Security Enhancement Algorithm for Data Transmission for Next Generation Networks

Neha Jain
TCET
Mumbai

Vikas Kaul
TCET
Mumbai

S K Karayankhedkar, Ph.D.
Principal, MGMCET,
Navi Mumbai, Maharashtra, India

ABSTRACT
This paper presents the design and implementation of a symmetrical hybrid based AES algorithm as a security enhancement for data transmission which is further improved by using chaos. This work outlines the possible weaknesses within the current AES encryption algorithm especially against algebraic based cryptanalysis. It proposes the idea on integrating AES within the Feistel network, hence resulting into the development of the Hybrid AES algorithm. That hybrid algorithm is further enhanced by chaos.The characteristics of chaos sequence make the space of key infinite. Hence we get a system which is much difficult to break by cryptanalysis..

General Terms
Security, Fiestel-Network, AES algorithm

Keywords
Chaos, Control Key, Encryption Key

1. INTRODUCTION
It is a thousand years since cryptography formed. In recent years, the requirement of information security is enhanced, so a lot of encryptions are presented, such as RSA, DES, AES and so on. A good encryption system should have complex functions and a small change of key will lead a big change of the results [1]. A truly safe system is “one time one key”, but it is difficult to do so. Alone with the development of computer and math, if one system has a limited key space, it can be broken easily. Such as DES algorithm, in 1998, it can be broken in 56 hours. Therefore, people want to explore new methods [2] to the requirement of information safety. How to improve the key space and the nonlinear factors are given attention by scientists.
AES is a new method of encryption. But the corestructure of the AES itself renders a clean, simplealgebraic method, hence yielding the algorithrnsusceptible towards algebraic based cryptanalysis attacks.This issue can be solved by using AES within a Fiestel network.

Also the original AES cryptographic system is definite and the key space is limited. The chaos system is non-periodic, not convergence, and sensitive to initial conditions. Due to these characteristics, it has got more and more attention too. Using chaos in key generation method of AES helps to get a large key space and a complex key.

2. BACKGROUND
2.1 Literature Survey
In 1949 Shannon C E. started a work in the field of secret communication which is named as Communication
Theory of SecrecySystems published in bell Systems Technical Journal. Many algorithms had been made after that like stream cipher ,block cipher etc. On 2 October 2000, after a three-year study period in which 15 block ciphers competed, the US National Institute of Standards and Technology (NIST) announced that the block cipher Rijndael would become the Advanced Encryption Standard
.N. Courtois and Pieprzykhad done cryptanalysis of block cipher algorithms [3] in year 2002. After some time S. MurphyandMJ.BRobshawidentified essential Algebraic Structure within the AES .This paper proved that AES is prone to algebraic attack [4]. This work had been published in Advances in Cryptology CRYPTO 2002, Vol. 2442 .In 2005, H. Nover has done Algebraic cryptanalysis on AES [5]which is published in University of Wisconsin, USA.To overcome the drawback of Algebraic attacks on AES, M.B. Vishnu, S.K. Tiong,M. Zaini,S.P. Koh, introduced a new algorithm called Hybrid AES-DES used to secure transmission of digital motion image in 2008.
In year 2001, L Kocarev worked for a new concept which included chaos in cryptography. The paper chaos-based Cryptography:a Brief overview was published in IEEE Circuits and Systems Magazines in 2001. An Improved AES algorithm based on chaos by Yuan Kun, Zhang Han Li Zhaohui was published in 2009 International Conference on Multimedia Information Networking and Security. Performance Analysis of various encryption algorithm [12] concluded that AES can be a good choice for our work.

2.2 AES
The Advanced Encryption Standard (AES) is an encryption algorithm for securing sensitive information by U.S. Government agencies. TheRijndael algorithm proposed as an accepted standard is discussed in the sections that follow. Figure1 elucidates the main steps comprising the AES

algorithms [6]. The four major functions that comprise the AES are Add RoundKey, Substitute bytes, Shift Rows and Mix Columns. Rijndael is a substitution linear transformation network with 10, 12 or14 rounds, depending on the key size.
AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits. Rijndael specified with block and key sizes that it may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits.

