ISSN 2047-3338

Chaos Based Secure Real Time Protocol (CSRTP)

Mazen Tawfik Mohammed[1], Alaa Eldin Rohiem[2] and Ali El-moghazy[3]
[1,2,3]MTC College, Egypt
[1]mazen.mtc@gmail.com, [2]alaa_rohiem@yahoo.co.uk, [3]moghazymtc@yahoo.com

***Abstract*– Secure Real-time Transport Protocol (SRTP) provides confidentiality, message authentication, and replay protection for the Real-time Transport Protocol (RTP) traffic. There are common encryption algorithms that have been developed to protect data such as advanced encryption algorithm (AES). Chaotic encryption is new trend in cryptography based on chaos theory. Chaos is a class of complex behaviors that can emerge from nonlinear dynamical systems. A distinctive and readily observable property of chaotic systems is sensitive dependence on initial conditions. The main purpose of this paper is to propose an alternative scheme to provide confidentiality in SRTP using chaotic systems. The proposed scheme is implemented using Microsoft open source project for conference. The Chaos Based SRTP (CSRTP) is tested using StsGui NIST Statistical suite and Cryptool software [3] for security while Wireshark [4] is used for quality of service (QoS) analysis. The results related to CSRTP shows its superiority in terms of confidentiality and quality of service (QoS) compared with conventional SRTP protocol.**

***Index Terms*– Chaos, Real-time Transport Protocol (RTP), Real-Time Transport Control Protocol (RTCP), Secure Real-Time Transport Protocol (SRTP), Advanced Encryption Standard (AES), Authentication and Integrity**

I. INTRODUCTION

REAL-time Transport Protocol (RTP) is the Internet Engineering Task Force (IETF) standard [1], which is intended to provide end-to-end network transport functions suitable for applications transmitting real-time data, such as audio, video over multicast or unicast network services. RTP protocol suite consists of two parts; RTP and Real-Time Transport Control Protocol (RTCP). RTP is designed to carry real time data, while RTCP is used to monitor the quality of service and convey information about the participants in on-going session. RTP is susceptible to several attacks [10], including third-party snooping of private conversations, injection of forged content, and modification of packets to degrade voice quality. Several security protocols are used for network security including Internet Protocol Security (IPSec) [5], Secure Socket Layer (SSL)/Transport Layer Security (TLS) [6], and Secure Real-Time Transport Protocol (SRTP). Security services could be achieved using Internet Protocol Security (IPSec), the cost here is the added latency and it must be applied on a hop-by-hop basic. TLS is not suitable for real-time traffic and is only applied to TCP connections [7]. SRTP is the Internet Engineering Task Force (IETF) standard [2]. It provides confidentiality, message authentication, and replay protection for RTP traffic and it is suitable for real-time traffic. The SRTP RFC3711 specifies Advanced Encryption Standard (AES) algorithm [8] for encrypting RTP payload. The authentication of the header and the encrypted payload is computed using HMAC-SHA1 [9]. Several enhancements of authentication on SRTP have been proposed [11]. The combination of chaotic theory and cryptography forms an important field of information security. The characteristics of chaotic signals make chaos a robust cryptosystem against statistical attacks. Due to some inherent features of images like bulk data capacity and high data redundancy, it is difficult to handle them by traditional encryption methods [12]. In this paper we introduce a novel technique for securing images and videos based on SRTP protocol and chaotic systems (CSRTP). The paper is organized as follows: Section 2 introduces SRTP packet format and processing. Chaotic systems are introduced in Section 3. The proposed scheme (CSRTP) is introduced in section 4. Results and comparison with standard SRTP are given in section 5. Section 6 is the conclusion.

II. SRTP OVERVIEW

In this section we introduce the standard SRTP packet format, SRTP packet processing and confidentiality in SRTP as describe in RFC3711.

A. SRTP Packet Format

Fig. 1 shows the SRTP packet format, the packet consists of header, encrypted payload and the authentication code.

The header fields are:

- Version (V): indicates the version of RTP used (now version 2).
- Padding (P): indicates the padding, additional information on the header (payload encrypted case).
- Extension (X): indicates the presence of the header extension.
- CSRC Count (CC): The contributing source (CSRC) count contains the number of CSRC identifiers that follow the fixed header.

- Marker (M): It is intended to allow significant events such as frame boundaries to be marked in the packet stream.
- Payload (PT): this field identifies the format of the RTP payload.
- Sequence number: the sequence increments by one for each RTP data packet sent, and may be used by the receiver to detect packet loss, and to restore packet sequence. The initial value of the sequence number should be random.
- Timestamp: contains the time SRTP data are sent and is used to overcome jitter and synchronization problems.
- Synchronization source SSRC identifier: This identifier should be chosen randomly, is used to distinguish each RTP stream from another on the same session (overcome RTP stream conflict).
- Master Key Identifier (MKI): The MKI identifies the master key from which the session keys were derived.
- Authentication tag: configurable length, recommended. The authentication tag is used to carry message authentication data for RTP header and the encrypted portion of the SRTP packet.

In SRTP, for each packet, the authentication code of the entire header and encrypted payload is computed using HMAC-SHA1 algorithm.

