comparing to the cumulative sum expected in random sequence. Let define the partial sums Ψ_ℓ $(\ell = 1,..,\mathrm{L})$ of the sequence (2 κ_i - 1) as [10]:

$$\Psi_\ell = \sum_{\mathrm{i}=1}^{\ell}(2\kappa_{\mathrm{i}} - 1) \ \ , \ell = 1, \ldots, \mathrm{L} \qquad \ldots(20)$$

Then the cumulative sums test is given by [10]:

$$P_{value} = 1 - \sum_{i=(\frac{-L}{\xi}+1)/4}^{(\frac{-L}{\xi}-1)/4}\left[\Phi\left(\frac{(4\mathrm{i}+1)\xi}{\sqrt{\mathrm{L}}}\right) - \Phi\left(\frac{(4\mathrm{i}-1)\xi}{\sqrt{\mathrm{L}}}\right)\right] + \sum_{i=(\frac{-L}{\xi}-3)/4}^{(\frac{L}{\xi}-1)/4}\left[\Phi\left(\frac{(4\mathrm{i}+3)\xi}{\sqrt{\mathrm{L}}}\right) - \Phi\left(\frac{(4\mathrm{i}+1)\xi}{\sqrt{\mathrm{L}}}\right)\right] \qquad \ldots(21)$$

where $= max_{1\leq\ell\leq\mathrm{L}}|\Psi_\ell|$, and

$\Phi(\mathrm{r})$ is standard normal cumulative probability distribution function that is given by:

$$\Phi(r) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{r} e^{-t^2/2}\, dt \qquad \ldots (22)$$

All the above statistical tests will be successful tested if $\mathrm{P}_{\mathrm{value}} \geq 0.01$ and the tested sequence can be considered as random sequence.

Autocorrelation Test

The autocorrelation test is calculated as [24]:

$$\chi^2(\mathrm{d}) = \frac{(\mathcal{R}(\mathrm{d})-\mho)^2}{\mho} \qquad \ldots (23)$$

where $\mathfrak{R}(\mathrm{d}) = \sum_{\mathrm{i}=1}^{\mathrm{L}-\mathrm{d}} \kappa_{\mathrm{i}} * \kappa_{\mathrm{i}+\mathrm{d}}\ ,\ 0 \leq d \leq L-1$, ... (24)

$\mho = \frac{\mathrm{N}_1^2(\mathrm{L}-\mathrm{d})}{\mathrm{L}^2}$, and ...(25)

N_1 is the number of ones in the tested sequence. The test will be successful if $\chi^2(\mathrm{d}) \leq 3.841$.

Objective Quality Measure for Speech Encryption

The most three common objective measures are considered here to evaluate the performance of speech encryption system. These are Log-likelihood Ratio Measure (LLR) [2],[25], frequency weighted segmental signal to noise ratio(SNR) (fwSNRseg) [25] and SNR loss [26]. The brief description of these measures is summarized down.

Log-Likelihood Ration (LLR) Measure

For an original unsecured speech signal with linear predictive coding (LPC) vector, $\vec{\mathrm{a}}_{\mathrm{O}}$, and encryption speech coefficient vector, $\vec{\mathrm{a}}_{\mathrm{E}}$, the LLR measure is defined by [25]:

$$\mathrm{LLR} = \log\left(\frac{\vec{a}_E \mathbf{R}_O \vec{a}_E^T}{\vec{a}_O \mathbf{R}_O \vec{a}_O^T}\right) \qquad (26)$$

where $\mathbf{R}_O$ is the autocorrelation matrix of the original signal and $(.)^T$ is transpose of a vector. The LPC order used in this paper is 10 with frame length 20 ms. [25].

Frequency Weighted Segmental Signal to Noise Ratio (fwSNRseg) Measure

The frequency-weighted segmental SNR (fwSNRseg) is defined as [25]:

$$\mathrm{fwSNRseg} = \frac{10}{N_f} \times \sum_{m=0}^{N_f-1} \frac{\sum_{j=1}^{N_B} W(j,m) \log_{10} \frac{|O(j,m)|^2}{(|O(j,m)| - |E(j,m)|)^2}}{\sum_{j=1}^{N_B} W(j,m)} \qquad \ldots(27)$$

where W(j,m) is the weight placed on the j^{th} frequency band, N_B is the number of bands, N_f is the total number of frames, |O(j,m)| is the spectrum of the original signal in band j at frame m, and E(j,m) is the spectrum of the encryption signal. The spectra |O(j,m)| is calculated by dividing the bandwidth of the signal into 25 bands as listed in Table (1) in [26]. The weighting function W(j,m) can be calculated from the spectrum of original speech signal as [25]:

$$W(j,m) = |O(j,m)|^{0.2} \qquad \ldots(28)$$

Signal to Noise Ratio Loss (SNR_{LOSS})