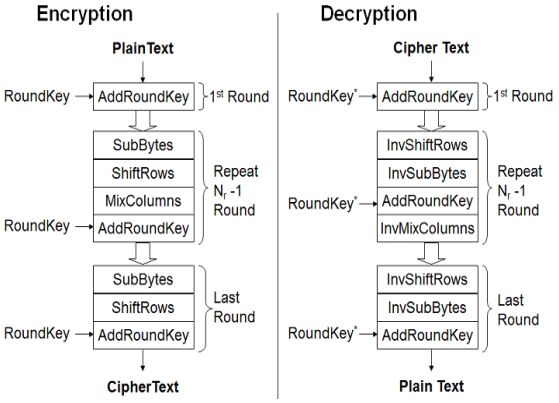

Fig 1 Major Functions of AES

2.2 Chaos

The chaos is one kind of nonlinear movement form. It is produced by a definite system, and it relies on the initial condition, and it is unpredictable. The chaos system has several characteristics [7]: stochastic, sensitive to initial condition, long-term unpredictability and so on.Chaos theory studies the behavior of dynamical systems that are highly sensitive to initial conditions. Small differences in initial conditions yield widely diverging outcomes for such dynamical systems, rendering long-term prediction impossible in general. This happens even though these systems are deterministic, meaning that their future behavior is fully determined by their initial conditions, with no random elements involved. In other words, the deterministic nature of these systems does not make them predictable.This behavior is known as deterministic chaos, or simply chaos.

3. NEW ALGORITHM

3.1 Hybrid AES using Fiestel Network

Mathematically, the idea of a hybrid [8] based AES can be construed with reference to basic Feistel equations. The repetition of these equations is based on the number of rounds as adapted by the FeisteI network, which in the case of DES was standardized at 16. However, by incorporating the AES within these yield the following results;

$Ln = Rn$----------(1)

$Rn = AES\ (Ln - (Rn - l, K, J)$----------(2)

From Equation (2), each *Rn-l* and *Kn*is channelled into the round function, which basically revolves on a XOR function between these variables. The output of the round function is then XORed with *n-* before being channelled as input data for the AES algorithm. The result from the AES process represents *Rn•* The AES operations include the byte substitution, shift row, mix columns and add round key operations. Equations (1) and (2) are then iterated over a period of rounds, retrospective to the number of keys as generated from the key schedule process. In this algorithm the key schedule process for the hybrid system is directly adapted from the AES standard and the round keys for the AES process are directly adapted from the expanded keys. The scheme of using a common set of keys for the round functions within the Feistel network and the AES functions as called during the operation reduces the computational complexity in creating multiple sets of keys for each overall hybrid operation. However, the mathematical modelling for the key expansion of the AES limits its generation at 10 keys based on the number or rounds as applied for a 128 bit based AES encryption process. Hence, the proposed number of iterations for the hybrid system is set at 10. Nonetheless, the iterations also vary based on the level of security implementation for the Hybrid AES. Note as seen from Equation (2), with every round of iteration, the AES function is performed with different sets of generated results based on varying sets of expanded keys. Fig. 2 below displays one round of a Hybrid AES algorithm.

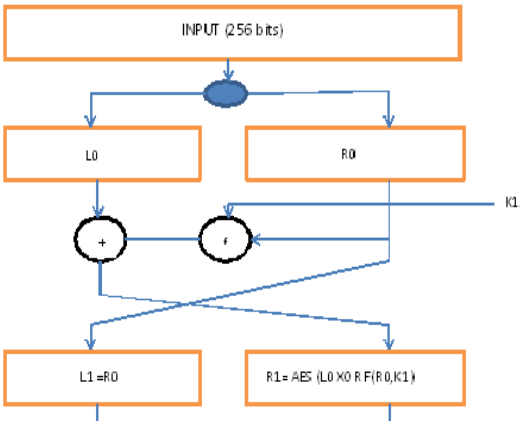

Fig 2 One Round of Hybrid AES

Despite its improved security features, the performance of the algorithm represents a possible setback to the hybrid structure. A complete Hybrid AES operation performs 10 layers of Feistel calculations, utilizing the nonlinear Equations (1) and (2) as well incorporating 10 sets of AES. This increases the strain onto the computational density needed to complete the encryption and decryption processes. Consequently, the number of layers as applied for the hybrid structure is set a varying parameter as controlled by the user to perform the encryption and decryption processes. Meanwhile, the nature of application of the Hybrid AES is also based on the Quality of Service (QoS) of the algorithm itself. In environments that require increased security policies for data and multimedia transmission and storage, a higher number of layers of the algorithm yield a suitable solution. Inverse policy is applied for environments with lower security policies which the number of layers are reduced.