B. SRTP Packet Processing

Fig. 2 shows SRTP packet processing on sender side.The sender determine the index of the SRTP packet using the rollover counter and the sequence number, then encryption key and authentication key are derived using the index and the master key (and master salt), then encrypt the RTP payload, for message authentication, compute the authentication tag for the encrypted portion of the packet, and then append the authentication tag to the packet. If necessary, update the ROC and send the packet. Rollover counter is a 32 bit length, which records the number of times the sequence number has been reset to zero after passing through 65,535.

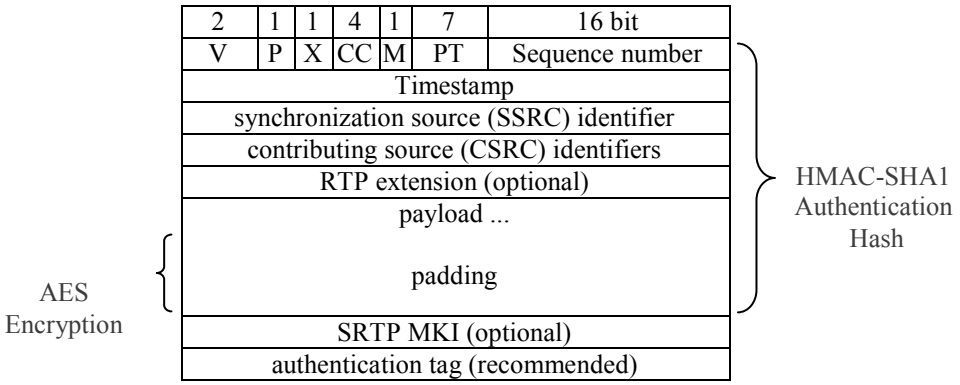

Fig. 1. The format of an SRTP packet

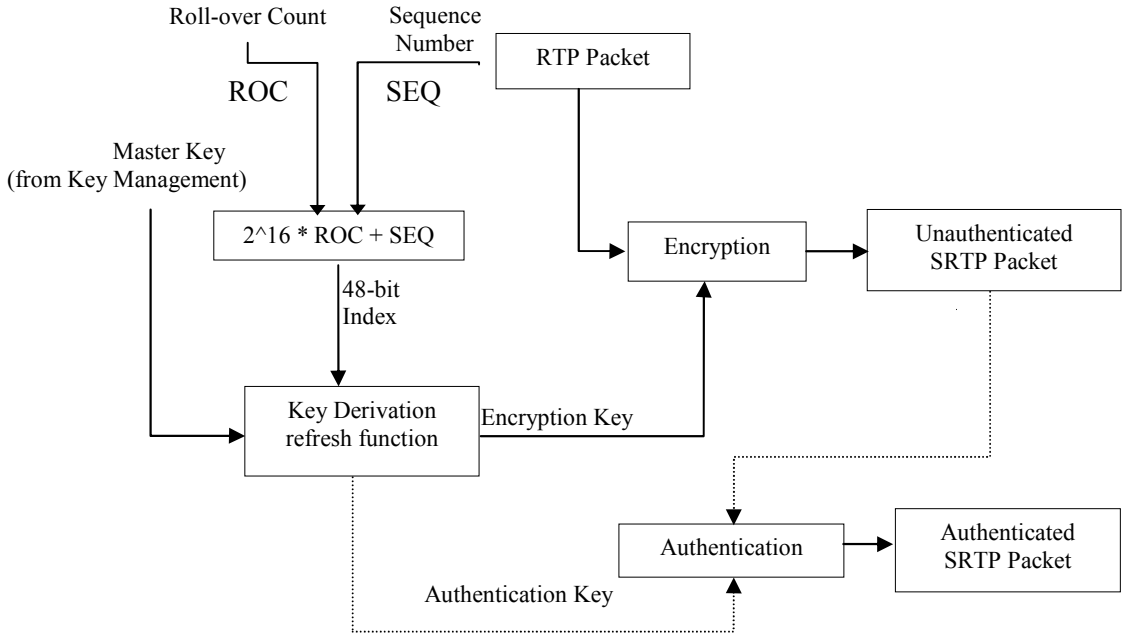

Fig. 2. SRTP packet processing on sender side

Fig. 3 shows SRTP packet processing on receiver side. In the receiver side the packet index is calculated using the rollover counter and sequence number. The encryption and authentication keys are derived using the index and the master key. The authentication tag of the received packet is computed using the predefined algorithm (HMAC-SHA1) and compares with the tag of the received message. The data is authentic if both the tags are the same then decrypt the encrypted portion of the packet. Otherwise it is invalid and then the packet is rejected.

C. Confidentiality in SRTP

Fig. 4 shows encryption in SRTP using AES algorithm in counter mode of operation. In counter mode each packet is encrypted with a different key stream. The key stream is pre-computed since it is not depend on the payload of the packet. The payload is divided into multiple of 128 bits because the block size of AES is 128 bits.