Jianfen Ma and Loizou in [26] proposed new objective measure that is used to predict the intelligibility of enhanced speech signal in noise environment by measuring the loss in signal to noise ratio between the processed and clean speech signal. This method can be used to sense the level of intelligibility in encryption system. The SNR loss in j^{th} band and m^{th} frame is written as[26]:

$$L(j,m) = log_{10}\left(\frac{|O(j,m)|^2}{|E(j,m)|^2}\right) \qquad \ldots(29)$$

L(j,m) is limited in the range [-3,3] as[26]:

$$\hat{L}(j,m) = \min(\max(L(j,m), -3), 3) \qquad \ldots(30)$$

Then, SNR loss can be mapped to the range of [0,1] as[26]:

$$SNR_{LOSS}(j,m) = \begin{cases} \frac{\hat{L}(j,m)}{-3} & \text{if } \hat{L}(j,m) < 0 \\ \\ \frac{\hat{L}(j,m)}{3} & \text{if } \hat{L}(j,m) \geq 0 \end{cases} \qquad \ldots(31)$$

The average weighted SNR_{LOSS} is calculated by averaging the weighted $SNR_{LOSS}(j,m)$ over all band (N_B) and frames (N_f) as follows [26]:

$$\overline{SNR}_{LOSS} = \frac{1}{N_f} \sum_{m=0}^{N_f-1} \frac{\sum_{j=1}^{N_B} W(j).\, SNR_{LOSS}(j,m)}{\sum_{j=1}^{N_B} W(j)} \qquad \ldots(32)$$

where W(j) is the weight is calculated according to band important functions were taken from Table (1) in [26] where the center frequencies are arranged from 50 – 3597.63 Hz in 25 band.

Simulation Results

The unsecured speech signal that is used in this simulation is the words from one to ten numbers that is sampled at 8000 sample/sec with 2^{16} levels of quantization. The signal duration is 10.85 seconds and all the silence is eliminated from it. Figure (4) shows the unsecured speech signal. The initial and parameter values taken for chaotic systems are ($\alpha_1 = 16, \beta_1 = 45.92, \mu_1 = 4$, $x_1(0)$= -2, $y_1(0)$=-3, $z_1(0)$=6) and ($\alpha_2 = 35, \beta_2 = 28, \mu_2$=3, $x_2(0)$=-1, $y_2(0)$=2, $z_2(0)$=4) for Lorenz and Chen respectively. RK4 method is used to solve the ordinary differential equation of chaotic system with step size h=2^{-7}. A fixed point 2's complement format is used for the numerical solutions of chaotic system with word length= 40 bits and fractional length =24 bits. LFSR scrambling has generator polynomial = [39 8 0]. All the system functions are implemented using MATLAB 7.12 (R2011a).

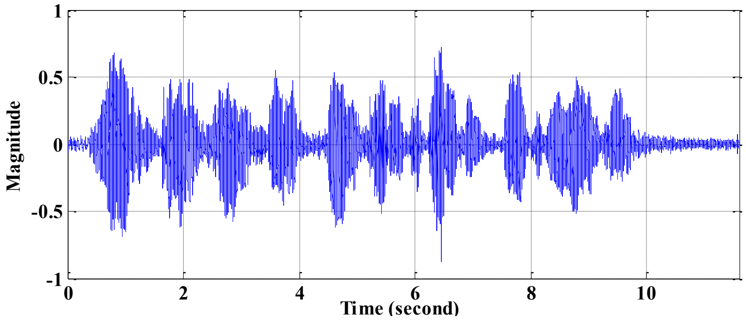


Figure (4) Unsecured speech signal

Statistical Randomness Results

Table (1) shows the statistical randomness tests that are explained in section 4 for Lorenz, Chen and Gold FPC-PRBG. It can be seen that all tests value greater than the threshold level 0.01, therefore the sequences production are random numbers. Also the Gold sequence appears to have good statistical measure compared with Lorenz and Chen based FPC-PRBG. Figure (5) shows the autocorrelation of Lorenz, Chen and Gold FPC-PRBG using Equation (23). The combination of Lorenz and Chen sequence will enhance the autocorrelation characteristic where all values of $\chi^2(d) \leq 3.841$.

