New Secure E-mail System Based on Bio-Chaos Key Generation and Modified AES Algorithm

Haider K Hoomod, A M Radi
1 Department of computer Science, college of Education, University Al-Mustansiriya
Drrhjnew@gmail.com

Abstract. The E-mail messages exchanged between sender's Mailbox and recipient's Mailbox over the open systems and an insecure Networks. These messages may be vulnerable to eavesdropping and itself poses a real threat to the privacy and data integrity from unauthorized. The E-mail Security includes the following properties (Confidentiality, Authentication, Message integrity). We need a safe encryption algorithm to encrypt Email messages such as algorithm Advanced Encryption Standard (AES) or Data Encryption Standard DES as well as biometric recognition and chaotic system. The proposed E-mail system security is uses modified AES algorithm and use secret key-bio-chaos that consist of biometric (Fingerprint) and chaotic system (Lu and Lorenz). This modification makes the proposed system more sensitivity and randomness. The execution time for both encryption and decryption of proposed system is much less from original AES, in addition to being compatible with all Mail Server.

1. Introduction
The E-mail message transmitted via the internet will be vulnerable to eavesdropping and threats to the privacy of E-mail because it insecure channel [1].there are two protocols, the Simple Mail Transfer Protocol (SMTP) and Post Office Protocol third (POP3). The SMTP, this protocol allows for user send E-mails to another user and not to received E-mail [2], The POP3, This type of protocol enables the user to access the mailbox and download the messages to the computers in addition to providing the possibility to read the message even in the case of the presence of Internet service, Those protocols are unsafe [3,4]. The AES algorithm is one of the most important algorithms that are related to encryption and decryption message contents of e-mail system because has many from characteristics (Secure, accepted Cost, Flexible, Simplest) [5]. However, these algorithms have some shortcomings encryption speed has a poor efficiency at a low level, if the attachments are large, it is, therefore, necessary to develop AES algorithm and make it more efficient in implementing encryption and decryption [6], the algorithm isn't the secret; it's known to the public. The secret is the key. Although encryption is effective in transferring sensitive data across an insecure channel but lacks the handle of long keys because maintenance and sharing of these long and random keys have become a critical problem in encryption systems. These problems are handled well by using a biometrics system that eliminates the need to remember the key or even to exchange it over an open network [7], can be integrated with chaotic mapping that has many important properties corresponding to encryption because Randomization, sensitivity is the initial conditions and control parameters. These features make from chaotic systems a powerful choice in building powerful cryptographic systems and as well as generate a secret key strong has sensitive and random against all types attacks [8]. In this paper will be using
modified AES algorithm, key-bio-chaos that consist of biometric (Fingerprint) and chaotic system (Lu and Lorenz or Lorenz) in the design of a proposed E-mail system security.

2. **Advanced Encryption Standard**
AES is an encryption algorithm used the symmetric key and used in encrypt/decryption the contents of the message between two parties. The data block length and a key length of AES can be varied according to the requirement. Three key lengths: 128, 192, 256, whose iteration cycle number is 10, 12 and 14 round respectively, AES encryption process is shown in ‘figure 1’. Each round consists of the following four steps: SubBytes, ShiftRows, MixColumns, AddRoundKey. There are a number of benefits of AES will be relevant in providing E-mail system security as Secure, accepted Cost, Flexible, Simplest. However, these methods have some shortcomings encryption speed has a poor efficiency at a low level, if the attachments are large, it is, therefore, necessary to develop AES algorithm and make it more efficient in implementing encryption and decryption [9].

![Figure 1](image-url). AES Encryption and Decryption process

3. **Chaotic Systems**
Chaos theory is based on nonlinear behaviours (which are highly sensitive to their initial parameters), it has enabled structures sensitive equations of this theory from generating unpredictable random
values that correspond with diffusion and confusion principles in order to construct cryptographic systems that have the maximum type of entropy [8] and robust against any type of attacks. We need to use a three-dimension chaotic system such as Lu and Lorenz are suitable to encrypt the three components of the color image and in addition to text.

