Audio Encryption in Handsets

A.V. Prabu
Lecturer,
Dept.Ofae&Ie
G.I.E.T,Gunupur
Orissa,India

S. Srinivasarao
Hod, Dept of Ece
Giacre,Rayagada
Orissa, India

Tholada Apparao
Asso.Prof, Dept Of Eee
G.I.E.T,Gunupur,
Orissa,India

M. Jaganmohan Rao
Asso.Prof, Dept Of Ae&Ie
G.I.E.T,Gunupur,Orissa,India

K. Babu Rao
Asst.Prof, Dept. Of Ece,
G.I.E.T,Gunupur,
Orissa,India

ABSTRACT
A novel method to encrypt audio(sound) stream of data by applying chaos is discussed. A pair of one-dimensional logistic maps is used for generating a chaotic sequence. The routine tests of encryption are performed and the results are observed. The proposed scheme is then implemented in real time on a mobile phone and the robustness of the idea is established.

Index Terms — chaotic System, cipher-block chaining (CBC) mode , Mean squared error (MSE), Peak signal to noise ratio, cryptography, Audio encryption & Output Feedback Mode

1. INTRODUCTION

1.1 Encryption

Encryption process deals with secure transmission of data. The necessity of using encryption in a communication system is to protect the data from being received by persons other than the intended recipient. Thus encryption is an indispensable block in the transmission section of any communication system.

Mathematically encryption involves mapping of a plain text to a cipherext using a well-defined function. A common algorithm is agreed upon by both the sender and the receiver and is used both to encrypt the plain text and to decrypt the cipher text. The efficacy of any encryption technique can be gauged by the length and type of its key. In symmetric key cryptography, the keys used for encryption and decryption are the same, whereas they are different in asymmetric key cryptography. The proposed scheme is based on symmetric key cryptography.

1.2 Chaotic System

A chaotic system is a nonlinear deterministic dynamical system which exhibits pseudorandom behaviour. The output values of chaotic systems vary depending on specific parameters and initial conditions. Different parameter values yield different periods of oscillations at the output of the systems.

Chaos sequences are generated in an extremely simplistic manner through the use of difference equations. These sequences appear totally random to an external observer, in spite of their deterministic generation, as they are sensitively dependent on initial conditions. Hardware implementation of chaotic sequences is also not quite complex.

Specific maps are available when it comes to generation of chaotic sequences [3, 17]. The most famous of them all is the one-dimensional chaotic map called the logistic map [5]. It is defined as follows:

$$x_n = rx_n(1-x_n); 0 < x_n < 1, 0 < r < 4 - (1)$$

where 'r' is a variable parameter used to alter the period of the limit cycle oscillations. From r=3.57 the iterations become totally chaotic and begin to lend themselves to the purpose of encryption.

1.3 Security in Mobile Phones

The proliferation of the mobile phone market in the ongoing decade calls for increased security [13] in data transfer applications. Various standards have been established in this regard, but research for a completely robust encryption technique is still on.

This paper deals with chaotic encryption [4, 10] techniques for audio file transfers between mobile phones. A logistic map based algorithm is proposed and its performance is verified through standard encryption tests. The idea is then implemented on a physical system and the claim is asserted.

2. AUDIO ENCRYPTION IN MOBILE NETWORKS

With rapid advances in circuit design and prime focus on miniaturization, mobile phones have kept shrinking in size with each passing day. Hence power consumption and charge storage assume particular importance in mobile technology. Any design of a mobile communication block must take this into full account.

Enlargement of the mobile community has increased the call for secure data transmission. A computationally simple technique can be implemented easily using few components and hence consumes less power, but has limitations in the amount of security it can provide. The task of this paper is to choose an efficient and simple chaos-based encryption [9, 15, 16] strategy to meet the requirements of hardware implementation standards [14].

The one-dimensional logistic map is a simple difference equation, the values of which at various instants depend upon the initial condition and the parameter. The operation of the logistic map can be verified both mathematically and electronically.

For example, assuming an initial condition x(0)=0.5 and parameter 'r'=3.48, using equation (1), and iterating for a large

number of times, one gets four values 0.487, 0.869, 0.395, 0.832 one after another continuously. Thus period four limit cycle oscillations are observed with a parameter value of 3.48.

