Assessing the Performance of Classical and Chaotic Techniques for Image Encryption

1Said Hraoui, 1Faiq Gmira, 1,2Abderrahim Saaidi, 1Abderrahmane Ould Jarar, 1Khalid Satori

1LIIAN, Department of Mathematics and Informatics Faculty of Science Dhar-Mhraz PB 1796 Atlas-Fez, Morocco
2LIMAO, Department of Mathematics, Physics and Informatics Polydisciplinary Faculty-Taza, PB1223, Morocco

Abstract: The increasing transfer of multimedia data creates more information security needs. To meet the requirements of confidentiality, multiple encryption algorithms have been developed in recent years. Due to the widespread use of image data in various fields (medical, industrial, ...), it is necessary to use and adapt these secured techniques for this type of data. In this perspective, an analysis study of two encryption algorithms applied to images is performed in order to assess their robustness in terms of security. The first is the classical cryptosystem known as Advanced Encryption Standard (AES) and the second is issued from chaotic signals based on a logistic map.

Key words: Symetric encryption, AES, Logistic map, Chaotic signals.

INTRODUCTION

Recently, the multimedia data transfer (texts, images, videos,...) over all kinds of wired/wireless networks is increasing rapidly, this imposes to have some reliable techniques, secure and commonly accepted to ensure the integrity, the confidentiality and the data security. Data encryption is often the only effective way to meet these requirements. Consequently, these last years, several work proposed crypto-systems related to the data images; characterized by some special properties such as bulky data capacity and strong correlation among pixels, of which non-exhaustively we quote, those based on the conventional classical algorithms, such as DES (Data Encryption Standard) and AES (Advanced Encryption Standard) which are also based on number theory and algebra concepts and these are very common and widely used (Advanced Encryption Standard (AES), 2001; Medien, Z., 2007; Deamen, J., V. Rijimen, 2002; Karthigaikumar, P., 2011) and others based on the chaotic systems (Morteza Saberi Kamarposhti, 2012; Fengling Han, 2007; Chong Fu, 2007; Guodong Ye, 2010; Yong Wang, 2011; Yong, Z., 2011; Lili Liu, 2012; Ariffin, M., M. Noorani, 2008), these systems were originated from the study of the dynamics of nonlinear systems and they are known for their ergodicity property; sensitivity to initial conditions and better combination of satisfaction in terms of speed, diffusion and complexity all summarized in table 1. These important properties satisfy cryptography requirements.

In this paper we made a comparative study between a classical crypto-system based on AES and another one based on the chaotic attractor known by the name the logistic map (Baptista, M.S., 1998; Shujun, L., 2004).

This article is organized as follows: after an introduction, a brief overview of previous work is presented in the second section. The AES algorithm is described in the third section. Section four presents the chaotic attractor based on a logistic map. Implementation Part of these algorithms and analyzing their robustness is described in the fifth section. Finally, it ends with a conclusion.

Previous Work:

To encrypt multimedia data, different techniques have been proposed in literature. In this section, a brief overview of image encryption methods is presented with an aim to improve applications computational time for transmission.

The authors of (Puech, W., 2006; Lala Krikor, 2009) presented a new selective encryption method based on AES stream cipher that encodes a portion of the bitstream issued by Huffman encoding. This method has led to an improvement in computation time and storage compression ratio JPEG format original.

In papers (Pareek, N.K., 2006; Shubo Liu, 2009) a new image encryption technique based on the use of two chaotic maps and a key length of 80 bits is presented. The results shown in this paper illustrate the implementation possibility of this method for real-time application and its use in transmission.

The authors of (Puech, W., 2006; Lala Krikor, 2009) presented a new selective encryption method based on AES stream cipher that encodes a portion of the bitstream issued by Huffman encoding. This method has led to an improvement in computation time and storage compression ratio JPEG format original.

In papers (Pareek, N.K., 2006; Shubo Liu, 2009) a new image encryption technique based on the use of two chaotic maps and a key length of 80 bits is presented. The results shown in this paper illustrate the implementation possibility of this method for real-time application and its use in transmission.

Corresponding Authors: Sidi Mohamed Ben Abdellah University, LIIAN-Department of Mathematics and Informatics Faculty of Science Dhar-Mhraz P.B 1796 Atlas-Fez, Morocco
Paper (Yong Wang, 2011), has an encryption algorithm based on AES and spatiotemporal chaos. The principle of combining the steps of permutation and diffusion to reach a level of indistinguishability is also important to improve the processing speed and the strength of the encryption algorithm.