Table (1) Statistical randomness tests measure

Randomness Test	P_{value} Lorenz FBC-PRBG	P_{value} Chen FBC-PRBG	P_{value} Gold FBC-PRBG
Frequency	0.5837	0.9506	0.8966
Block Frequency	0.1878	0.2208	0.9312
Runs	0.4052	0.4378	0.5141
Serial	0.8389	0.6098	0.998
DFT	0.8203	0.805	0.9483
Cumulative Sum	1	1	1

Speech Quality Measure Results

The objective measures explained in section 5 can be used to test the quality performance of speech encryption signal compared with original unsecured speech signal. Table (2) shows the results when Lorenz, Chen and Gold FPC-PRBG are used as key stream in FPC-SC system. Also in the same table the objective measure results for the decryption speech signal with the correct key is illustrated. It can be seen from this table the test measures give good estimation about the security of the speech signal.

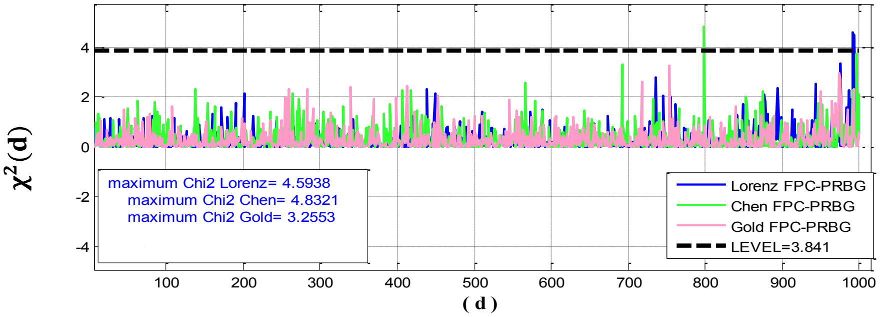


Figure (5) Autocorrelation statistical randomness test

Table (2): Quality measure results

Speech encryption signal			
Key Types	**LLR**	**fwSNRseg**	**SNR_{LOSS}**
Lorenz FPC-PRBG	2.9964	-22.3019	0.9861
Chen FPC-PRBG	2.9664	-22.3987	0.9867
Gold FPC-PRBG	2.9678	-22.3736	0.9869
Recovered speech signal with correct key			
Correct key	0	Infinity	0

Figure (6) shows the waveform time domain of the encryption signal using Gold FPC-PRBG as secret key. Figure (7) and (8) shows the power spectral density (PSD) estimate using periodogram and spectrogram for the original and encrypted speech signal respectively with FFT length 1024 points. It can be seen that the encrypted signal has distorted behavior and unintelligible in both time and frequency domain.

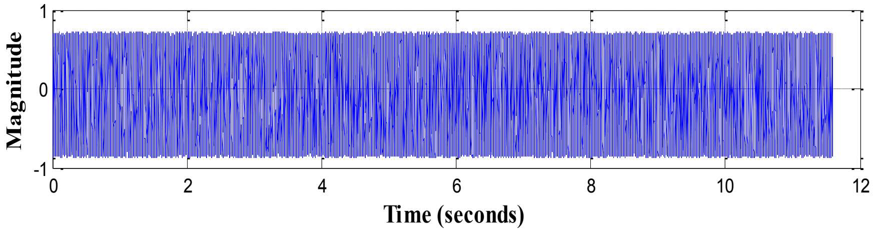
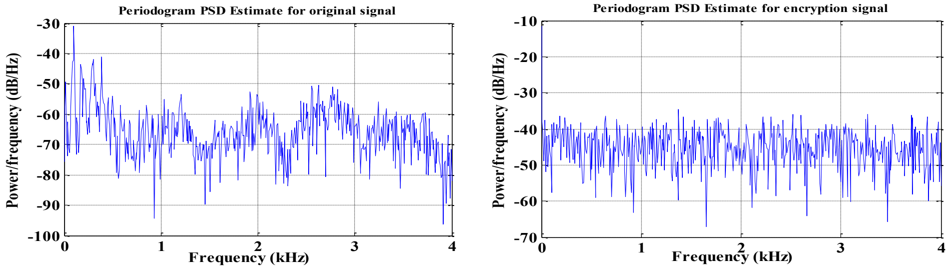
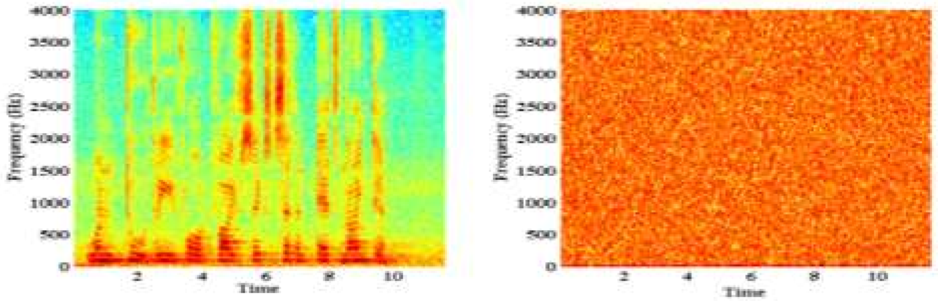