In particular, the parameter values can be varied from 2.5 to 4 and the period of the limit cycle oscillations can be evaluated. The resulting plot that depicts the possible output values for different parameter conditions is called the Bifurcation Diagram, as shown in Figure 1.

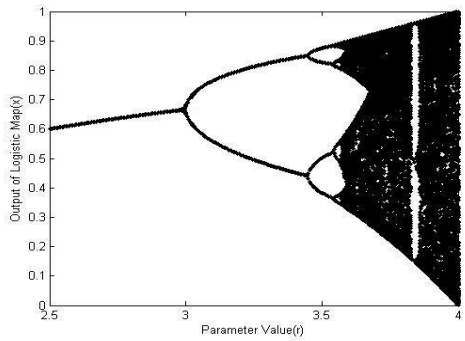

Fig.1: Bifurcation plot of logistic map

Thus a larger value of parameter is chosen to obtain a highly chaotic yet deterministic discrete-time signal.

Iterations of the logistic map with an appropriate parameter value and initial condition can help in performing audio encryption. As the output values of the map are truly pseudorandom in nature and could be determined only by the parameter values and initial conditions, a one-to-one mapping between the quantized audio signal values and the number of iterations required to obtain the different output values is utilized to accomplish the encryption.

3. CHAOTIC ENCRYPTION USING 1-D MAP

From a paper by Baptista [2], it is understood that it is possible to encrypt a text message consisting of alphabets using the logistic map. Each character is encrypted by iterating the logistic map equation for a specific number of times to transfer the trajectory from an initial value towards a chaotic attractor.

The parameter is chosen such that the values lie inside the chaotic attractor of Figure 1. Then the region is partitioned into S sites depending upon the number of characters to be encrypted. Every character is encrypted by a value obtained by iterating the logistic map for some stipulated number of times. The iteration number is sent to the receiver. The receiver decrypts the text by iterating the equation for the same number of times.

The method put forward in this paper involves the generation of two lists of 256 distinct chaotic values through the use of a pair of logistic maps varying in initial conditions and parameter values. The values are then sorted in ascending order and the positions of the various values in the unsorted lists are noted. The positions in the two lists are 8 bit numbers. They are then appended to create a random table of 65536 entries with numbers ranging from 0 to 65536. This table acts as a mapping between indices and entries; quantized input is substituted by the former and the corresponding table entries make up the cipher text.

4. AUDIO ENCRYPTION IN MOBILE PHONES

The entire scheme for audio encryption adopted in this paper is represented as a block diagram in Figure 2.

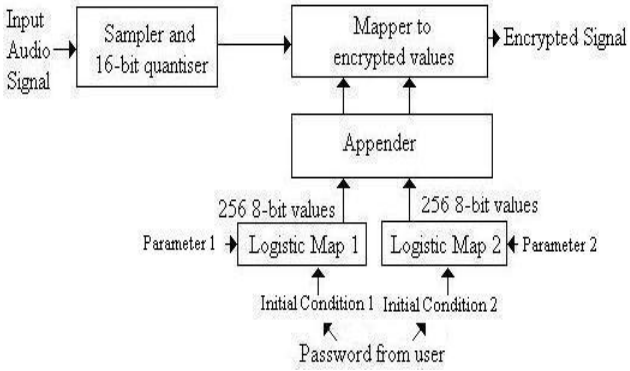

Fig. 2: Block Diagram of Chaotic Audio Encryption Scheme

The algorithm for the chaotic audio encryption scheme is as follows:

(i) The analog audio input is sampled at a frequency well above the Nyquist frequency of the signal.

(ii) 16-bit quantization is used to digitize the discrete signal obtained in step-1.

(iii) Each 16-bit number is converted to its equivalent decimal value.

(iv) A password is requested from the user and two suitable numbers between 0 and 1 are generated using any two different mathematical functions on the ASCII values of the password data. They act as initial conditions x (0) and y (0) for the logistic maps.

$$x_{n+1} = r_1 x_n (1 - x_n);$$
$$y_{n+1} = r_2 y_n (1 - y_n), 0 < r_1, r_2 < 4 - (2)$$

(v) Two parameter values ‘r1’ and ‘r2’ are chosen such that the period of the limit cycle oscillations, as observed from the bifurcation map, is greater than 256.

(vi) The initial values and the parameters are iterated using the equations (2) for a trial period of 1000 times, to arrive at the operating point region of the bifurcation map.