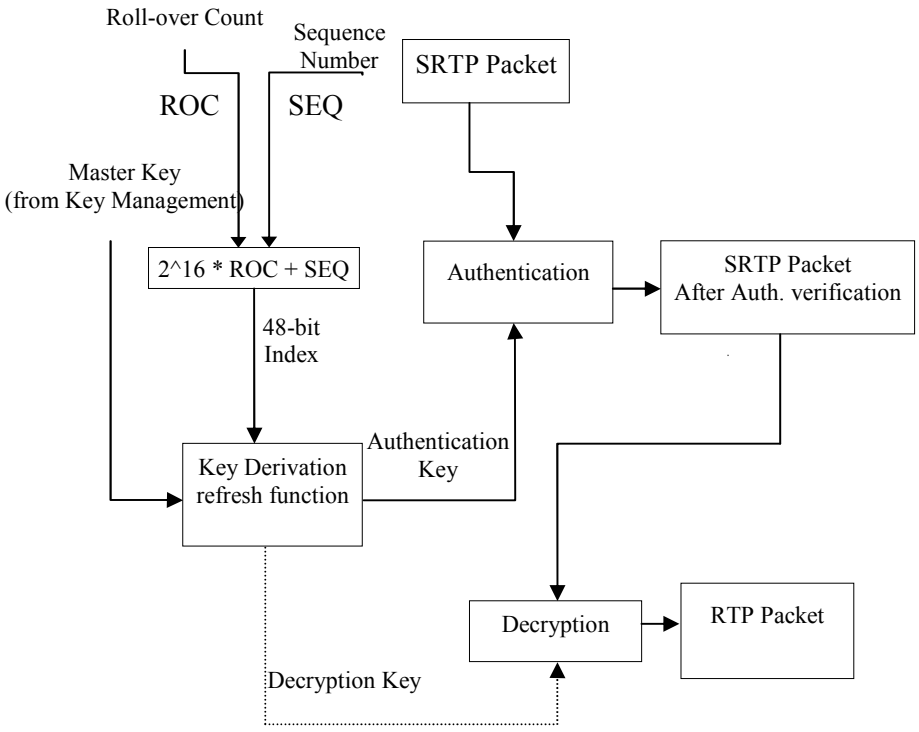

Fig. 3. SRTP packet processing on receiver side

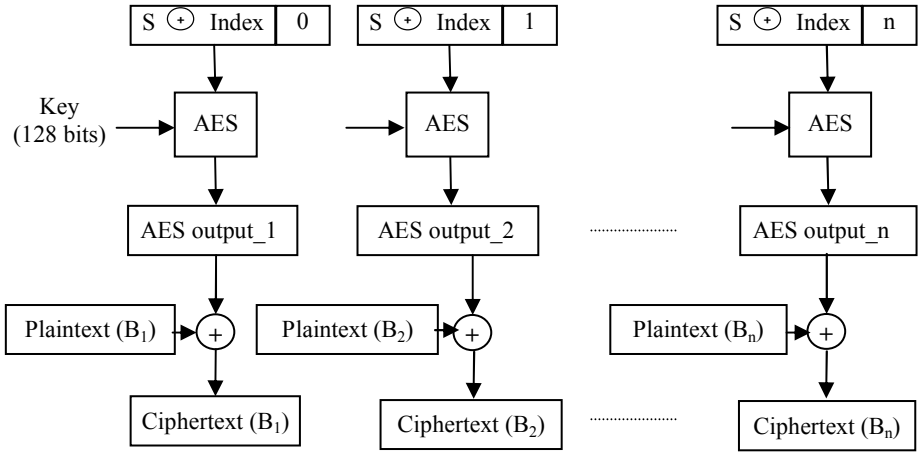

Fig. 4. Default encryption in SRTP

Where, Index: index (sequence number of RTP packet which is 48 bits length) and S: salt (randomizer up to 112 bits).

D. SRTP Weakness

SRTP uses AES algorithm for encrypting the payload (plaintext data). The block size of input plaintext should be multiple of 128 bits. If the payload is not multiple of 128 bits then padding is needed for the payload. This causes several risks in SRTP protocol [RFC3711].The attacker uses this information to predict the plaintext data.

III. CHAOTIC SYSTEM

Chaos Systems are nonlinear dynamical systems. Depending on the time range they are described by difference equations (discrete-time systems) or differential equations (continuous-time systems). Henon map [14], logistic map [15] and Couple Chaotic Systems Based Pseudo Random Generator (CCSPRBG) [16] are example of discrete-time systems. Rossler system [17] and the Lorenz system [18] are example of The continuous-time systems. Chaotic System is sensitive to initial condition, this means that the different initial condition produces different trajectory, the same conditions can produce the same trajectory. Lyapunov Exponents is used to define if the system has chaotic behavior or not. If the system is chaotic the difference between two trajectories with close initial condition will exponentially increase after a very short time. The difference is defined using the following equation [13]:

$$d_t=d_0\, 2^{\lambda t} \quad (1)$$

where:

d_0: is initial distance.

d_t: is the distance at t time.

λ: is Lyapunov Exponents.

The value of Lyapunov Exponents (λ) is solved by averaging the points, using the following equation [13]:

$$\lambda = \frac{1}{t_N - t_0} \sum_{k=0}^{N} \log_2 \frac{d(t_k)}{d(t_{k-1})} \quad (2)$$

Where:

N: the number of points.

t_0: time at initial point.

t_N: time at point N.

$d(t_k)$: the distance at point k.

$d(t_{k-1})$: the distance at point k-1.

λ: is Lyapunov Exponents.

If $\lambda > 0$ the system is considered as chaotic however if $\lambda \leq 0$ the system has a regular motion and is not chaotic.