Figure (6) the waveform time domain of the encrypted signal.



(a) Original signal **(b) Encrypted signal**

Figure (7) Power spectral density estimate of speech signal



(a) Original signal (b) Encrypted signal

Figure (8) Spectrogram of speech signal

Security Analysis

One of the most important analysis is the key space of the ciphering system. The key space of FPC-SC system depends on the initial conditions and the parameters of chaos system that are used to generate FPC-PRBG. For Lorenz and Chen based FPC-PRBG there are $\{\alpha_1, \beta_1, \mu_1\}$ and $\{\alpha_2, \beta_2, \mu_2\}$ respectively. For Gold FPC-PRBG the key space is combined both the key space of Lorenz and Chen system i.e. $\{\alpha_1, \beta_1, \mu_1, \alpha_2, \beta_2, \mu_2\}$. Therefore the encryption system based Gold FPC-PRBG has extra key space over Lorenz and Chen system by 3 numbers each signed (2's complement) fixed point number has the range $[-2^{(40-1)}, 2^{(40-1)}]$ [21]. This key space can be increased more and more if combined more than two chaotic systems together.

The second important analysis is the sensitivity of the keys. To test the key sensitivity in each case, the only one of the parameters is changed with small addition value, δ, and other remaining parameters are unchanged. Table (3) shows the quality measure results for recovered speech signal for different tests, where for each test only one parameter in generation of Gold FPC-PRBG is changed by adding 10^{-7} to that in correct key. It can be seen all quality measure indicates that the voice is appeared like random noise and unintelligible. Table (4) shows the quality measure results for recovered speech signal for different tests when α_1 is change with different values of δ.

Table (3) the quality measure results for recovered speech signal for different tests where in each test only one parameter is changed from that of the correct key by added 10^{-7} to it.

Speech decryption signal using incorrect key			
Test	**LLR**	**fwSNRseg**	**SNR_{LOSS}**
$\alpha_1 + 10^{-7}$	2.6708	-20.8420	0.9725
$\beta_1 + 10^{-7}$	3.0187	-21.8355	0.9861
$\mu_1 + 10^{-7}$	3.0664	-21.8412	0.9863
$\alpha_2 + 10^{-7}$	3.0476	-21.8354	0.9860
$\beta_2 + 10^{-7}$	2.9661	-21.628	0.9851
$\mu_2 + 10^{-7}$	2.603	-21.6500	0.9510

Table (4) The quality measure results for recovered speech signal for different tests when only α_1 is changed to with different values of δ.