(vii) The resulting values are again iterated for 256 times yielding two 256-valued lists, each with distinct floating point numbers.

(viii) The numbers in the two lists are sorted independently in ascending order and the number of iterations (excluding the initial 1000 iterations) that yielded them is tabulated along with it. The iteration numbers in their order alone are retained for further usage in the algorithm and the actual chaotic floating point numbers are discarded.

(ix) This step aims at generating distinct integers ranging from 0 to 65535 and spanning it

completely, using the above lists. Each of the elements (iteration numbers) in one of the lists is taken one by one sequentially and appended in front of every element of the second list.

(x) An index column is generated by listing the position of the 65536 integers.

(xi) The quantized values of the audio sample are looked up in the index column and are replaced with the corresponding iteration numbers.

(xii) The process is continued recursively till the entire audio file is encrypted.

(xiii) At the receiver side the user is expected to key in the same password in order to obtain the same initial conditions for the logistic maps. The functions that operate on the password are agreed upon by both the sender and receiver.

(xiv) It is also ensured that the parameters of the maps, sampling frequency and the number of bits of quantization are also same at the transmitter and receiver ends.

(xv) Steps (vi) to (xi) are again repeated at the receiver end using the available data.

(xvi) The received 16-bit data are searched for in the iteration number column and are replaced by the corresponding indices.

(xvii) Inverse quantization and digital to analog conversion are performed to retrieve the original signal.

Figure 3 shows the plots of original and encrypted waveforms as functions of time. The encryption parameters are: r1=3.94, r2=3.97, x(0)=0.41 and y(0)=0.51. In Figure 3b the amplitude values are uniformly distributed thereby making the signal incomprehensible.

An encryption standard [12] implemented on a mobile phone should not reduce its processing capability or lead to spurious battery discharge. A version of the programming language Java, namely Java 2 Micro Edition (J2ME) is used to verify the performance of the algorithm on a mobile phone. The implementation details and the results are presented in Section – V.

Figure 4 plots the autocorrelation function of the original and encrypted signals. From the plot, it is evident that the adjacent samples are completely de-correlated in the encrypted signal. Figure 4b resembles the ACF of noise, thereby depicting pure random nature.

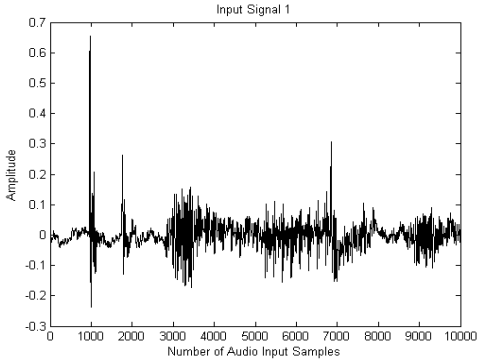

Fig. 3a: Original Signal as a function of time

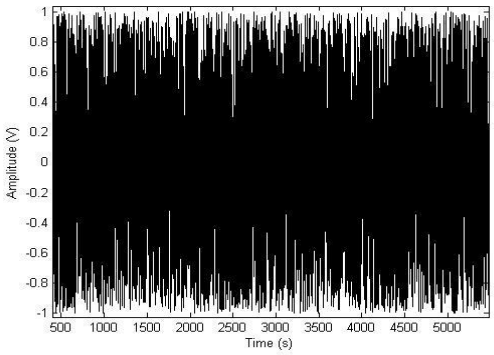

Fig. 3b: Encrypted Signal as a function of time

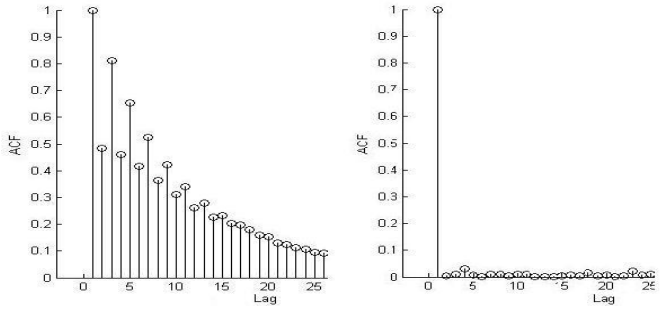

Fig. 4: a b

Autocorrelation functions of Original and Encrypted signals respectively.

