Military Technical College
Kobry El-Kobba,
Cairo, Egypt

11-th International Conference
on Aerospace Sciences &
Aviation Technology

CHAOTIC CRYPTOSYSTEM USING THE AES ENCRYPTION ALGORITHM AS ENCRYPTION AND DECRYPTION RULE

Shehata A. R. *, Elagooz S.S. *, and Dahshan H. M.*

ABSTRACT

Chaos and cryptography have some common features, such as sensitivity to variables and parameters change. Many fundamental characteristics of chaos, such as the ergodicity and mixing property and the sensitivity to initial conditions can be connected with the "confusion" and "diffusion" property in cryptography. A combination between cryptosystems realized in analog circuits and conventional cipher has been made by using the AES as the encryption and decryption rule in the chaotic cryptosystem based on chaos synchronization techniques. The proposed algorithm has been simulated and applied in encrypting and decrypting images. The results show that encrypted data have passed all statistical tests and the confusion and diffusion properties have also been demonstrated by testing the histograms of the ciphered images and calculating the amount of correlations between the adjacent pixels in the ciphered image.

KEY WORDS: Chaos, AES, and Synchronization.

* Egyptian Armed Forces

I. Introduction

Recently, synchronization of chaotic systems and its application to secure communications have received considerable attention. Different methods have been developed in order to hide the contents of a message using chaotic signals. However, the attacks proposed in [1-5] have shown that most of these methods are not secure or have a low security. These considerations have led to propose a new chaos-based secure communication scheme [6], [7]. Fig.1. shows the block diagram of the chaos-based cryptosystem noises.

Once a connection has been established between the transmitter and the receiver, the transmitter generates chaos and transmits one of its state variables to the receiver. The received signal is used to drive the system and generates another set of chaos on the receiver side. After synchronization between the transmitter and the receiver is completed, it is just a simple matter to add data at the transmitter side and subtract the identical chaos on the receiving side. The random appearance of the signal makes it less vulnerable to intruders. Hence the data on a shared medium is nothing but garbage for the intruder. But the same data when received at the destination can be decrypted using the corresponding reverse process.

Another aspect of the synchronized chaos is that the intruder has to coincide to the time in which the transfer between two nodes takes place. If it is not the case, the intruder cannot synchronize completely. Hence it may be stated that the system security increases as the time of transmission increases and it becomes difficult to remain in synchronization for an unwanted user and this in turn guarantees security.

The aim of this paper is to present a method that can be used in order to increase the communication security. The proposed method combines the conventional cipher (AES encryption algorithm) with the synchronization of chaotic systems. The paper is organized as follows: section one is an introduction. In section two, the proposed algorithm is designed. In section three, the proposed algorithm is simulated and applied in encrypting and decrypting images. In section four, the confusion and diffusion properties are demonstrated by testing the histograms of the ciphered images and calculating the amount of correlations between the adjacent pixels in the ciphered image. In chapter five, large numbers of encrypted data are tested using the NIST statistical tests for randomness. Section six is a conclusion.

II. DESIGN APPROACH

In order to hide the contents of a message using chaotic signals, the chaotic systems involve two chaotic signals. The first signal is used for the chaotic encryptor and decryptor synchronization and the other signal is used as a key signal of the AES encryption algorithm.

The intruder needs to reconstruct the key signal which is different from the transmitted signal. It seems very difficult to create reconstruction methods in order to obtain the key signal. Such methods have not been reported so far.
The general block diagram of a Chua's circuit-based cryptosystem with the AES encryption algorithm as the encryption and decryption rule is illustrated in Fig.2.

Where $v_R(t)$ is the transmitted signal, $v_2(t)$ is the key signal and $p(t)$ is the plain signal.

The state equations of this cryptosystem are described in Equations (1) and (4).

- For the encryptor:

$$\begin{cases} \dfrac{dv_1}{dt} = \dfrac{1}{C_1}\left[\dfrac{1}{R}(v_2 - v_1) - f(v_R)\right]; \\ \dfrac{dv_2}{dt} = \dfrac{1}{C_2}\left[\dfrac{1}{R}(v_1 - v_2) + i_L\right]; \\ \dfrac{di_L}{dt} = \dfrac{1}{L}(-v_2). \end{cases} \tag{1}$$

where $f(v_R)$ is the nonlinear characteristic of Chua's diode from Chua's circuit, given by [8]:

$$f(v_R) = -2\tanh(0.38 v_R) \tag{2}$$

The voltage vR is given by:

$$v_R = v_1 - e(p(t)), \tag{3}$$

where e(p(t)) represents the encrypted signal.