Speech decryption signal using incorrect key			
Test	**LLR**	**fwSNRseg**	**SNR_{LOSS}**
$\alpha_1 + 10^{-7}$	2.6708	-20.8420	0.9725
$\alpha_1 + 10^{-6}$	2.9628	-20.842	0.9858
$\alpha_1 + 10^{-5}$	2.9628	-20.842	0.9858
$\alpha_1 + 10^{-4}$	2.9628	-20.842	0.9858
$\alpha_1 + 10^{-3}$	2.9628	-20.842	0.9858
$\alpha_1 + 10^{-2}$	2.9628	-20.842	0.9858

Implementation Of Fbc-Prbg Using Xilinx System Generator (Xsg)

The XSG block diagram of Lorenz FPC-PRBG system using RK4 is shown in Figure (9). The details for each block in Figure (9) are shown in Figures (10-14). The system is designed using Xilinx ISE design suite 14.1 with master clock period about 1000 ns (1 MHz). In this system h=2^{-7} and fixed point precision is 40 bits with 24 binary point and signed (2's complement) arithmetic type. These values are founded in experimentally to be optimal case for RK4 to solve and generate Lorenz attractors. At beginning the initial conditions are loaded to the three registers {-2,-3, 6} and then these registers are fed to the four units K_1,K_2, K_3 and K_4 that are implemented according to Equations (4) that is applied for each state of Lorenz differential equation. $\{k_0, k_1, k_2, k_3\}$for state x_1, $\{m_0, m_1, m_2, m_3\}$for state y_1 and $\{n_0, n_1, n_2, n_3\}$for state z_1. Estimation signal block is used to calculate x_1(t+1), y_1(t+1) and z_1(t+1) according to Equation (3). The 40 bits for each state is scrambled using LFSR with 40 bits number, ('8000000101') feedback polynomial and ('B5A459567F') initial value. The scrambled states x_1, y_1, z_1 are feedback to be loaded to three registers to produce another sample value of Lorenz system. The binary stream sequences are taken from the output of XOR Xilinx logical block. In the same manner can be implemented Chen FPC-PRBG system. Figure (15) shows XSG block diagram of Gold FPC-PRBG system. Table (5) shows XC4VSX55-10FF1148 utilization summary for FPC-PRBG system.

Throughput of the system is defined as number of bits per second and is calculated as [12]:

Throught(bits/sec)=$N_B \times f_m$ …(33)

where N_B is number of bits per cycle and f_m is maximum frequency allowed for the system. For FPC-PRBG system N_B=40×3=120 (bits/cycle), f_m=6.822, 6.649 and 6.502 MHz for Lorenz, Chen and Gold FPC-PRGB respectively and the corresponding throughputs are 818.64,7978.88 and 780.24 Mbits/sec.

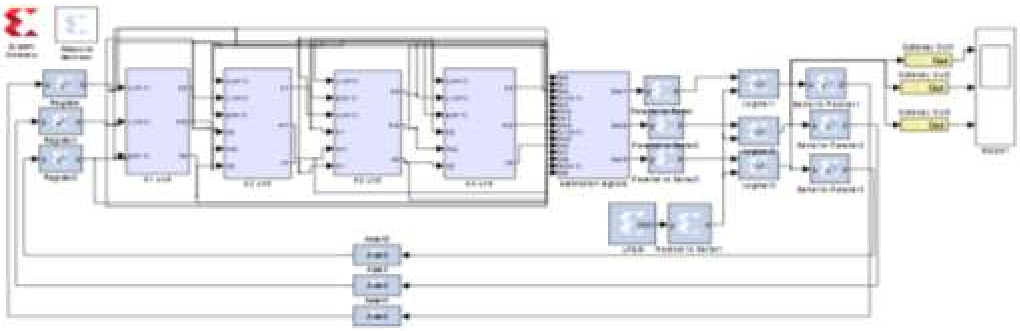


Figure (9) XSG block diagram of Lorenz FPC-PRBG system

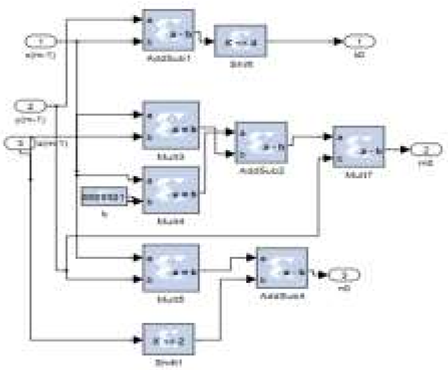


Figure (10) XSG block diagram of K1 unit.

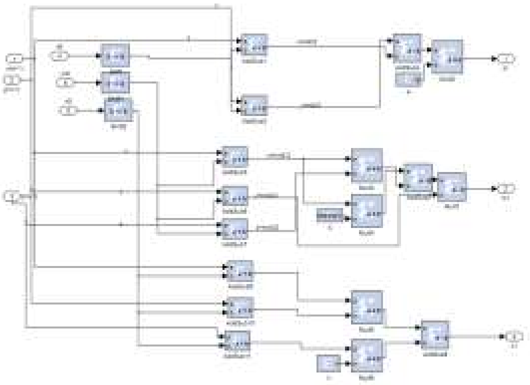


Figure (11) XSG block diagram of of K2 unit.