5. PERFORMANCE ANALYSIS

All performance analyses of this section have been carried out using Matlab 7.0 software package on a Pentium 4 processor with clock speed of 3 GHz and the system has 512 MB RAM. An audio file comprising voice data, sampled at 22.05 kHz has been analyzed and the numerical results have been provided. The times enlisted are exclusive of the generation process of the chaotic values. The same algorithm and results are found to hold good even for music files.

A larger part of this work is aimed at improving the chaos-based encryption scheme proposed in [1], for suiting real time applications. The 2-D Arnold Cat map based scheme proposed in [1], fails to lend itself to implementation on a mobile phone, due to the large number of computations involved. Stacking two lists of 65536 16-bit values consumes both memory and processing time. In the proposed algorithm, the chaotic values are generated as 16-bit floating point numbers and are discarded once they are sorted using in-place sorting algorithms like the heap sort. Thereafter a memory of 512 8-bit values is needed temporarily. Appending is then performed resulting in 65536 16-bit values requiring a memory of 131 kB. These alone occupy the memory throughout the encryption or decryption process and all the remaining values are deleted. Moreover, the computations are based on a single list of 65536 elements, as opposed to two such lists as is the norm in [1]. In addition to these, encryption in [1] is prolonged due to the presence of searching operation of the quantized audio samples amidst 65536 integers.

An additional feature that has been implemented is the password authentication system. This ensures that anyone in possession of the mobile phone does not get to hear the

transmitted audio through the use of the two parameter values. The initial conditions are generated using linear functions of the ASCII values corresponding to the password, which yield unique values for every password.

The implemented system displays a wide range of merits. The installation of the software on the phone does not degrade the speed or performance of any other application. The encrypted audio file and the original file are of the same duration, thereby ensuring that the process does not increase the number of bits transmitted.

The algorithm proposed in Section – IV operates on the mode of Electronic Codebook (ECB). The times required for performing encryption and decryption using the proposed algorithm is shown in Table 1 as a function of number of audio input samples. As the audio file size becomes bigger, there is a linear rise of the time required for computations. Moreover decryption is found to be more prolonged than encryption as a sequential search is performed amidst 65536 index values to determine the actual audio sample. Faster search algorithms like the binary search also are unsuitable as they require a sorted list.

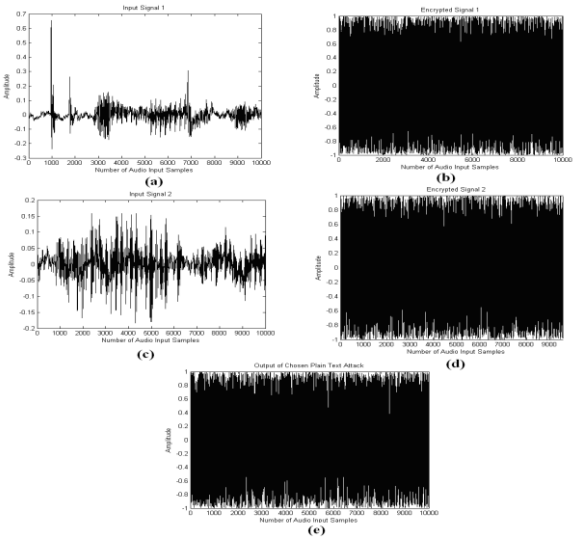

Fig. 5 : Plot of waveforms depicting the robustness of the ECB mode against XOR-based chosen plaintext attack

An advantage of the ECB mode of operation could be stated as the absence of any XOR based operation. Thus it is found to be robust against XOR-based chosen plaintext attacks [7]. Figure 5 depicts the robustness of a plaintext encrypted using the ECB mode. Fig. 5a and 5b are the plaintext transmitted and cipher text obtained by the attacker respectively. Fig. 5c is the actual message sent by a user over the ECB-based encryption system. Fig. 5d is the actual signal that travels along the channel obtained after encryption. Fig. 5e is the result of the XOR-based chosen plaintext attack, which is totally different from the expected Fig. 5c. Thus the XORing of the attacker's plaintext, cipher text and the cipher text of the actual message transmitted gives a signal that is non-identical to the intended plaintext.

Reduction of the decryption time necessitates a different configuration of the encryption-decryption process. Due to the ineffectiveness of decryption of the Electronic Codebook (ECB) mode that has been proposed, alternate modes are sought for and implemented. The block diagrams of the alternate methods of Cipher Block Chaining (CBC) and Output Feedback (OFB) are shown in Figures 6 and 7 respectively.