In paper (Chengqing Li, 2011), the authors pointed out that a modified scheme based on chaotic standard and a logistic map is still insecure against the same known/chosen-plaintext attack. In addition, some other security defects existing in both the original and the modified schemes are also reported.

In paper (Yin Dai, Xin Wang, 2012), the authors proposed a new encryption algorithm based on a composition of Logistic Map (LM) and Chebyshev Map (CM) for to overcome the periodic bursts presented for some values of the control parameter of logistic map. The authors apply firstly the LM encoding, after the CM encoding is applied. The experimental evaluation proves that the new algorithm has higher security, a wider key space and the 213 values of the encrypted image are distributed closer to a uniform distribution.

**Aes Algorithm Description**

In Cryptography, we can find several areas of study. The techniques change from type to type and class to class. The figure below illustrates the classification of standard cryptosystems.

![Fig. 1: Overview of the field of traditional cryptosystems.](image)

AES (Advanced Encryption Standard) is a block cipher algorithm with a secret key (Deamen, J., V. Rijimen, 2002; Medien, Z., 2007). It is the successor of the famous DES (Data Encryption Standard), which became vulnerable.

The use of simple binary operations, such as permutations and substitutions, AES has proved its effectiveness and low cost memory. This allows the algorithm to operate in applications supporting large files such as images.

The AES algorithm uses a large combinations number of related round’s pair (key lengths, block length) (Pareek, N.K., 2006; Yong, Z., 2011). There are actually 3 variants of the AES cipher, each of which uses a different key length. The permissible key lengths are 128, 192, and 256 bits. For data blocks of 128 bits, the number of rounds may take respectively the values 9, 11 or 13.

In our case, the image is divided into blocks of 128 bits with which we are going to form a squared matrix in order to work on the 128-bit (key length) version of the AES algorithm. Bits of such a block are arranged in a 4x4 matrix with which we represent each byte in hex for reasons of size and also for good readability.

Figure 2 describes the operations used to encrypt one block of data with the AES algorithm (Pareek, N.K., 2006; Yong, Z., 2011). These steps begin with "Operation AddRoundKey" which consists of modulo 2 addition of each 128-bit block of the image with its counterpart in the matrix encryption key (original key). This matrix will be used as input to the next step. After that, this input enters the encryption rounds that depend on the size of the used key. Regular operation of each round contains four steps.

1. **SubByte**: Each byte of the block is replaced by another value from an "S-box" (a matrix obeys Shannon’s property of confusion (Shannon, C.E., 1948)).
2. **ShiftRow**: the lines are shifted cyclically with different "offsets".
3. **MixColumn**: each column is treated as a polynomial multiplied over GF (2^8) (Galois Field) by a constant matrix which obeys also the principle of diffusion of Shannon.
4. **AddRoundKey**: a simple exclusive "or" between the present data and key in the current round. This step aims to generate at each iteration a key matrix that will be used in the next iteration and which eliminates the key-related attacks by disappearance of the symmetry.
The AES algorithm performs the 10th round, which is almost similar to other rounds except for the removal of "Operation Mix Columns" before producing the final image encryption.

Fig. 2: AES Algorithm scheme.

**The Logistic Map Attractor:**

The term "chaos" defines a particular state of a system whose behavior is never repeated, and each chaotic system is known by several properties, a partial list of these properties is shown in the table below (Fengling Han, 2007; Chong Fu, 2007). The chaotic signals data encryption is done by the superposition of the initial information to a chaotic signal. Chaotic maps have also a pseudo-random behavior that can be used to encrypt information through substitution or masking processes.

<table>
<thead>
<tr>
<th>Chaotic property</th>
<th>Cryptographic property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensitivity to initial conditions/control parameter Mixing property.</td>
<td>- Diffusion with a small change in the plaintext/secret key</td>
<td>- A small deviation in the input can cause a large change at the output.</td>
</tr>
<tr>
<td></td>
<td>- Diffusion with a small change in one plain-block of the whole plain text</td>
<td>- A small deviation in the local area can cause a large change in the whole space.</td>
</tr>
<tr>
<td>Structure complexity.</td>
<td>Algorithm (attack) complexity.</td>
<td>A simple process has a very high complexity.</td>
</tr>
</tbody>
</table>

Table 1: A partial list of chaos and cryptography properties.

The main reason why cryptographers used chaotic maps in so many chaotic cryptosystems, is the high dependency of the dynamics of chaotic maps on an external value or set of values and the initial conditions of the system, and therefore result the dependency of the cryptosystem on the secret key, also having a critical point independent to the value of control parameters, whereas the statistical complexity decrease as the control parameters increase (David Arroyo, 2009; David Arroyo, 2008).