A. The Lorenz System

Lorenz system was created to analyze the unpredictable behavior of the weather. By greatly simplifying and truncating a set of nonlinear partial differential equations. The system is described by the following differential equations [18]:

$$\begin{aligned} \dot{x} &= \sigma (y - x) \\ \dot{y} &= \gamma x - y - xz \\ \dot{z} &= xy - bz \end{aligned} \quad (3)$$

Fig. 5(a) shows the states variables of Lorenz system.

A typical Lorenz chaotic attractors are shown in figure (5.b) attractors are plotted with parameters $\sigma = 10, \gamma = 28$, and b=8/3 with initial conditions (x_0; y_0; z_0)=(1; 1; 1). Note that the Lorenz equation has three parameters and two nonlinearities (*xz* and *xy*), each of which is a function of two variables [19]. The theoretical Lyapunov exponent for the Lorenz system is equal to1.5 [20].

IV. PROPOSED CHAOTIC ENCRYPTION SYSTEM (CSRTP)

This section describes the proposed chaotic encryption system to provide confidentiality in SRTP. Encryption using chaotic system needs defining the mapping scheme for trajectory, choosing valid initial condition and parameters, then generating random number sequence (PRN), and storing this sequence, encrypting message based on random number sequence. Decryption process is started by using the same initial condition and parameters to generate the same PRN and then decrypting the cipher text. The initial condition and parameters are considered as keys.

The chaotic system must pass NIST statistical test, the chaotic system is based on 3 dimensions chaotic system which is Lorenz system, but the normal 3 dimensions system doesn't pass NIST statistical tests. The proposed modification in Chaotic system is based on random initial conditions, and the good choice for initial condition is sequence number which is random number. Fig. 6 shows Encryption/Decryption processes, that are performed through the following steps:

1) Determine the sequence of the SRTP packet.
2) Generate initial condition form sequence number.
3) Generate PRN using chaotic system.

Apply XOR function between PRN and RTP traffic to produce SRTP packets.

Table 1 shows the basic differences between CSRTP and SRTP.

One more advantage for the use of the proposed CSRTP is that the output of chaotic system is based on sequence number as initial conditions. The initial conditions in chaotic encryption are random values for each packet; this means that the proposed chaotic encryption has more randomness which increases confidentiality in SRTP.

V. PERFORMANCE AND SECURITY ANALYSIS

A. Test Bed Configuration

The test bed is composed of a network with three endpoints (PC1, PC2, and PC3) and Layer three-switch supporting SPAN (mirror) port as shown in Fig. 7. Two computers are used for real-time transmission and the third for interception. Each computer has the following parameters: 3 GHz (CPU), 1 Gbytes RAM, network card of 1Gbps data rate and

Windows Xp operating system. Also each computer has an external microphone and speaker for voice and camera for video. CSRTP is implemented using Visual C#. net 2008. Two buffers are used one for send/receive and the second for processing. The size of the Payload for testing is 1440 bytes.

B. Security Analysis

The security analysis will be performed using (StsGui) suite [21] and Diehard software [22] to perform the randomness tests.

1) Randomness Test using NIST

Table 2 gives the P-value of NIST randomness tests for AES encryption in counter mode and chaotic encryption in SRTP. The threshold level to pass test is P-value= 0.01. The NIST statistical tests for generated Pseudo Random Number (PRN) using chaotic system are passed. The test results given in Table 2 and Table 3 show that encryption using chaotic system (CSRTP) are passed all tests while encryption using AES algorithm in counter mode fails in universal statistic and rank test.

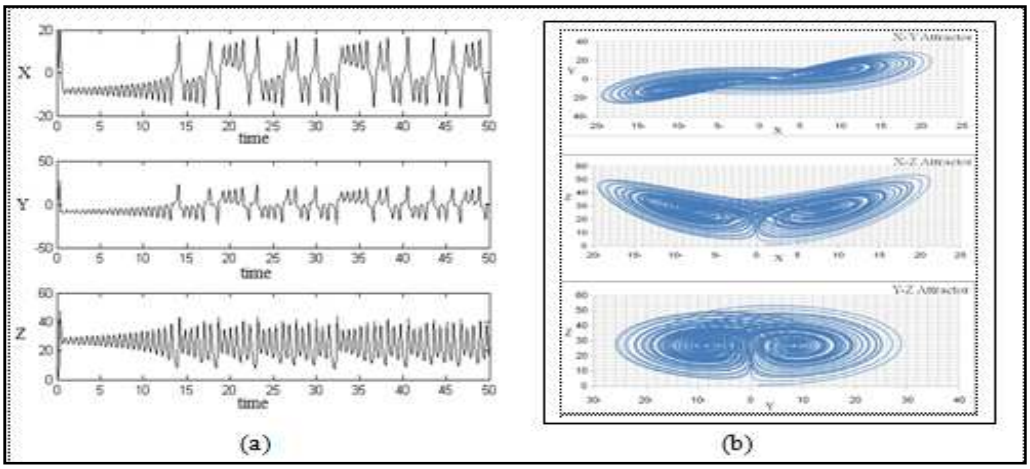

Fig. 5. (a) The states variables of Lorenz system, and (b) Attractors of Lorenz system