In the cipher-block chaining (CBC) mode, each block (quantized sample) of plaintext is XORed with the previous cipher text block before being encrypted. This way, each cipher text block is dependent on all plaintext blocks processed up to that point. But this method could be hazardous if a single bit in a plaintext gets corrupted due to noise prior to encryption, leading to errors in all cipher text

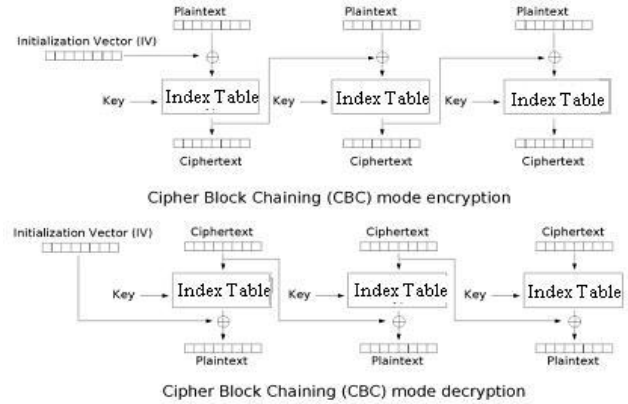

Fig. 6: Block diagram of Cipher block chaining mode

Input sample size	ECB MODE		CBC MODE	
	Encryption Time (s)	Decryption Time (s)	Encryption Time (s)	Decryption Time (s)
1e3	0.039	1.75	0.046	1.765
1e4	0.047	16.904	0.078	15.969
2e4	0.062	34.312	0.115	33.969
3e4	0.069	61.605	0.125	52.843
5e4	0.078	80.79	0.187	84.968
1e5	0.109	168.703	0.297	169.609

Table 1: Times required for encryption and decryption processes as a function of the number of input samples in the ECB and CBC modes.

samples. Similarly during decryption, a single bit error in a cipher text corrupts two samples of plaintext. Moreover, no improvement in decryption time is found as the mode does not overcome searching operation. Table 1 displays the times taken for encryption and decryption in the ECB and CBC modes. It is clear that while no improvement is achieved in the decryption period in the CBC mode, the encryption is also delayed due to the XOR operation and the dependence on the immediate past cipher text sample.

The Output Feedback Mode (OFB) is tried as the next alternative and is found to present the best solution, the reasons for which are stated as follows:

1) From the block diagram (Figure 7) of OFB, it is obvious that the majority of the time in the encryption and decryption processes in this mode is spent towards the creation of chaotic data using the logistic map. In any parallel processor, a single clock cycle is expected to perform the entire encryption and

decryption process. Completely parallel system architecture is the key merit of OFB.

2) As in ECB, noise corruption of a single data sample in the plaintext or cipher text only affects the corresponding output in the other. There is no threat of error propagation in OFB.

3) The password and chaos-based table generation could be performed well in advance of the arrival of the actual audio file.

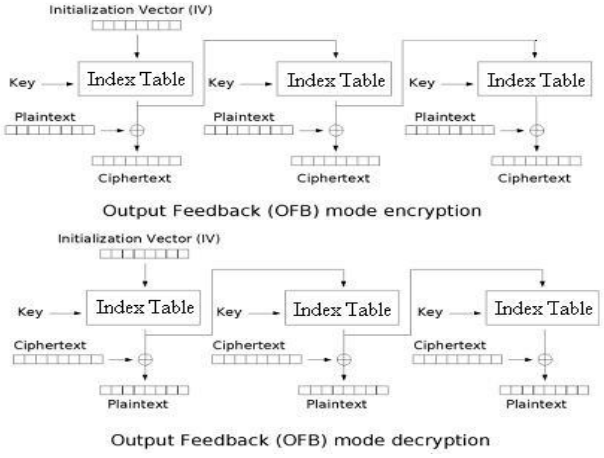

Fig. 7: Block diagram of Output Feedback Mode

4) The time for decryption is also largely reduced as the process is completely devoid of any searching operation.