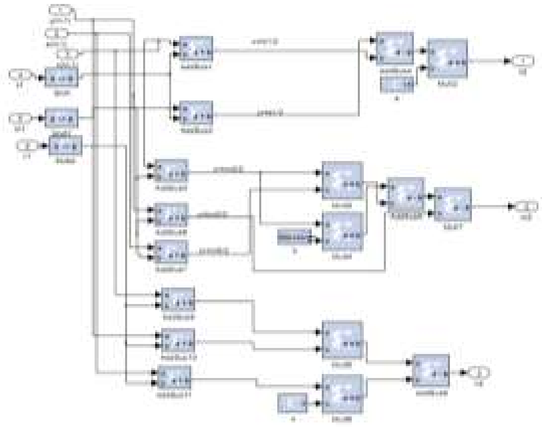


Figure (12) XSG block diagram of K3 unit.

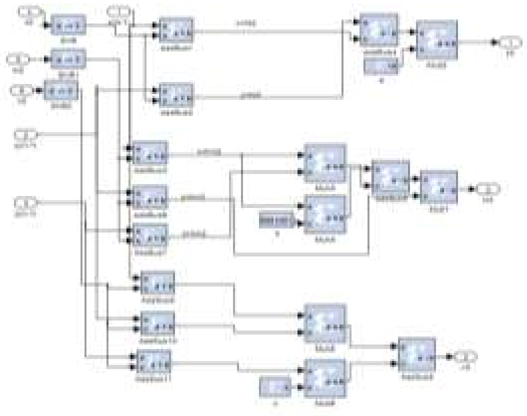


Figure (13) XSG block diagram of K4 unit.

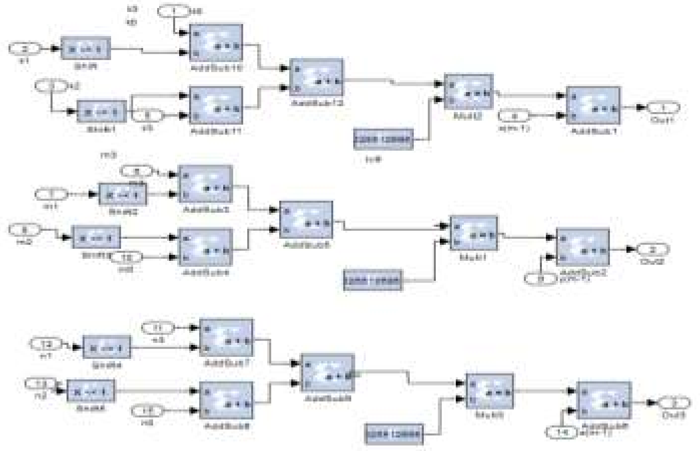


Figure (14) XSG block diagram of Estimation Signal.

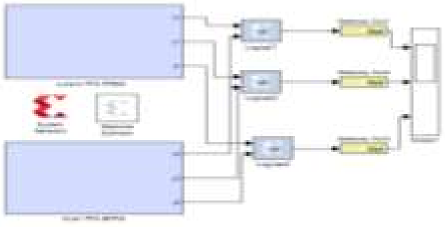
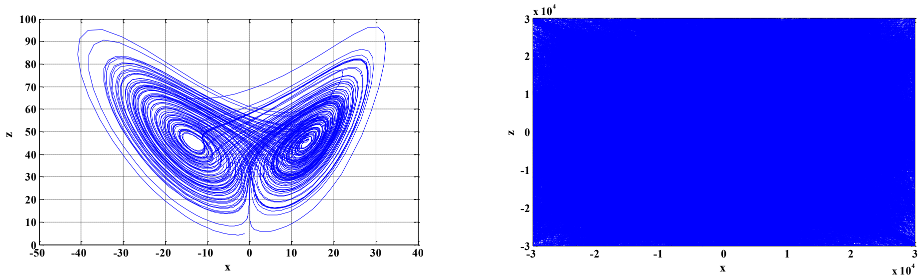