3.2 Improvement in AES using Chaos

The AES used within the Fiestel Network can be improved by this concept. Some scholars used two two-dimensional chaotic systems to get two sequences, and thenthey do “XOR” with the two sequences. Theresults of this operation are the keys of the wholesystem [11]. We also used two chaos systems which can generate two keys. One can be used as the encryption key, the other one as the controller key which can control the times of row-shift. The characteristics of chaos sequence make the space of key infinite.
In order to test easily, the improved algorithm uses two simple chaotic systems [9]. The key is the initial value of each chaotic sequence. Its expression is:

$$\begin{cases} y_{i+1} = (y_i + \frac{kH}{2\pi}\sin\frac{x_i 2\pi}{H}) \bmod H \\ x_{i+1} = (x_i + y_{i+1}) \bmod H \end{cases}$$

Where $x \in [0,1), y \in [0,1), k > 0$.

[10] shows methods to get chaotic maps according to various block cipher encryption based on Fiestel network.

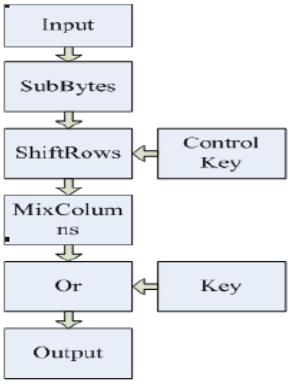

Fig 3 Structure of enhancement in AES

.

Step1: Reading 256 bit data as input, dividing it into the two parts of equal size (128 bit).
Step2: Perform fiestel function operation with the right part using round key. XOR the result with the left part.
Step3: The result of above step will be an input to AES rounds.
Step4: Inputs two chaos system's starting values to produce sequence which needs in the encryption process. The first sequence uses for doing the 'XOR' operation with the input datewhich had been transformed, the second sequence each time produces four keys. The first five of each key is the order numbers of each line shift.
Step5: After each round of AES, two chaos sequences produce the new encryption key and the control key;
Step6: The output we get after all AES round should be considered as next left part of the Festel network.
Step 7: Continue the same process until we complete all the rounds we fixed for Fiestel network.
Figure 4 on next page shows the detail structure of hybrid AES in which AES rounds are also shown with chaotic sequenced keys.

4. PERFORMANCE ANALYSIS OF HYBRID AES

4.1 Key space analysis

Shneier a famous scholar put forward: a goodkey space must be large, so the powerful attack isimpossible[6]. Chaos system meets it very well.The ergodicity of chaotic system make the spaceof key distribution uniformity and the key spaceunlimited, so it can better against some shortcuts.This new method has six initial values. If the typeof initial value selection is double, the key spaceof the chaotic sequences can be10^{15} , and the keyspace of the whole encryption system canbe10^{90} . It is more than the original AES whosekey space is 2^{128} .

4.2 Key sensitivity analysis

Shneier pointed that a good encryption system must be extremely sensitive to the key of encryption, a small change of the key leads to great changes of the results. Ineach encryption process, the chaotic sequencesoperate with plaintext so we can say ciphertext is dependent on plaintext.

4.3 Statistical analysis

According to the Shneier's theory, any encrypted system can be broken by statistical analysis method [15]. We use chaotic sequence [6] to increase the nonlinear parts of encryption process. So the plaintexts are high diffusing, the analysis method also become very difficult.

5. RESULTS

The algorithms have been implemented in Matlab R2012a software. The following parameters have been used:

1. Encryption Time: The time required by the algorithm for processing completely a particular length of data is called the simulation time. It depends on the processor speed, complexity of the algorithm etc. The smallest value of simulation time is desired.
2. CPU Usage: The amount of CPU memory utilization during the execution of algorithms.
3. Throughput: It depicts the number of bits encrypted per unit time. The Formula is as follows:
Throughput = Total no of bits / Total Encryption Time
4. Avalanche Effect: A desirable property of any encryption algorithm is that a small change in either the plaintext or the key should produce a significant change in the cipher text. In, particular a change in one bit of the plaintext or one bit of the key should produce a change in many bits of the cipher texts.

Various tests have been done on all the above mentioned algorithm. The summary of their performance is shown in table 1,2,3 and in figure5,6,7.

Table 1 Comparison of various Algorithm w.r.t Encryption and Decryption Time

Encryption technique	Encryption time(sec)	Decryption time (sec)
AES	0.12	0.17
Hybrid AES using Fiestel Network	1.78	1.79
Improved HYBRID AES sing chaos	1.91	1.94