- For the decryptor:

$$\begin{cases} \dfrac{dv_1}{dt} = \dfrac{1}{C_1}\left[\dfrac{1}{R}(\tilde{v}_2 - \tilde{v}_1) - f(v_R)\right]; \\ \dfrac{dv_2}{dt} = \dfrac{1}{C_2}\left[\dfrac{1}{R}(\tilde{v}_1 - \tilde{v}_2) + i_L\right]; \\ \dfrac{di_L}{dt} = \dfrac{1}{L}(-\tilde{v}_2). \end{cases} \tag{4}$$

$$\tilde{e}(p(t)) = \tilde{v}_1 - v_R$$

where $\tilde{e}(p(t))$ is the encrypted signal, recovered by the receiver.

III. ENCRYPTION PROCESS

The encryption function *e*( ) is done by the AES algorithm. We use the AES with a block length 128-bits and key length128-bits. The encryption process is performed in the following steps:

- The encrypter consists of a chaotic system and an encryption function *e*(t).
- The cryptographic key *k*(t) is one of the state variables of the chaotic system.
- The plain text *p*(t) is converted to blocks each with 128-bit length.
- The key signal *v2*(*t*) is converted to a block with 128-bits length.
- For each time sample a plaintext block is encrypted with a new key block to enhance the security.
- Now, the encrypted signal *e*(*p*(*t*)) is kept not greater than 0.8 volts peak-to-peak.
- The normalized *e*(*p*(*t*)) is mixed with another state variable of the chaotic system and the output is used to synchronize both the encrypter and the decrypter.

- It should be noted that both the encrypted signal $e(p(t))$ and the key signal $v_2(t)$ are not sent to the decrypter.
- Because the encrypted signal is a function of $v_2(t)$ and $p(t)$ and since the encrypted signal is used to drive the Chua's circuit, it hides both the dynamical and the statistical characteristics of $v_2(t)$ and $p(t)$.

IV. DECRYPTION PROCESS

The decryption process is done by the AES encryption algorithm. The decryption process is performed in the following steps:

- The decryptor consists of a chaotic system and a decryption function d( ).
- Only when the decryptor and the encryptor are synchronized, the decryptor can find the encrypted signal and the key signal. Then, the decryption function d( ) is used to decrypt the received signal.
- After synchronization between the transmitter and the receiver is completed, the received signal is subtracted from the same state variable that is mixed with the encrypted signal at the encryptor to obtain $\tilde{e}(p(t))$.
- Each $\tilde{e}(p(t))$ signal is decoded to a block of 128-bits which represent the encrypted block.
- The key signal $\tilde{v}_2(t)$ is taken from the synchronized Chua's circuit at the receiver and converted to 128-bits key to be used by the AES algorithm at the decryptor to decrypt the encrypted block.
- Each received block is decrypted using a new key which is the same as the key used for encryption.

V. SIMULATIONS

A MATLAB® SIMULINK model has been developed to demonstrate the results of encrypting an image using the AES encryption algorithm as the conventional cipher algorithm in the chaotic cryptosystem. Fig.3a shows the Transmitted masked signal. Figure 3b shows the attractor generated by the transmitter. Fig.3c shows the synchronization error between the transmitter and the receiver and it shows that after short transient time the transmitter and the receiver are completely synchronized. Figure 4 shows the synchronization between the transmitter and the receiver for different parameter mismatch values and it is obvious that the parameter mismatch is acceptable for maximum of 5 %. Fig.5. shows an example of encrypting and decrypting an image using the chaotic cryptosystem with the AES as the encryption and decryption rule. The plain image and the decrypted image were compared. The result shows that there are 2 % differences between the two images due to synchronization errors.

VI. IMAGE STATISTICAL ANALYSIS

The encrypted image has good confusion and diffusion properties. These properties have been demonstrated by a test on the histograms of the ciphered images and on the correlations of adjacent pixels in the ciphered image [9].

- Histograms of ciphered images. Select several 256 gray-level images with size of 512 x 512 that have different contents, and calculate their histograms.
- Correlation of two adjacent pixels. To test the correlation between two vertically adjacent pixels, two horizontally adjacent pixels, and two diagonally adjacent pixels in a ciphered image, respectively, the procedure is as follows: First, randomly select 1000 pairs of two adjacent pixels from an image. Then, calculate their correlation coefficient.