In this article we focus our study on the logistic map known by the "chaotic attractor".

**A. Logistic Map Equation:**

The logistic map is a second degree polynomial (Shannon, C.E., 1948) widely used in different arrears, expressed by the following recurrence relation:

\[ X_{t+1} = \lambda X_t (1 - X_t) \]  

(1)

Where \( \lambda \in [0, 4] \) is a control parameter of the logistic map, the variable \( X_t \in [0, 1] \) with \( t \) is the iterations number used to generate the iterative values. When varying the parameter of the logistic map \( \lambda \), we see that for a good choice of the initial condition \( x_0 \), the chaotic nature occurs only when \( \lambda \in [3.57, 4] \). This is clear in the bifurcation diagram of the logistic map on Figure 3.
B. Algorithm of the Logistic Map:

The chaotic encryption is the result of the original image and the signal generated by the chaotic attractor superposition. The algorithm below shows the image encryption through the use of the logistic map described by the recurrence equation (1).

```plaintext
x ← Plaint-image;
[a b] ← sizeof(x);
N ← a*b;
// generating the matrix chaotic
m(1) ← initial value;
for i :1 to N-1
begin
    m(i+1) ← m(1)*m(i)-m(1)*m(i)^2;
end
m ← mod(1000*m,256);
n ← 1;
// superposition original image and attractor
for i : 1 to a
begin
    for j : 1 to b
    BEGIN
        encrypted_image(i,j) ← xor(m(n),x(i,j));
        n ← n+1;
    end
end
write encrypted_image;
```

Fig. 3: Bifurcation diagram for the logistic map.

Fig. 4: The logistic map algorithm.

The algorithm exposed in figure 4 shows the simplicity of chaotic encryption implementation using the logistic map compared with that of the AES, which presents a complexity in all the operations that constitutes it. In addition, pixels that are equal within the chaotic encryption are not coded the same way (difficulty of making a statistical cryptanalysis). Finally, the use of this technique is justified by the simplicity of the algorithm and the encryption speed which is more important than the absolute security of the image.

Comparative Study:
To evaluate the security and robustness of these two cryptosystems, we will conduct statistical analysis which includes respectively histogram and correlations analysis in accordance with running speed.

We used Matlab to execute the code of our two selected encryption techniques. The codes are executed on a computer with a Pentium dual-core CPU T4200 at a 2GHz speed in order to analyse the result of the encryption operations. The test images used are: Lena (512 x 512 bmp), Baboon (512 x 512 bmp).

A- Comparison of Encryption Speed:

We calculated the time needed for both algorithms to encrypt 128 bytes of plain text -the table 2- shows the results obtained:
Table 2: Performance speed of AES and the logistic map.

<table>
<thead>
<tr>
<th>Simulations in MATLAB</th>
<th>Encryption time with AES</th>
<th>Encryption time with Logistic Map</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 byte</td>
<td>1.04 ms</td>
<td>0.37 ms</td>
</tr>
<tr>
<td>128 bytes</td>
<td>133.31 ms</td>
<td>47.24 ms</td>
</tr>
</tbody>
</table>

These results proves that The Logistic map have superiority over AES encryption in terms of running speed.

B- Histogram-Analysis:

We know that the image histogram reflects the information on the distribution of its pixels values. A spy can do a statistical attack by analyzing the histograms of an encrypted image and that by using the algorithms of attacks (Lenstra, A.K., 1982) to obtain some useful information of the original image. This leads us to say that a well encrypted image should have a histogram with a uniform distribution.

Both algorithms were tested on a pair of two test images Lena and Baboon, Both of these images statistical properties are presented in Figure 5.

![Fig. 5](image)

Therefore, the most the histogram of the encrypted image is smooth and evenly distributed as possible, the less a spy can extract information about the original image (clear image) and thus the security of the cryptosystem is higher.

From Figure 4, the encrypted images histograms by AES and chaotic attractor have a nearly uniform distribution with a very slight difference noticed on the distribution of the chaotically encrypted image histogram (Figure 4-(f)). This shows the robustness of AES compared to the chaotic attractor.