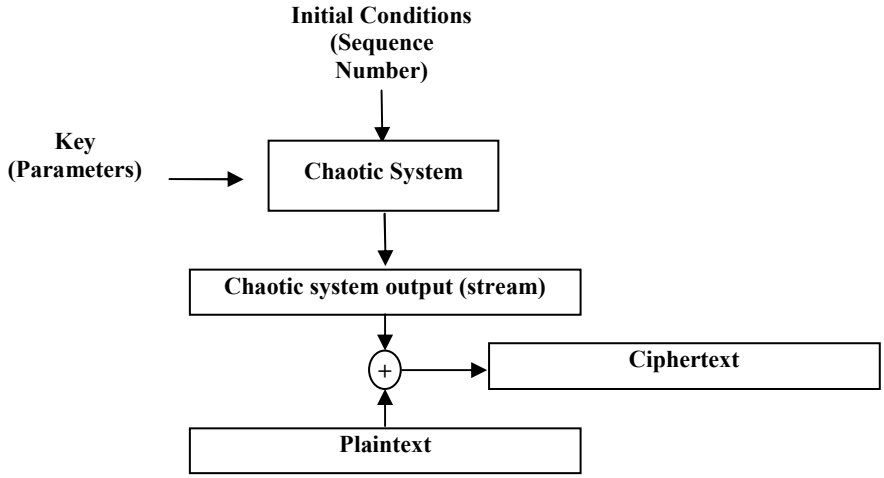

Fig. 6. Encryption in CSRTP

Table 1. Comparison between CSRTP and SRTP

0	CSRTP	SRTP
Encryption time	The time required for encryption is smaller	The time required for encryption is larger.
Padding	No padding because the length of chaotic system output is variable.	SRTP needs padding when the length of payload is not multiple of 128 bits.
Real-time application	chaotic system is stream oriented which is suitable for real-time traffic	AES is block cipher which is less suitable for real-time traffic

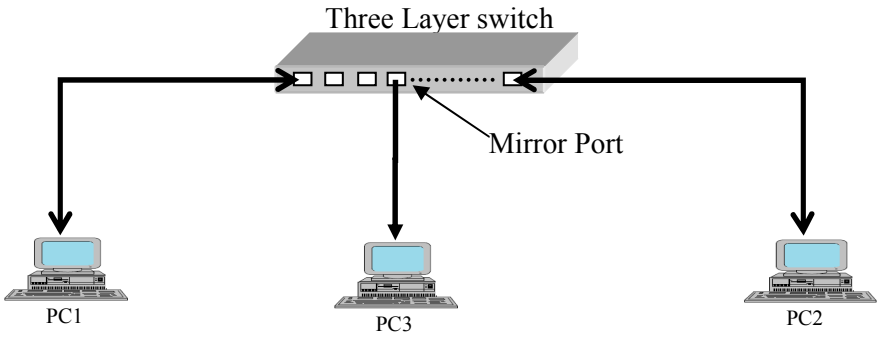

Fig. 7. Test Bed Hardware

Table 2. P-value of NIST randomness tests for AES encryption and chaotic encryption

Test	Standard (AES)		Proposed (Chaotic)	
	P-Value	Result	P-Value	Result
Block frequency	0.639202	Passed	0.842082	Passed
Non–overlapping Template Matching	0.999524	Passed	0.998222	Passed
Overlapping Template Matching	0.151616	Passed	0.517109	Passed
Universal statistic	0.001538	Not Passed	0.644407	Passed
Approximate Entropy	0.710580	Passed	0.012920	Passed
Serial	0.681789	Passed	0.731886	Passed
Linear complexity	0.312291	Passed	0.684890	Passed
Frequency	0.225409	Passed	0.984178	Passed
Cumulative sums (Forward) (Reverse)	0.453113 0.369424	Passed	0.691081 0.419021	Passed
Runs	0.825505	Passed	0.582113	Passed
Longest runs of ones	0.093720	Passed	0.188601	Passed
Discrete Fourer Transform	0.440975	Passed	0.433590	Passed
Random Excursions	0.881711	Passed	0.797979	Passed
Random Excursions Variant	0.958959	Passed	0.783443	Passed
Rank	0.004749	Not Passed	0.598656	Passed

Table 3 gives randomness test of AES algorithm using Diehard battery.

Table 4 gives randomness of Chaotic encryption using Diehard battery. The results show that the output of chaotic encryption is better than AES.

The results of randomness tests (NIST suite and Diehard battery) show that chaotic encryption using Lorenz system with random initial conditions (based on sequence number) satisfies requirement for randomness test. The results show that chaotic encryption has good randomness properties. We can conclude from All these that chaotic system is more adequate for encryption in SRTP.

2) Image Histogram Test

To perform this test, An image (plain image) is encrypted using chaotic-system and AES algorithm. Then the histograms for both ciphers are calculated. Fig.(8) shows the original image (plain image), image encrypted using AES algorithm and chaotic system. The histograms of the two ciphered images are nearly the same and fairly uniform and significantly different from the original image. Therefore, they do not provide any indication to employ any statistical attack.

3). Image Encryption Quality Analysis

Most of previous studies on image encryption were based on the visual inspection to judge the effectiveness of the encryption technique used in hiding features. Visual inspection is insufficient in evaluating the amount of information hidden. So, we need to have a quantitative measure to evaluate the degree of encryption quantity, which we will call the encryption quality. The main goal here is to use a mathematical model for the measurement of the amount of encryption quantity of chaotic and to compare it with that of AES. In all experiments, we use the grey-scale images (Plain Image), of size grey-scale (0-255) as the original images (plain images).