3.1. Lu Chaotic System

The Lu system is a three dimensions chaotic system and it is described ‘as in equation (1), equation (2) and equation (3)’ [10]:

\[ \dot{X} = a(y - x) \]  \hspace{1cm} (1)

\[ \dot{Y} = -xz + cy \]  \hspace{1cm} (2)

\[ \dot{Z} = xy - bz \]  \hspace{1cm} (3)

3.2. Lorenz Chaotic System

Lorenz system is also three dimensions chaotic system and the Lorenzo system steps and its equations are described ‘as in equation (3), equation (4) and equation (5)’ [10]

\[ \dot{X} = \sigma (y - x) \]  \hspace{1cm} (4)

\[ \dot{Y} = x(\rho - z) - y \]  \hspace{1cm} (5)

\[ \dot{Z} = xy - \beta z \]  \hspace{1cm} (6)

4. Biometric Recognition

Biometric is a technique based on the physiological or behavioral characteristics of humans such as face features, palm, iris, fingerprint, finger or hand geometry, voice, keystroke dynamics, handwritten signature, etc. Usually, common passwords, have many disadvantage factors: Ease of forgotten, stolen, lost, replication, etc. It is worth mentioning that the characteristics of the human body have a uniqueness cannot be repeated. It cannot be copied, stolen or forgotten. It is safe in provides authentication for Email message [11].

This biometric can be used to generate an exclusive and unique key for each individual. These features make biometric a powerful option in building cryptographic systems because it can take advantage of strengths in both fields while encryption provides confidentiality, biometrics provides properties non-repudiation and eliminates the need to remember passwords or to carry codes etc, can integrate it with a number of other technics, such as chaotic systems that make those systems more random and sensitive to the initial information [12].

Amid various Biometric identifications technologies, Fingerprint recognition has been successful due to its two vital characteristics uniqueness and permanence that’s ability to stay unchanged over the lifetime and simplicity feature extraction by use image fingerprint [13]. After extracting the fingerprint feature as shown in ‘figure 2’ it integrates with a chaotic mapping which previously mentioned to produce a key-bio-chaos has characteristic random and sensitivity of initial values use in building strong encryption systems.
5. The Proposed E-mail system security:
The proposed system consists from two part are modified AES algorithm (MAES) and generate a secret key based on biometric (fingerprint) and chaotic mapping (Lu and Lorenz) and also use protocols (SMTP and POP3) in the sending and receiving In sending and receiving emails.

5.1. Generate secret key
The Lu system taking its initial conditions after extract features fingerprint as shown in figure (2) for generating three random numbers used as inputs to the three equations of Lorenz system to generate random masks, when dealing with Email attachment (image) will produce three random masks, Each mask has size 4096 (4 * 4) equal to the three dimensions of the image (256*256), in the same way implement on the message content (text, file) but use one random mask to be XOR with the encrypted message contents that is produced from modified AES. after that will performing permutation for each block of random masks, The resulting blocks will be used as changing key for modified AES algorithm and the same time multiplication each block of changing key values in number 3 for produce new key to be XOR with the next state coming from shift-rows process in modified AES that will be explained later.

5.2. Modified AES algorithm (MAES)
The MAES, it uses same operations of original AES except for Mix-Columns operation and compensation for it in two XOR and shift-cycle operations as well as has two keys-bio-chaos which mentioned earlier in the process of Generate Key-bio-chaos, each key has size 4*4 byte that changing random values completely in each encryption or decryption process.

After splitting the message contents (file, image, text) to blocks size 4 * 4 byte, each block refers to the state. This state with two keys-bio-chaos are passed to the modified AES algorithm operations for produce encrypted message contents (image, file, text) as shown in ‘figure 3’ that describe the
main encryption steps of modified AES and then to be XOR with mask-bio-chaos which is the output of the Lorenz system mentioned earlier in the process of Generate Key-bio-chaos for produce finial cipher-message contents. This modification adds more sensitivity and randomness to the system and reducing time required in both encryption and decryption for content (Text/Image) message during an exchange of messages between the sender’s Mailbox and the recipient’s Mailbox via the network using protocols (SMTP, POP3), and In addition to being compatible with all Mailserver.
Figure 3 Encryption and Decryption Process of Modified AES
6. The sending and receiving side of the proposed system
The system mainly has two sides. The first side is called “sending side”, the second side is called “receiving side”

6.1. Sending side:
The algorithm (1) describes process encryption of the message contents in this side.

Algorithm (1): Encryption process

Input: Plain-message contents (image, file, text).
Output: Send cipher-message contents (image, file, text).