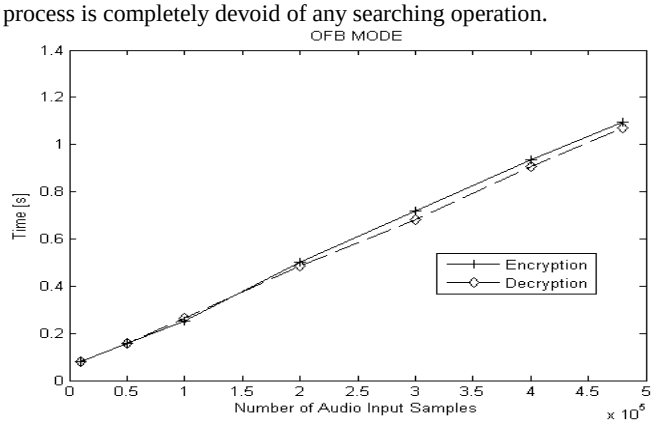

Fig 8: A plot of the times required for encryption and decryption processes as a function of the number of input samples in the OFB mode.

Figure 8 shows a plot of the times required for encryption and decryption using the OFB mode. The times taken for encryption are nearly the same when compared to the ECB mode, and the decryption times are reduced as expected.

The true security in the proposed algorithm is provided by the password and the parameter values that are agreed upon by the transmitter and receiver. While modifying the password for every new input file increases the computational time, it plays an important role in enhancing the security of the system. For fast encryption of many audio files, a single password may be deemed enough. Thus with OFB mode of execution of the chaos based algorithm, a trade-off is possible between security and time. Higher levels of security could be attained by using separate passwords for the two logistic maps or by increasing the number of logistic maps and creating an index of more than 65536 values.

The proposed algorithm is found to be better in certain aspects to the Advanced Encryption Standard (AES) algorithm.

	TIME FOR ENCRYPTION (s)	
MODE	AES	Proposed Algorithm
ECB	0.2399	0.07
CBC	0.2509	0.128
OFB	0.1909	0.13

Table 2: Comparison of encryption times of AES [11] and the proposed algorithm for a file size of 65 kB

1) AES operates on blocks of data of 128 bits, which needs temporary storage of the input audio samples. This algorithm does not store the input samples. Once the one-to-one mapping is generated through chaos, the input samples are effectively supplanted by the iteration numbers through in-place operations.

2) The four rounds of the AES algorithms along with the initial and final rounds do provide an extraordinary level of security, but the demerit of the standard is the greater time involved in the encryption – decryption processes.

The duration of the proposed algorithm is compared with the AES algorithm for a file size of 65 kB [11] and the results are shown in Table 2. From the table, the claims regarding the speed of the proposed algorithm are justified.

Test	Expected Results	Obtained Results
Monobit test (Number of ones in a 20000 bit stream)	9654 - 10346	9948
Poker test (A function of the number of occurences of the 16 4-bit numbers in a 20000 bit stream)	1.03 - 57.4	45.23
Runs test (Successive occurences of 1s and 0s in a 20000 bit stream)	Length: 1: 2267 - 2733 2: 1079 - 1421 3: 502 - 748 4: 223 - 402 5: 90 - 223 6: 90 - 223	2541 1285 641 289 165 140
Long Run Test (Runs longer than 34)	0	0

Table 3: Results of standard tests on encrypted data

Mean squared error (MSE) and Peak signal to noise ratio (PSNR) are calculated for the encrypted audio file using these formulae.

$$MSE = \frac{1}{N}\sum_{i}\left|x(i)-e(i)\right|^2$$

$$PSNR = 20\log_{10}\left(\frac{65535}{\sqrt{MSE}}\right)$$

Here x and e are the input and encrypted signals respectively

and N is the number of samples in the audio signal. An extremely high value of MSE of 7.157E8 and a correspondingly low PSNR of 7.77dB were obtained. The high MSE stood for complete deviation of the encrypted data from the signal, as is also apparent from the ACF plot, shown in Figure 4.

Various encryption validity tests [6] have been performed on the encrypted signal and the outcome is tabulated in Table 3.

6. CONCLUSION

A robust chaos-based audio encryption scheme has been proposed. The technique is found to be computationally simple and memory-inexpensive.Different modes of encryption like ECB, CBC and OFB are tried and tested for speed and security and OFB mode of operation is found to be the fastest in terms of speed. The encrypted data satisfied various standard tests for randomness.