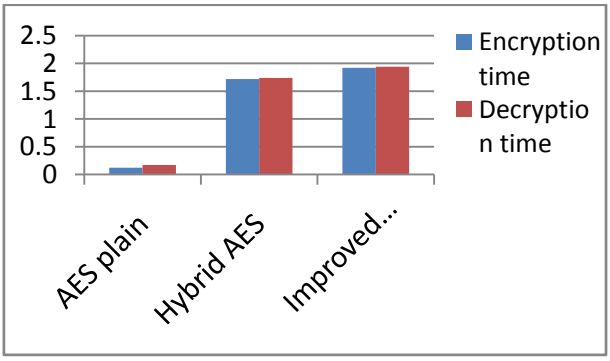

Fig5 Comparison between various encryption algorithm

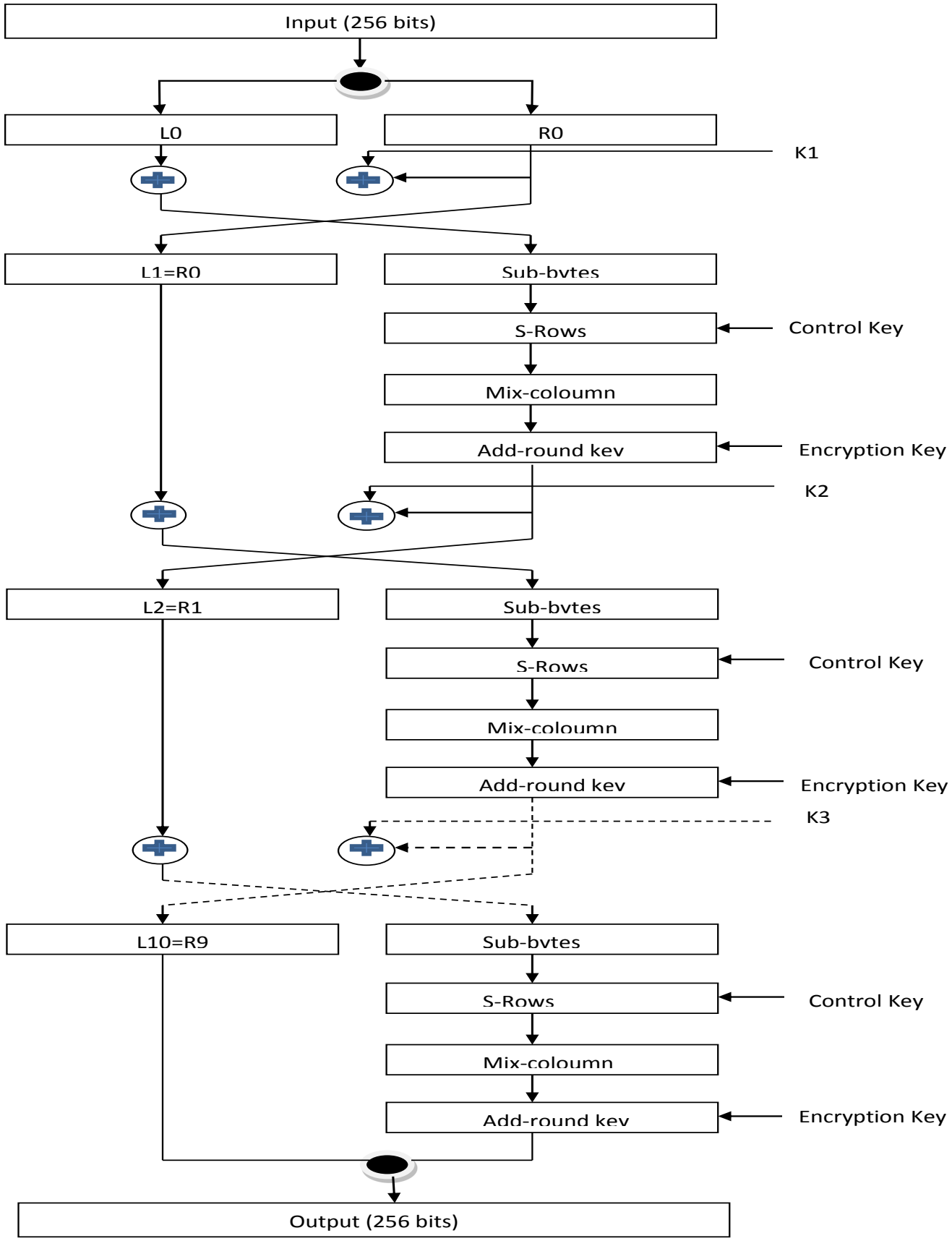

Fig 4 Structure of hybrid AES including chaos

Table 2 Comparison of various Algorithm w.r.t CPU usage and Throughput

Technique	CPU Usage (in %)	Throughput (bits/sec)
AES	22%	1066.67
Hybrid AES	25%	143.82
Improved AES	24%	13.40