Figure 6 shows that the histogram of the ciphered image is fairly uniform and is significantly different from that of the original image. Table 1. shows the correlation coefficients of two adjacent pixels for horizontal, diagonal and vertical directions. Figure 7 shows the correlations of two horizontally adjacent pixels in the plain-image and that in the ciphered-image encrypted by chaotic cryptosystem with AES algorithm. It indicates that the adjacent pixels of the plain image are highly correlated and have correlation coefficient equal to 0.9616. Adjacent pixels of the ciphered image have very low correlation coefficient and equal to 0.001.

VII. STATISTICAL TEST RESULTS

Hundred plaintexts have been encrypted with different keys by the standard AES and the chaotic cryptosystem with the AES as the encryption and decryption rule. The encrypted data have been tested using the NIST statistical tests [10]. Table 2. gives tests results of the standard AES encryption algorithm and the proposed chaotic cryptosystem. PS-value refers to the P-value of the standard AES encryption algorithm. PCS-value refers to the P-value of the chaotic cryptosystem. The two algorithms have passed all tests since all P-values ≥ 0.1. Fig.8. illustrates the P-value of each test in a bar chart and it shows that the proposed chaotic cryptosystem and the standard AES have passed all tests.

VIII. CONCLUSIONS

The AES encryption algorithm has been used as the encryption and decryption rule in the chaotic cryptosystem based on chaos synchronization. The proposed algorithm has been simulated and applied in encrypting and decrypting images. The ciphered images have passed all the NIST statistical tests. The confusion and diffusion properties have also been demonstrated by testing the histograms of the ciphered images and calculating the amount of correlations between the adjacent pixels in the ciphered image.

REFERENCES

[1] Short, K. M., "Steps toward unmasking secure communications", Int. J. Bifurcation Chaos, vol. 4, no. 4, pp. 959–977, 1994.

[2]Shujun et al., "Statistical properties of digital piecewise linear chaotic maps and their roles in cryptography and pseudo-random coding", 8th IMA Int. Conf. Proc., Berlin, Springer-Verlag 2001.

[3] Shannon, C.E., "Communications theory of secrecy system", Bell Systems Tech. J. 28, pp. 656 -715, 1949.

[4] Yaobin Mao,et al., "A Novel Fast Image Encryption Scheme Based on 3D Chaotic Baker Maps", International Journal of Bifurcation and Chaos, June 2003.

[5] Zhou, C. and Chen, T., "Extracting information masked by chaos and contaminated with noise: Some considerations on the security of communication approaches using chaos," Phys. Lett. A, vol. 234, pp. 429–435, 1997.

[6] Yang, T. et al.," Cryptography based on chaotic systems", IEEE Trans. Circuits and System, vol. 44, pp. 469–472, May 1997.

[7] Yang, T. and Chua, L. O., "Impulsive control and synchronization of non-linear dynamical systems and application to secure communication", Int. J. Bifurcation Chaos, vol. 7, no. 3, pp. 645–664, 1997.

[8] Mohamed I. S. and Alaaeldin R. S., "Chaotic algorithms for data encryption", IEEE Int. Conf. Acoustics, Speech, and Signal Processing. (ICASSP 2001), vol. 2, pp. 997–1000, 2001.

[9] Yaobin Mao et al, "A Novel Fast Image Encryption Scheme Based on 3D Chaotic Baker Maps", International Journal of Bifurcation and Chaos, June 2003.

[10] NIST, Special Publication 800-22; A Statistical Test Suite for Random and Pseudo-Random Number Generators for Cryptographic Applications; 2001; Available online at http://csrc.nist.gov/rng/SP800-22b.pdf.

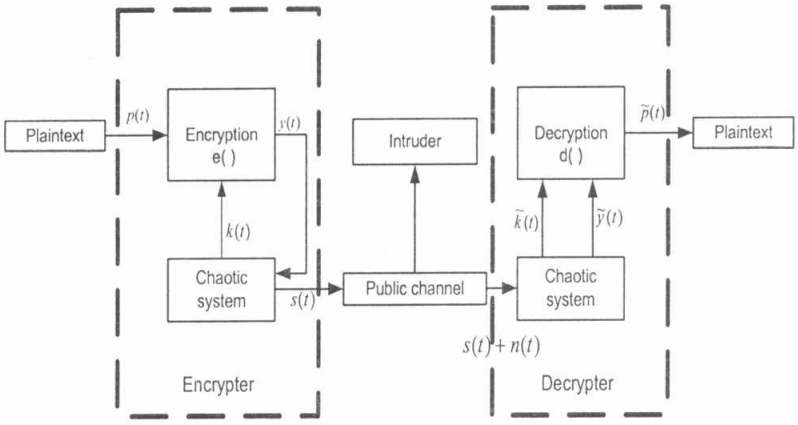


Fig.1. Block diagram of the chaos-based cryptosystem.