Considerable scope for improvement is available from this work. The effectiveness of the scheme can be tested by embedding it in a complete digital communication system [8]. The system could be tested for robustness in noisy channels by transmitting the encrypted signal through channel noise models like the AWGN or Rician or Rayleigh fading channels. Alternatively the performance of other chaotic maps can be analyzed and compared with the logistic map on grounds of simplicity, efficiency and speed. Work is in progress to implement a similar algorithm for imaging and video applications. Also, real time encryption on a mobile phone as and when the data is being transmitted is an interesting aspect that is within our purview.

7. REFERENCES

[1] K. Ganesan. K. Murali, R. Muthukumar, "Look-Up Table Based Chaotic Encryption of Audio Files", *IEEE Asia Pacific Conference on Circuits and Systems, 2006*, pp. 1951-1954, APCCAS 2006.

[2] M.S.Baptista, "Cryptography with chaos", *Physics Letters A*, Vol. 240, pp. 50–54, 1998.

[3] T. Yang, C.W. Wu and L.O. Chua, "Cryptography based on chaotic systems, "*IEEE Transactions On Circuits & Sysems - I*, Vol. 44, pp. 469-472, 1997.

[4] Su Yong; Han Zhen; Luo Siwei; "A new method of the chaos encryption", *ICSP '98, Fourth International Conference on Signal Processing Proceedings, 1998*, Vol.1, 12-16, pp. 233 – 236, Oct. 1998.

[5] Luo, J.; Shi, H., "Research of Chaos Encryption Algorithm Based on Logistic Mapping", *IIH-MSP '06, International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2006*, pp. 381-383, Dec 2006.

[6] FIPS PUB 140-1 "Security requirements for cryptographic modules", *Federal Information Processing Standards Publication*, 1994.

[7] M.I. Sobhy and A.E.R. Shehata, "Methods of attacking chaotic encryption and Countermeasures", *IEEE International Conference on Acoustics, Speech and Signal Processing*, Vol. 2, pp. 1001 – 1004, 7-11 May 2001.

[8] Chin Yi Chee and Daolin Xu, "Secure digital communication using controlled projective synchronisation of chaos", *Chaos, Solitons & Fractals*, Vol. 23, Issue 3, pp. 1063-1070, February 2005.

[9] Xiaogang Wu, Hanping Hu and Baoliang Zhang, "Analyzing and improving a chaotic encryption method", *Chaos, Solitons & Fractals*, Vol. 22, Issue 2, pp. 367-373, October 2004.

[10] Kocarev, L., "Chaos-based cryptography: a brief overview", *IEEE Circuits and Systems Magazine,* Vol. 1, Issue 3, pp. 6 – 21, 2001.

[11] Nawal El-Fishawy and Osama Abu Zaid, "Quality of Encryption Measurement of Bitmap Images with RC6, MRC6 and Rijndael Block Cipher Algorithms", *International Journal of Network Securit*y, Vol. 5, No. 3, pp. 241-251, Nov. 2007.

[12] Ahmet Eskicioglu and Edward Delp, "An overview of multimedia content protection in consumer electronics devices", *Signal Processing Image Communication*, Vol.16, pp.-681 – 699, 2001.

[13] Ahmet Eskicioglu, John Town and Edward Delp, "Security of digital entertainment content from creation to consumption", *Signal Processing Image Communication*, Vol.18, pp.-237 – 262, 2003.

[14] M. Delgado-Restituto, M. Linan and A. Rodriguez-Vazquez, "CMOS 2.4pm chaotic oscillator: experimental verification of chaotic encryption of audio", *Electronics Letters*, Vol. 32, Issue 9, pp.795-796, 1996.

[15] Wenwu Yu and Jinde Cao, "Cryptography based on delayed chaotic neural networks", *Physics Letters A*, Vol. 356, Issues 4-5, pp. 333-338, August 2006.

[16] Shujun Li, Guanrong Chen, Kwok-Wo Wong, Xuanqin Mou and Yuanlong Cai, "Baptista-type chaotic cryptosystems: problems and countermeasures", *Physics Letters A*, Vol. 332, Issue 5-6, pp 368-375, November 2004.

[17] Yong Wang, Xiaofeng Liao, Tao Xiang, Kwok-Wo Wong and Degang Yang, "Cryptanalysis and improvement on a block cryptosystem based on iteration of a chaotic map", *Physics Letters A*, Volume 363, Issue 4, pp 277-281, April 2007.