Step1: Read plain-message contents (image, file, text).
Step2: If attachment (image), resize (256*256).
Step3: Split the message contents (image, file, text) into a set of block size 4*4 byte.
Step4: If size block ≠ 16 byte, add values zeros to length block, block=16 byte.
Step5: Read image fingerprint.
Step6: Extract features fingerprint as shown in section 4.
Step7: Message encrypted XOR three masks random of image (256*256) / one mask of message contents (file, text).
Step8: The proposed system send cipher-message (image, file, text) via protocol SMTP.
Step9: END

6.2. Receiving Side
This algorithm (2) shows steps of decrypting the message contents in proposed system

Decryption process algorithm (2)

Input: cipher-message contents (image, file, text).
Output: plain-message contents (image, file, text).

Step1: The proposed system received E-mail cipher-message contents (image, file, text) by protocol POP3.
Step2: Read cipher-message contents (image, file, text)
Step3: Read image fingerprint
Step4: Extract features fingerprint as shown in section 4.
Step5: Message encrypted XOR three masks random of the image (256*256) / one mask of message contents (file, text).
Step6: Split the message contents (image, file, text) into a set of block size 4*4 byte.
Step7: Apply modified AES algorithm (decryption process) that take two keys-bio-chaos 4*4 with blocks 4*4 byte for output decrypt-message.
Step8: If output modified AES algorithm is file or text will go to the condition if output> 0 then plain message = output( The purpose of this process is to remove the excess zeroes that were previously added to the encryption process if the output of modified AES algorithm is file or text).
Step9: Output plain-message (image, file, text).
Step10: END

7. Experimental Results
In this system, A series of tests were execution out on the message contents (body and attachment) which the encrypted in at the originator's point and decryption upon receipt. This tests showing the efficiency of modified AES algorithm compared to the original AES algorithm, The main flaw that is resolved is a waste of time (lost) in the encryption and decryption process in the original AES
algorithm, which need a lot of time when dealing with large data in E-mail attachment (Image, file), also random the key that is based on chaotic (Lu and Lorenz) and biometric (fingerprint) used in this system. This Experiments on a PC with Intel Core i7 CPU @ 2.70GHz, 8G RAM with Windows 8, types experiments are:

7.1. Analysis of the Key Sensitivity:
The proposed system is sensitive to the key change even if it is a slight change, for example, we encrypt the contents of the message with a key (0.4), a small change in the key (0.400000000001) and then execute operation decryption was the result the message was not decrypted.

7.2. The Histogram Analysis
This test shows pixel density levels in message attachments (image) encrypted as graphs. (Table 1) shows the level of density in each level of color before and after encryption in modified AES.

| Image       | Histogram |
|-------------|-----------|
|             | R         | G         | B         |
| Original    | ![Graph](Image1) | ![Graph](Image2) | ![Graph](Image3) |
| Encryption  | ![Graph](Image4) | ![Graph](Image5) | ![Graph](Image6) |
| Original    | ![Graph](Image7) | ![Graph](Image8) | ![Graph](Image9) |
| Encryption  | ![Graph](Image10) | ![Graph](Image11) | ![Graph](Image12) |

7.3. Correlation Analysis
In the (table 2) shows correlation analysis between the Email message contents when using the original AES and modified AES based on key-bio-chaos consists from biometric (fingerprint) and chaotic system (Lu and Lorenz).
Table 2. Correlation Analysis between plain and cipher message
(A) attachment (Image), (B) attachment (File), body (Text)

| Attachment (Image) | Correlation Analysis | Proposed Modified AES | Original AES |
|--------------------|----------------------|-----------------------|--------------|
|                    | R        | G        | B        | R        | G        | B        |
| 1                  | 0.0067   | -0.0059  | -0.0037  | -0.0034  | 0.0050   | -0.0029  |
| 2                  | 0.0043   | -0.0035  | 0.0029   | 0.0028   | 2.3283   | -6.5870  |
| 3                  | -0.0049  | -0.0082  | -0.0030  | -0.0041  | -0.0064  | 0.0033   |