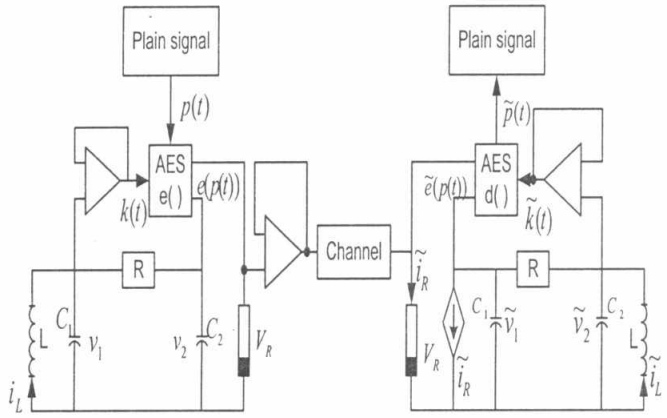


Fig.2. Block diagram of a Chua's circuit-based cryptosystem.

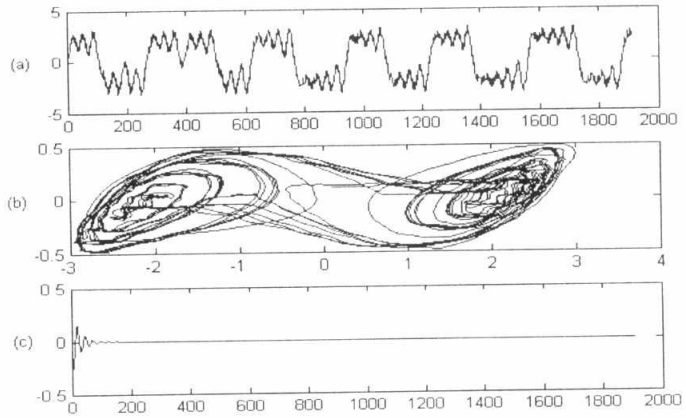


Fig.3. Chaotic cryptosystem simulation results:
(a) Masked signal transmitted in communication channel.
(b) The attractor generated by the transmitter.
(c) Synchronization error between transmitter and receiver.

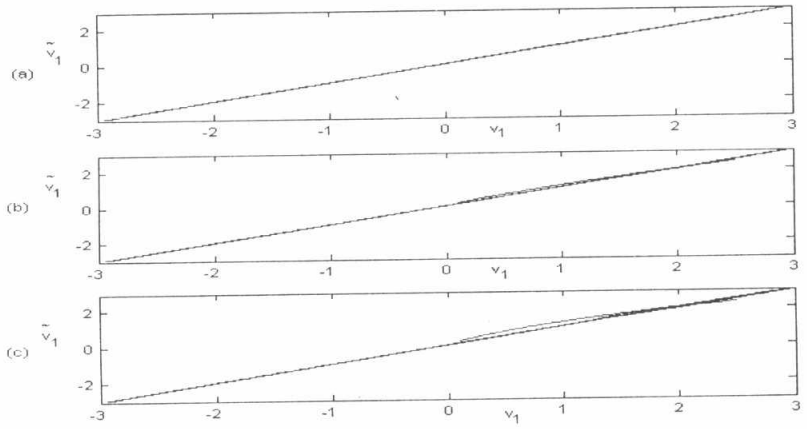
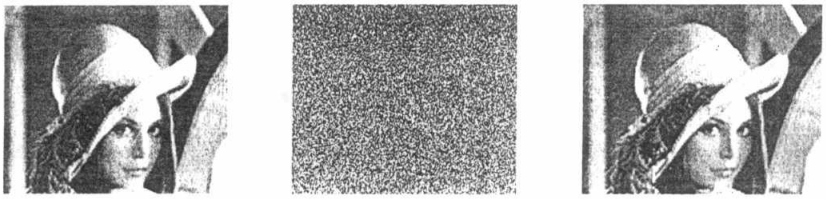
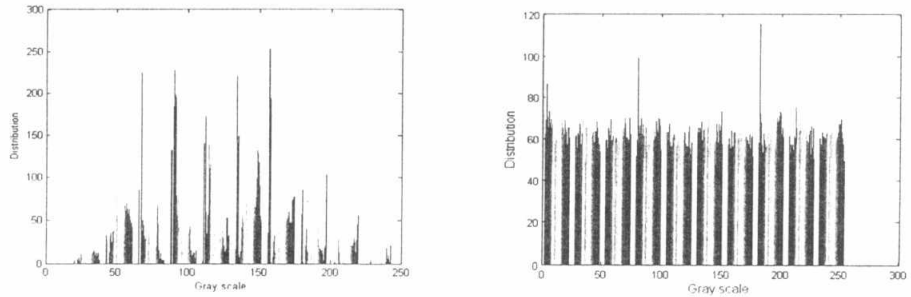