With the application of encryption to an image a change takes place in pixels values as compared to those values before encryption. Such change may be irregular. This means

that the higher the change in pixels values, the more effective will be the image encryption and hence the encryption quality. So the encryption quality may be expressed in terms of the total changes in pixels values between the original image and the encrypted one. A measure for encryption quality may be expressed as the deviation between the original and encrypted image. The quality of image encryption may be determined as follows:

Let F, F' denote the original image (plain image) and the encrypted image (cipher image) respectively, each of size M*N pixels with L grey levels. $F(x, y)$, $F'(x, y) \in \{0,.., L-1\}$ are the grey levels of the images F , F' at position (x, y) , $0 \le x \le M-1$, $0 \le y \le N-1$. We will define $H_L(F)$ as the number of occurrence for each grey level L in the original image (plain image), and $H_L(F')$ as the number of occurrence for each grey level L in the encrypted image (cipher image). The encryption quality represents the average number of changes to each grey level L and it can be expressed mathematically as:

$$\text{Encryption Quality} = \frac{\sum_{l=0}^{255} | H_L(F') - H_L(F) |}{256} \quad (4)$$

Table 5 gives the results of Encryption quality of AES and chaotic for an image file (Plain Image), From the results we can conclude that confidentiality in SRTP using Lorenz system (CSRTP) is higher than confidentiality using AES algorithm (SRTP)

Table 5. Encryption Quality of AES and chaotic

AES Algorithm	Chaotic System
4462.7	**4471.1**

C. Quality of Service (QoS) Analysis

The QoS performance is calculated in terms of delay and jitter.

1) Delay Calculations and Measurement

The total acceptable delay for a VoIP packet is 150ms [8]. The delays are classified into call setup delay and delays during call. The call setup delay (T_{cs}) that happens before the actual call, generally consists of:

- The signaling delays caused by signaling protocol.
- Initial key exchange delay.

The possible delays during call are:

- The encryption delay (T_{enc}).
- The authentication delay (T_{aut}).
- The authentication verification delay ($T_{aut\text{-}ver}$).
- The decryption delay (T_{dec}).
- The coding/decoding delays ($T_{c/d}$).
- The network delays (T_{net}).

The per-packet call delay for SRTP is calculated as below:

$$\text{Call Delay} = T_{enc} + T_{aut} + T_{aut\text{-}ver} + T_{dec} + T_{net} + T_{c/d} \quad (5)$$

T_{enc} for chaotic encryption system is changed.

Table 6 gives the total delay for five samples, each sample consist of 500 packets for SRTP and CSRTP. The measurement is done using Wireshark software. The results indicate that the average delay for CSRTP is less than SRTP.

Table 6. Delay for SRTP and CSRTP

	Max delay (ms)					Average
	1	2	3	4	5	
SRTP	143.09	142.07	141.37	141.13	142.32	141.996
CSRTP	142.07	140.71	140.61	140.14	140.11	140.728

2) Jitter Calculations and Measurement

RFC 3550 defines an formula for jitter calculation as the following:

$$J(i) = J(i-1) + (|D(i-1,i)| - J(i-1))/16 \quad (6)$$

Where:

D(i-1, i): The Relative Transit Time of two consecutive packets.

i: Current packet index.

i-1: Previous packet index.

J(i): Current jitter.

J(i-1): Previous jitter.

Table 7 gives the total jitter for five samples, each sample consist of 500 packets for SRTP and CSRTP. The measurement is done using Wireshark software. The results indicate that the jitter for CSRTP is less than SRTP.

Table 7. Jitter for SRTP and CSRTP

	Max Jitter (ms)					Average
	1	2	3	4	5	
SRTP	465.31	466.65	465.76	465.47	465.36	465.71
CSRTP	465.77	465.60	465.20	465.06	465.02	465.33

Decreasing in delay and jitter using chaotic system encryption is due to decrease in time needed for encryption compared to AES algorithm.

VI. CONCLUSIONS AND FUTURE WORKS

This paper presents an alternative encryption technique to enhance confidentiality and quality of service for SRTP protocol which make it more suitable for secure real time applications. The proposed system is based on Lorenz chaotic generator and SRTP sequence number for generating random initial condition. The chaotic encryption is implemented using C#.net and Microsoft open source for conference. Evaluation and comparison with standard SRTP are achieved using statistical test suites (NIST, Diehard) for randomness tests, and using Wireshark for QoS. The results indicate that encryption/decryption time in CSRTP is less than the encryption/decryption time in SRTP. The conclusion is that chaotic system encryption using Lorenz with random initial conditions enhances QoS and security of SRTP protocol. Future work includes using of public key cryptosystem based on chaotic systems to solve the problem of key exchange.