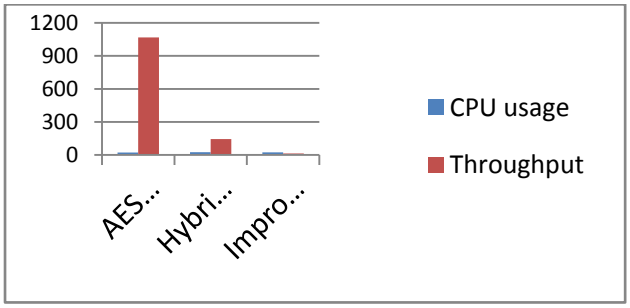

Fig6 Comparison of various Algorithm w.r.t CPU Usage and Throughput

Table 1 Comparison of various Algorithm w.r.t Avalanche Effect

Technique	Avalanche Effect	
	Change in 1-bit of Plain Text	Change in 1-bit of Key
AES	71	64
Hybrid AES structure	179	174
Improved AES	192	182

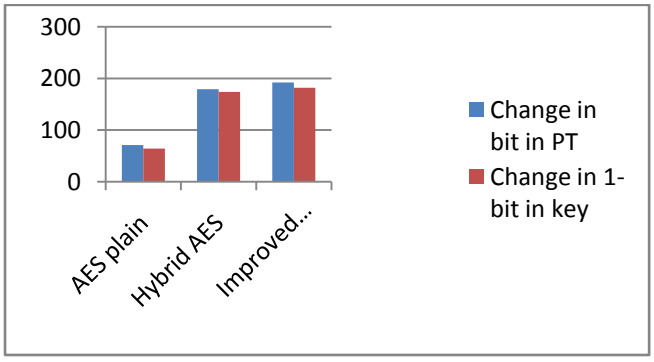

Fig7 Comparison of various Algorithm w.r.t Avalanche Effect

Configuration Used for Simulation: Microsoft Windows 7, Intel i5 CPU M480 @ 2.67 GHz, 4 GB RAM

5. CONCLUSION

The original AES encryption algorithm has considered differential attack and linear attack, so it can resistance these attack well. But the key space is limited, with the rapid development of computer science; its disadvantages are also increasingly. This paper puts forward a double-key encryption algorithm method based on chaos. Our paper uses the combined concept of AESand Fiestel network to obtain a hybrid model which can be used for encrypting various kinds of data. Nowadays it is very important to design strong encryption algorithms as the power of computers is growing day by day. Thus the hybrid model gives a better non linearity to the plain AES and as it is merged with fiestel network, there is better diffusion.

Hence the possibility of an algebraic attack on the hybrid model is reduced.Not only increasing the key space, but also the scrambling to plaintext. The nonlinear parts also further increase in the process. Safety analysis shows that the key space of the improved algorithm is unlimited, so it can resist statistical analysis attack very well.

6. REFERENCES

[1] Shannon C E, Communication Theory of Secrecy Systems, bell Systems Technical Journal,1949:28:656-715

[2] FengGuodeng, Pei Ding Cryptography introduction .BeiJing Science Press 1999

[3] Nicolas T. Courtois and Josef Pieprzyk,Cryptanalysis of a block cipher with over defined systems of equations

[4] S. Murphy, MJ.B Robshaw, "Essential Algebraic Structure within the AES", Advances in Cryptology CRYPTO 2002, Vol. 2442 of Lecture Notes in Computer Science, Springer-Verlag, August 2002

[5] H. Nover, "Algebraic Cryptanalysis of AES: Overview", University ofWisconsin, USA, 2005.

[6] Bruce Shneier .Applied Crptography :protocol Algorithms, and source code in C.Johnwiley&Sons,Inc, 1996

[7] L Kocarev.Chaos-based Cryptography: aBrief overview. IEEE Circuits and Systems Magazines, 2001:1(3):6~22

[8] M.B. Vishnu, S.K. Tiong. Security Enhancement of Digital Motion Image Transmission Using Hybrid AES-DES Algorithm, APCC2008 OF IEICE ,2008

[9] Yuan Kun, Zhang Han Li Zhaohui. An Improved AES algorithm based on chaos, International Conference on Multimedia Information Networking and Security 2009

[10] GoceJakimoski and LjupˇcoKocarev, Chaos and cryptography: Block Encryption Ciphers Based on Chaotic Maps.

[11] Zhao Rui. Wang Qingsheng. Wen Huiping. Design of AES Algorithm Based on Two Dimensional Logistic and Chebyshev Chaotic Mapping 2008
[12] Nadeem, A. and Javed, M.Y., "A Performance Comparison of Data Encryption Algorithms," IEEE Information and Communication Technologies, 2005.
[13] VikasKaul "Security Enhancement of Data Transmission for Next Generation networks" IJCA2012.