Figure (15) XSG block diagram of Gold FPC-PRBG

Table (5): XC4VSX55-10FF1148 utilization summary for FPC-PRBG system

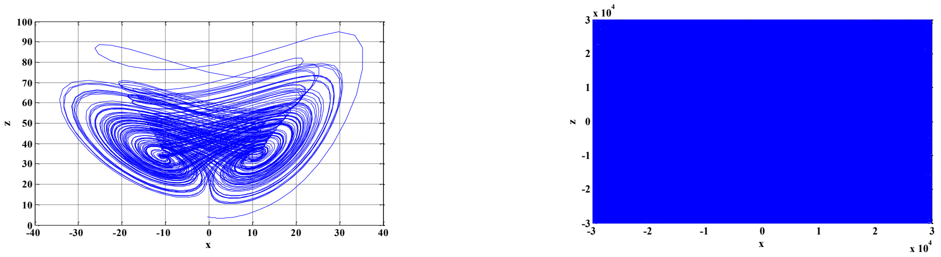
Types of FPC-PRBG	Number of Slice Flip Flops /%	Number of LUTs/%	Number of occupied Slices/%	Number of DSP48s/%	Max. path Delay from/to any node (ns)	Min. Period (ns) (Max. frequency (MHz))
Lorenz- Based	573/1	2236/4	1343/5	168/32	134.189	146.58(6.822)
Chen-Based	573/1	2236/4	1343/5	200/39	138.237	150.39 (6.649)
Gold	1134/2	4472/9	2681/10	368/71	141.4	153.788 (6.502)

Figure (16) and (17) shows plot of x-z attractor before and after scrambling for Lorenz and Chen respectively



(a) Before scrambling (b) After scrambling

Figure (16) x-z attractor for Lorenz system



(a) Before scrambling (b) After scrambling

Figure (17) x-z attractor for Chen system

CONCLUSION

In this paper, fixed point chaotic (Lorenz and Chen system) based PRBG is designed and implemented used for speech encryption system. Fixed point RK4 is used to solve the differential equation of Lorenz and Chen system. New sequence is generated from combined both Lorenz and Chen PRBG called Gold FPC-PRBG. The simulation results show that the random statistical and encryption performance of Gold FPC-PRBG is better than of Lorenz and Chen FPC-PRBG. The FPC-PRBG is implemented and tested using Xilinx System Generator (XSG) with Xilinx Virtex 4 FPGA device, the system is accessed routed for this device with throughput 120 Mb/s for 40 bit fixed point operation. The analysis of speech encryption proved that FPC-PRBG has high security and large key sensitivity.

REFERENCE

[1] Hemlata Kohad, V. R. Ingle, M. A. Gailwad, “Security Level Enhancement in Speech Encryption using Kasami Sequence”, Research and Applications (IJERA), Vol.2, Issue 4, PP. 1518-1523, July-August 2012.

[2] Maher K. M. Alazawi, Jaafar Qassim Kadhim, “Speech scrambling Employing Lorenz Fractional Order Chaotic System”, Journal of Engineering and Development, Vol.17, No.4, PP. 195-210, October 2013.

[3] Aissa Belmeguenai, Khaled Mansouri and Mohamed Lashab, “Speech Encryption using Stream Cipher”, British Journal of applied Science and Technology, Vol8, No.1, PP. 107-125, 2015.

[4] K. Rajam, I. Raja Mohamed and K.J. Jegadish Kumar, “Design of Modified Exclusive-128 NLFSR Stream Cipher and Randomness Test”, International Journal of Computer Applications, Vol. 91, No. 12, PP. 32-36, April 2014.

[5] A. Lakshmi Devi and Vinusha Mandava, “Design and Hardware Implementation for RC4 Stream Cipher by using Verliog HDL”, International Journal of Scientific Engineering and Technology Research (IJSETR) , Vol. 4,Issue 31, PP. 6098-6102, August 2015.

[6] Norul Hidayah Lot@Ahmed Zawawi, Kamaruzzaman Seman, Nurzi Juana Mohd Zaizi, “A New Proposed Design of a Stream Cipher Algorithm: Modified Grain-128”, International Journal of Computer and Information Technology, Vol. 3, Issue 5, PP. 902-908, September 2014.

[7] Saad Najim Al Saad and Eman Hato, “A speech Encryption based on Chaotic Maps”, International Journal of Computer Applications, Vol. 93, No. 4, May 2014, PP.19-28, May 2014.