Table 3. Randomness tests of AES encryption using Diehard battery

No	Test name	Corresponding P-values (pass threshold=0.01)
1	Birthday spacing	0.448247
2	Overlapping, permutations	(0.369184)(0.313739)
3	Binary rank (31x31)(32x32) (6x8)	(0.947187)(0.501032)(0.848022)
	Monkey	
4	The bitstream	(0.6928),(0.3848),(0.1748),(0.2342),(0.8996), (0.1323),(0.0752),(0.0072),(0.2904),(0.0726), (0.9190),(0.1426),(0.4246),(0.1979),(0.9491), (0.9303),(0.7499),(0.7667),(0.9351),(0.7082)
5	Overlapping- Pairs-Sparse-Occupancy (OPSO)	(0.6813),(0.2902),(0.7756),(0.4002),(0.4529) (0.8799),(0.4149),(0.9121),(0.7630),(0.9317) (0.6911),(0.3869),(0.4734),(0.2438),(0.4529) (0.1347),(0.7767),(0.7928),(0.3204),(0.8887) (0.1175),(0.8063),(0.8308)
6	Overlapping-Quadruples-Sparse-Occupancy (OQSO)	(0.2047),(0.0879),(0.7432),(0.0912),(0.5735) (0.1642),(0.0110),(0.5588),(0.7966),(0.5735) (0.2761),(0.2390),(0.2038),(0.9095),(0.8546) (0.2453),(0.4577),(0.7011),(0.4032),(0.9535) (0.3330),(0.8302),(0.5077),(0.0605),(0.3593) (0.8652),(0.4510),(0.0669)
7	DNA	(0.5872),(0.3702),(0.3470),(0.8577),(0.8241) (0.9057),(0.0066),(0.5314),(0.2392),(0.3481) (0.6958),(0.4109),(0.2266),(0.2092),(0.5687) (0.7817),(0.1432),(0.3405),(0.4937),(0.2933) (0.9686),(0.4784),(0.7885),(0.1542),(0.1393) (0.1577),(0.8068),(0.2588),(0.8101),(0.3938) (0.1754)
8	Count the 1's	
	(i) in stream of Bytes	(0.258671),(0.331037)
	(ii) for specific Bytes	(0.7201),(0.6738),(0.9760),(0.0482),(0.1445) (0.2038),(0.1105),(0.3287),(0.9124),(0.5557) (0.8902),(0.8519),(0.3983),(0.5373),(0.6874) (0.5035),(0.9771),(0.4648),(0.1431),(0.6103) (0.7174),(0.2200),(0.8603),(0.2633),(0.7450)
9	Parking lot	0.369257
10	The minimum distance	0.981738
11	The 3D spheres	0.118070
12	The sqeeze	0.804748
13	The overlapping Sums	0.561564
14	The runs (i) Up - (ii) Down	(0.846439),(0.188485)-(0.424875),(0.201659)
15	The craps	(0.466389)