Fig.4. Synchronization between transmitter and receiver for different parameter mismatch:-
(a) 2 % Mismatch.
(b) 5 % Mismatch.
(c) 10 % Mismatch.



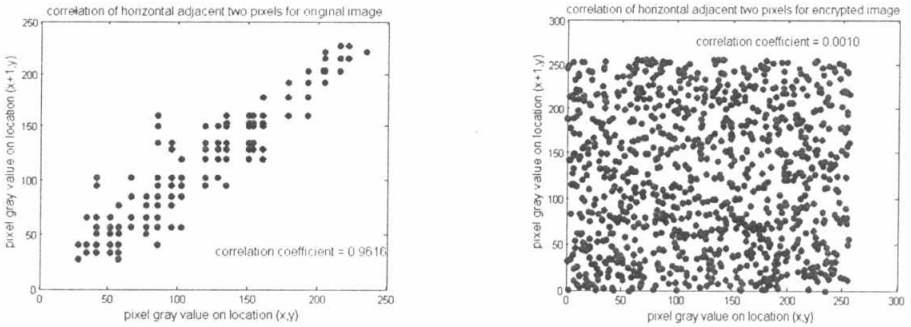
(a) Plain Image (b) Encrypted Image (c) Reconstructed Image

Fig.5. Encryption and decryption of Image using chaotic cryptosystem with AES algorithm



(a) The Histogram of Plain Image (b) The Histogram of Ciphered Image

Fig.6. Histograms of plain and ciphered image using chaotic cryptosystem with AES algorithm



(a) Plain Image Correlation (b) Ciphered Image Correlation

Fig.7. Correlations of two horizontally adjacent pixels in the plain-image and in the ciphered-image encrypted by chaotic- cryptosystem with AES encryption algorithm

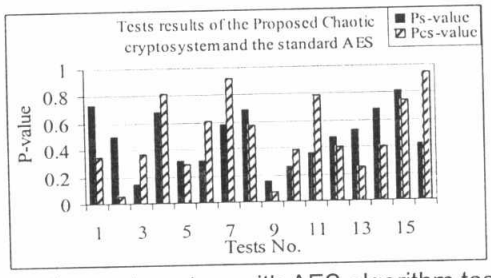


Fig.8. Chaotic cryptosystem with AES algorithm test results

Table 1. Correlation Coefficients of two Adjacent Pixels in two Images (Plain and Ciphered)

	Plain-image	Ciphered-image
Horizontal	0.9616	0.001
Vertical	0.9699	0.0453
Diagonal	0.9051	0.0296

Table 2. Chaotic cryptosystem with AES algorithm test results

No.	Test Name	PS-value	PC-value
1	Frequency(Monobit) Test	0.7310	0.3446
2	Frequency Test within a Block	0.5023	0.05
3	Runs Test	0.1456	0.365
4	Test for the Longest Run of Ones in a Block	0.6802	0.81
5	Binary Matrix Rank Test	0.3104	0.289
6	Discrete Fourier Transform(Spectral) Test	0.3114	0.609
7	Non-Overlapping Template Matching Test	0.5804	0.919
8	Overlapping Template Matching Test	0.6843	0.568
9	Maurer's "Universal Statistical" Test	0.1561	0.073
10	Lempel-Ziv Compression Test	0.2612	0.382
11	Linear Complexity Test	0.3532	0.788
12	Serial Test	0.4765	0.398
13	Approximate Entropy Test	0.5234	0.254
14	Cumulative Sums Test	0.6782	0.404
15	Random Excursions Test	0.8120	0.743
16	Random Excursion Variant Test	0.4237	0.947