[8] Majid Bakhtiari and Mohd Aizaini Maarof, “An Efficient Stream Cipher Algorithm for Data Encryption”, International Journal of Computer Science Issues (IJCSI), Vol.8, Issue 3, No.1, PP. 247-253, May 2011.

[9] Mivhalis Galanis, Paris Kitoses, Giogros Kostopoulos, Nicolas Sklavos and Costas Goutis, “Comparison of the Hardware Implementation of Stream Ciphers”, The International Arab Journal of Information Technology, Vol.2, Vo. 4, PP. 267-273, October 2005.

[10] Andrew Rukin et al., “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Application”, National Institute of Standards and Technology (NIST), Special Publication 800-22, Revision 1, August 2008.

[11] Musheer Ahmed, Bashir Alam and Omar Farooq, “Chaos based Mixed Stream Generation for Voice Data Encryption”, International Journal on Cryptography and Information Security, Vol. 2, No. 1, PP. 36-45, 2012.

[12] Shih-Liang Chen, Ting Ting Hwang and Wen –Wei Lin, “Randomness Enhancement Using Digitalized Modified Logistic Map”, IEEE Transactions on Circuits and System, Vol. 57, No. 12, PP. 996-1166, December 2010.

[13] Vinod Patidar and K. K.Sud, “A Novel Pseudo Random Bit Generator Based on Chaotic Standard Map and its Testing”, Electronic Journal of Theoretical Physics (EJTP) Vol. 6, No. 20, PP. 327-344, 2009.

[14] T. Addobbo, M. Alioto, A. Fort and S. Rocchi, “Low Hardware Complexity PRBGs based on a Piecewise-linear chaotic Map”, IEEE Transaction on Circuits and System, Vol.53, No.5, PP.329-333, May 2006.

[15] T. Addobbo, M. Alioto, A. Fort, S. Rocchi and V.Vignoli, “Efficient Post processing Module for a Chaos based Random Bit Generator”, IEEE international Conference on Electronic Circuits and System (ICECS), PP. 1224-1227, Dec. 2006.

[16] Vinod Patridar and K. K. Sud, “A pseudo Random Bit Generator Based on Chaotic Logistic Map and its Statistical Testing”, Informatica 33,PP. 441-452, 2009.

[17] Mohamed L. Barakat, Abhinov S. Mansingka, Ahned G. Radwan, and Khaled N. Salman, “Generalized Hardware Post- Processing Technique for Chaos Based Pseudorandom Number Generator”, ETRI Journal, Vol. 35, No. 3, PP. 448-458, June 2013.

[18] HanPing Hu, LingFeng Liu and NaiDa Ding, “Pseudorandom Sequence Generator based on the Chen Chaotic System”, Computer Physics Communications Journal 184, PP. 765-768, 2013.

[19] E. Lorenz, “Deterministic Nonperiodic Flow ”, J. Atmospheric Sci., Vol.20, No.2,PP. 130-141,1963.

[20] Nikolaos S. Christodoulou, “An Algorithm Using Runge-Kutta Methods of Orders 4 and 5 for Systems of ODEs”, International Journal Of Numerical Methods And Applications, Vol. 2, No. 1, PP.1-11, 2009.

[21] MATLAB R2015b, “Fixed Point Designer ^{TM} User’s Guide”, MathWorks, 2015.

[22] John G. Proakis, “Digital Communications”, Fourth Edition, New York, McGraw Hill, 2001.

[23] Alka Sawlikar and Manisha Sharma, “Analysis of Different Pseudo Noise Sequences”, International Journal of Computer Technology and Electronics Engineering (IJCTEE), Vol.1, Issue 2, PP. 156-161, 2011.

[24] Raghad Z. Al-Macdici, “Designing Security Keys for Satellite Images Encryption”, MSc. Thesis, Mustansiryha University, Baghdad, 2001.

[25] Yi Hu and Philips C. Loizou, “Evaluation of Objective Quality Measures for Speech Enhancement”, IEEE Transactions on Audio, Speech and Language Processing, Vol. 16, No. 1, January 2008.

[26] Jianfen Ma and Philips C. Loizou, “SNR Loss: A New Objective Measure for Predicting the Inteliigibility of Noise Suppressed Speech”, Speech Communication 53, PP. 340-354, 2011.