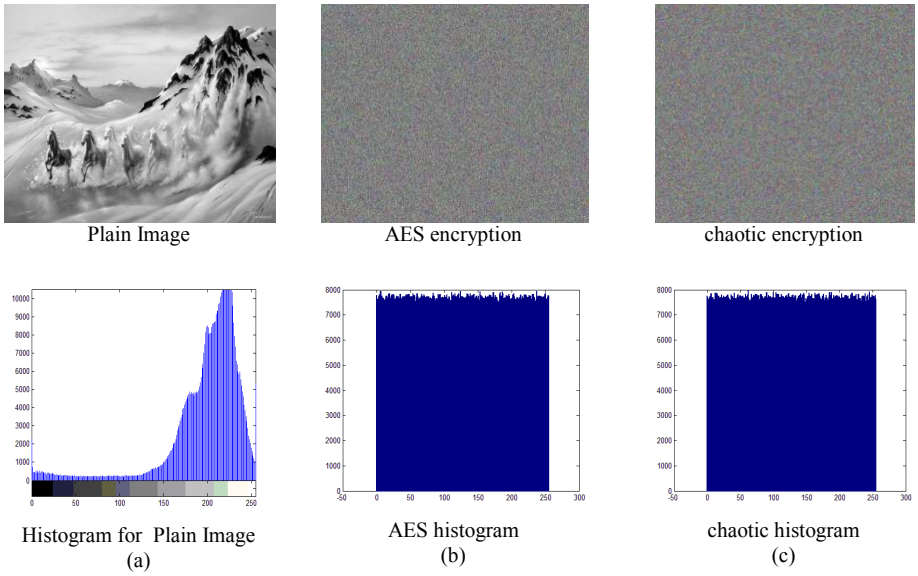

Fig. 8. Histograms of plain image, AES algorithm, and chaotic system

Table 4. Randomness tests for chaotic encryption using Diehard battery

No	Test name	Corresponding P-values (pass threshold=0.01)
1	Birthday spacing	1.000000
2	Overlapping, permutations	(0.319361)(0.014835)
3	Binary rank (31x31)(32x32) (6x8)	(0.407781)(0.451011)(0.357552)
	Monkey	
4	The bitstream	(1.0000),(1.0000),(1.0000),(1.0000),(1.0000), (1.0000),(1.0000),(1.0000),(1.0000),(1.0000), (1.0000),(1.0000),(1.0000),(1.0000),(1.0000), (1.0000),(1.0000),(1.0000),(1.0000),(1.0000),
5	Overlapping- Pairs-Sparse-Occupancy (OPSO)	(0.4940),(0.8729),(0.1634),(0.6175),(0.8919), (0.8671),(0.1810),(0.5869),(0.5325),(0.1083), (0.7288),(0.8015),(0.1931),(0.2459),(0.4474), (0.7868),(0.1643),(0.0712),(0.8874),(0.9816), (0.6739),(0.9473),(0.4611)
6	Overlapping-Quadruples-Sparse-Occupancy (OQSO)	(0.5023),(0.9328),(0.2125),(0.1433),(0.0281), (0.0386),(0.3342),(0.7718),(0.0106),(0.1650), (0.6142),(0.1625),(0.3479),(0.4874),(0.5907), (0.8106),(0.9056),(0.7047),(0.2627),(0.1488), (0.4591),(0.0152),(0.4230),(0.8079),(0.6246), (0.2853),(0.3979),(0.1351)
7	DNA	(0.2050),(0.9555),(0.1260),(0.6738),(0.2714), (0.7702),(0.5055),(0.0125),(0.6864),(0.3525), (0.8661),(0.3859),(0.6533),(0.4236),(0.6213), (0.6235),(0.3035),(0.0170),(0.6727),(0.3255), (0.0186),(0.9096),(0.4236),(0.9550),(0.4984), (0.2733),(0.8264),(0.9463),(0.8203),(0.2953), (0.6446)
8	Count the 1's	
	(i) in stream of Bytes	(1.000000),(0.999998)
	(ii) for specific Bytes	(0.9178),(0.9994),(0.9868),(0.7109),(0.7396), (0.9940),(0.8501),(0.9721),(0.4409),(0.4178), (0.6309),(0.9975),(0.7767),(0.7323),(0.4300), (0.9606),(0.1638),(0.4016),(0.3193),(0.7875), (0.9601),(0.3125),(0.4079),(0.4410),(0.3599)
9	Parking lot	0.432345
10	The minimum distance	0.461526
11	The 3D spheres	0.046207
12	The sqeeze	0.337988
13	The overlapping Sums	0.337542
14	The runs (i) Up - (ii) Down	(0.554520),(0.414288)-(0.116676),(0.213462)
15	The craps	(0.822895)

REFERENCES

[1] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", IETF RFC 3550, July 2003.

[2] M. Baugher, D. McGrew, E. Carrara, M. Naslund, and K. Norrman, "The Secure Real-time Transport Protocol", IETF RFC 3711, March 2004.

[3] Educational Tool for Cryptography and Cryptanalysis, for Windows, "URL:http://www.cryptool.com".

[4] The Network Protocol Analyzer for Windows and Unix, June 2008, "URL:http://www.wireshark.org".

[5] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol", IETF RFC 2401, November 1998.

[6] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol", IETF RFC 4346, April 2006.

[7] D.Kuhn, T.Walsh, and S.Fries, "Security Considerations for Voice Over IP Systems", Recommendations of the National Institute of Standards and Technology, ITU publications, June 2005.

[8] National Institute for Standards and Technology (NIST), "Advanced Encryption Standard (AES)", FIPS Pub 197, November 2001.

[9] H. Crawczyk, M. Bellare and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", IETF RFC 2104, February 1997.

[10] M.Adams and M.Kwon, "Vulnerabilities of the Real-Time Transport (RTP) Protocol for Voice over IP (VoIP) Traffic", Proceedings of IEEE Consumer Communications and Networking Conference. Held at Harrah's Las Vegas, Nevada: 9- 12 January 2009.

[11] M.Mohammed, A.Rohiem and A.El-moghazy, "Enhancement Packet Authentication and integrity in SRTP Protocol", Proceedings of the 7th ICEENG Conference, 25-27 May, 2010.

[12] Musheer Ahmad, "A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping", International Journal on Computer Science and Engineering, Vol.2 (1), 2009.

[13] Wolf, J. B. Swift, H. L. Swinney, and J. A. Vastano, "Determining Lyapunov exponents from a time series", Physica D, 1985.

[14] M. Henon,"A two-dimensional mapping with a strange attractor", Commun.Math. Phys, 1976.

[15] J. M. H. Elmirghani, R A. Cryan and S. H. Milner, "Performance of a novel echo cancellation strategy based on chaotic modulated speech", Proc. SPIE (special issue for chaotic circuits for communication), vol. 2612, pp. 158-169, Oct. 1995.

[16] Sh. Li, X. Mou and Y. Cai, "Pseudo-Random Bit Generator Based on Couple Chaotic Systems and its Applications in Stream-Cipher Cryptography", Indocrypt 2001, vol. 2247, pp. 316-329, Springer-Verlag, Berlin, 2001.

[17] Rossler and O. E., "An Equation for Continuous Chaos", Phys. Lett. A, vol. 57, pp. 397-398, 1976.

[18] C. Sparrow, "The Lorenz Equations in Chaos", Princeton University Press, 1986.

[19] J.C. Sprott, "Algebraically Simple Chaotic Flows", International Journal of Chaos Theory and Applications, Volume 5, 2000.

[20] T. Kilias, K. Kelber, A. Mogel and W. Schwarz, "Electronic chaos generators- Design and applications," Int. j. Electron. , 1995.

[21] The NIST Statistical Test Suite, "URL:http://csrc.nist.gov ", 2005.

[22] The Diehard Battery of Tests of Randomness, "URL: http://www.stat.fsu.edu ", 1997