(B)

| (File.txt) | Correlation Analysis | Proposed Modified AES | Original AES |
|------------|----------------------|-----------------------|--------------|
|            | R        | G        | B        | R        | G        | B        |
| 16kB       | 0.0089   |          |          | 0.0015   |          |          |
| 12kB       | 0.0061   |          |          | -0.0016  |          |          |

(C)

| Characters message | Correlation Analysis | Proposed Modified AES | Original AES |
|--------------------|----------------------|-----------------------|--------------|
|                    | R        | G        | B        | R        | G        | B        |
| 100                | 0.0089   |          |          | -0.0354  |          |          |
| 250                | -0.1511  |          |          | -0.0136  |          |          |
| 500                | -0.0332  |          |          | -0.0781  |          |          |

7.4. PSNR Analysis
This PSNR Peak Signal to Noise Ratio reflects the encryption quality. Mean Square Error (MSE) is the cumulative squared error between originally and encryption message contents (Body, Attachment) as shown in (tables 3).

Table 3. PSNR & MSE for Email message contents (A) attachment (Image), (B) attachment (File), body (text)

(A)

| Image | Proposed Modified AES | Original AES |
|-------|------------------------|--------------|
|       | MSE       | PSNR         | MSE       | PSNR         |
|       | R        | G        | B        | R        | G        | B        | R        | G        | B        | R        | G        | B        |
| Image |          |          |          |          |          |          |          |          |          |          |          |          |
| Image | 3.54     | 3.00     | 2.38     | 12.6     | 13.3     | 14.3     | 3.58     | 2.98     | 2.40     | 12.6     | 13.4     | 14.362   |
| Image | 06       | 59       | 29       | 740      | 851      | 938      | 26       | 42       | 02       | 228      | 165      | 4        |
| Image | 2.77     | 2.44     | 2.99     | 13.7     | 14.2     | 13.3     | 2.77     | 2.42     | 3.01     | 13.7     | 14.3     | 13.375   |
| Image | 82       | 04       | 82       | 272      | 901      | 962      | 46       | 07       | 23       | 328      | 253      | 8        |
| Image | 3.14     | 3.15     | 3.13     | 13.1     | 13.1     | 13.1     | 2.76     | 2.42     | 3.00     | 13.7     | 14.3     | 13.381   |
| Image | 33       | 74       | 90       | 909      | 715      | 969      | 49       | 00       | 83       | 481      | 266      | 5        |

(B)

| File.txt | Proposed Modified AES | Original AES |
|----------|------------------------|--------------|
| MSE      | PSNR               | MSE         | PSNR       |
| R        | G        | B        | R        | G        | B        | R        | G        | B        |
| 3.54     | 3.00     | 2.38     | 12.6     | 13.3     | 14.3     | 3.58     | 2.98     | 2.40     | 12.6     | 13.4     | 14.362   |
| 06       | 59       | 29       | 740      | 851      | 938      | 26       | 42       | 02       | 228      | 165      | 4        |
| 2.77     | 2.44     | 2.99     | 13.7     | 14.2     | 13.3     | 2.77     | 2.42     | 3.01     | 13.7     | 14.3     | 13.375   |
| 82       | 04       | 82       | 272      | 901      | 962      | 46       | 07       | 23       | 328      | 253      | 8        |
| 3.14     | 3.15     | 3.13     | 13.1     | 13.1     | 13.1     | 2.76     | 2.42     | 3.00     | 13.7     | 14.3     | 13.381   |
| 33       | 74       | 90       | 909      | 715      | 969      | 49       | 00       | 83       | 481      | 266      | 5        |
7.5. Entropy Analysis

This entropy calculates the uncertainty association of the random values, the good encryption algorithm should give low mutual information of values of the encrypted message contents, and this means that the entropy will be increased, and the entropy equation is as follows in the equation:

In this (table 4), the entropy of the proposed system is better than the original AES algorithm.

| Characters message | Proposed Modified AES | Original AES |
|--------------------|-----------------------|--------------|
| 100                | 7.2189                | 8.2035       |
| 250                | 7.2711                | 7.4844       |
| 500                | 7.5946                | 7.7625       |

Table 4. Entropy Analysis of message attachment
(A) Attachment (image), (B) Attachment (File.txt), (C) Body (Text)

7.6. Execution Time

This test calculates the execution time of the encryption process on the message contents (body, attachment) when sending and decrypting the message contents when received. In the (table 5), shows a less execution time in both models of the modified AES (MAES) algorithm function with Generate key-bio-chaos in the proposed system compared to the original AES algorithm.
Table 5. The execution times Encryption (A) Encryption process, (B) Decryption process

(A) message contents | Execute time encryption | Proposed Modified AES first | Original AES
--- | --- | --- | ---
Attachment | Image 256*256 | 9.852044s | 101.459606s
 | File 12 KB | 8.022659s | 14.305919s
 | File 16 KB | 8.517189s | 14.954298s
Body | 100 characters | 7.652578s | 8.000599s
 | 250 characters | 7.646128s | 8.244076s
 | 500 characters | 7.638534s | 8.462815s

(B) Message contents | Execute time decryption | Proposed Modified AES first | Original AES
--- | --- | --- | ---
Attachment | Image 256*256 | 9.119982s | 122.015908s
 | File 12 KB | 7.873978s | 14.127101s
 | File 16 KB | 7.498325s | 16.574347s
Body | 100 characters | 7.604548s | 8.474877s
 | 250 characters | 7.692139s | 7.974319s
 | 500 characters | 7.651514s | 8.118706s

8. Conclusion
E-mail provides an important means of communication between users. In this paper was proposed E-mail system secure capable of providing a high level of security for contents message and speed in encryption and decryption between two parties via an open network, in addition to compatible with all MailServers.

References
[1] Jang J, S Nepal and J Zic 2008 Trusted Email Protocol: Dealing with Privacy Concerns from Malicious Email Intermediaries IEEE
[2] S ANDREW TANENBAUM and J DAVID WETHERALL 2011 COMPUTER NETWORKS FIFTH EDITION.
[3] L Larry Peterson and S Bruce Davie 2003 Computer networks THIRD EDITION
[4] Ms.Priyanka S. Kamthe and Ms.Sonal P. Nalawade 2015 Email Security The Challenges of Network Security International Journal on Recent and Innovation Trends in Computing and Communication IJRITCC
[5] K P Singh and S Dod 2016 An Efficient Hardware design and Implementation of Advanced Encryption Standard (AES) Algorithm International Journal of Recent Advances in Engineering & Technology (IJRAET)
[6] K R Saraf, V P Jagtap and A K Mishra 2014 Text and Image Encryption Decryption Using Advanced Encryption Standard International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
[7] A G Reddy 2016 An Enhanced Biometric Based Authentication with Key-Agreement Protocol for Multi-Server Architecture Based on Elliptic Curve Cryptography PLOS ONE
[8] M T Mohammed, A E Rohiem, A El-moghazy, and A. Z. Ghalwash 2013 Chaotic Encryption
Based PGP Protocol \textit{International Journal of Computer Science and Telecommunications} \\
[9] Mathur N, R 2016 AES Based Text Encryption Using 12 Rounds with Dynamic Key Selection Elsevier. \\
[10] Leonov A. G Leonov and Kuznetsov V. N 2015 Elsevier \\
[11] Zhu H, Hao X, Zhang Y and Jiang M 2015 A Biometrics-based Multi-server Key Agreement Scheme on Chaotic Maps Cryptosystem \textit{Journal of Information Hiding and Multimedia Signal Processing} \\
[12] Chandra S, Paul S, Saha B and Mitra S 2013 Generate an Encryption Key by using Biometric Cryptosystems to secure transferring of Data over a Network IOSR \textit{Journal of Computer Engineering (IOSR-JCE)} \\
[13] Ankit K and Rekha J 2016 Biometrics as a Cryptographic Method for Network Security \textit{Indian Journal of Science and Technology}