B-Correlation Analysis:

Another statistical attack technique is the analysis of the correlation coefficient (Pareek, N.K., 2006; Yong, Z., 2011), which allows to evaluate the correlation between adjacent pixels and hence assess the robustness of the algorithm. We calculate the correlation coefficient for a sequence of adjacent pixels by the formula below:
\[ r_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \] (2)

Where \( x \), \( y \) are two vectors formed respectively by the values of the image's selected sequence pixels and the values of their adjacent pixels. The terms \( \text{cov}(x, y) \), \( E(x) \), \( D(x) \) are calculated by the following formulas:

\[ E(x) = \frac{1}{N} \sum_{i=1}^{N} x_i \] (3)

\[ D(x) = \frac{1}{N} \sum_{i=1}^{N} [x_i - E(x)]^2 \] (4)

\[ \text{cov}(x, y) = \frac{1}{N} \sum_{i=1}^{N} [x_i - E(x)][y_i - E(y)] \] (5)

Where \( N \) is the number of adjacent pixels selected from the image to calculate the correlation coefficient. \( x_i \) and \( y_i \) are, respectively, the elements of \( x \) and \( y \).

Table 3: Correlation coefficients of the AES and the logistic map algorithms.

<table>
<thead>
<tr>
<th></th>
<th>Horizontal</th>
<th>Vertical</th>
<th>Diagonal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Initial</td>
<td>0.9719</td>
<td>0.8724</td>
<td>0.9593</td>
</tr>
<tr>
<td>AES</td>
<td>0.00052</td>
<td>0.250</td>
<td>-0.00093</td>
</tr>
<tr>
<td>Chao</td>
<td>-0.0882</td>
<td>0.0321</td>
<td>-0.0479</td>
</tr>
<tr>
<td>Baboon</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Initial</td>
<td>0.9203</td>
<td>0.8631</td>
<td>0.8494</td>
</tr>
<tr>
<td>AES</td>
<td>-0.00042</td>
<td>0.0193</td>
<td>-0.00010</td>
</tr>
<tr>
<td>Chao</td>
<td>-0.0579</td>
<td>0.0412</td>
<td>0.0971</td>
</tr>
</tbody>
</table>

From the results above we see that the correlation coefficients of the original image are close to 1, which shows the strong correlation of adjacent pixels, the other pixels encrypted respectively by AES and logistics map images are near zero. And therefore we conclude that the two encryption systems make the adjacent pixels very independent. It is noted that these results shows the superiority of AES encryption, on the other hand we can see the inferiority of the logistic map encryption and this is mainly due to the periodic windows for some control parameter values of the logistic map.

Another technique to assess the quality of secure cryptosystems is the distribution visualization of the adjacent pixels horizontal and diagonal correlation of the original image and encrypted image (Figure 6).

The results above clearly show the strong horizontal and diagonal correlation of the original image adjacent pixels, while the encrypted images, respectively, whether by the AES or by the logistic map has a strong de-correlation which makes a statistical attack on these two cryptosystems almost difficult.

A- Robustness of the Two Cryptosystems:

Table 4 presents the correlations of the original image with the encrypted images respectively by AES and chaotic attractor. The value 0.0019 is well below 0.0204 it shows the robustness of the cryptosystem based on the AES algorithm compared to the one based on logistic map. The ultimate goal is not in the absolute security of the image, but it is to have a suitable encryption system for real-time applications. This made the chaotic encryption one of the most promising ways to securing multimedia data.

Table 4: Correlation between the original and the encrypted images.

<table>
<thead>
<tr>
<th></th>
<th>AES</th>
<th>Logistic map</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lena</td>
<td>0.0019</td>
<td>0.0204</td>
</tr>
<tr>
<td>Baboon</td>
<td>0.0023</td>
<td>0.0207</td>
</tr>
</tbody>
</table>
Fig. 6: (a) Correlation of horizontally adjacent pixels in the original image (Lena/Baboon), (b) Correlation of diagonally adjacent pixels of the original image, (c) Correlation of adjacent pixels horizontally Lena/Baboon encrypted by AES, (d) Correlation of diagonally adjacent pixels Lena/Baboon encrypted by AES, (e) Correlation of adjacent pixels horizontally Lena/Baboon encrypted by chaotic attractor, (f) Correlation of adjacent pixels diagonally Lena/Baboon encrypted by chaotic attractor.

Conclusion:
In this paper, we compared the efficiency of two techniques for image encryption, one with the AES algorithm and the other with the chaotic attractor. The experimental results of the statistical analysis shows that the two cryptosystems have chosen a level of reliability and a very satisfying security and can therefore withstand known statistical attacks, and thus we concluded using the histograms of the encrypted images and the pixels correlation that the AES has a slight advantage in terms of security, unfortunately, it is noted that the logistic map shows some periodic windows that make it vulnerable. However, due to the computational cost, and the simplicity of implementation this map is a good alternative for image encryption in real time communication applications with the condition to combine it with other chaotic maps or other encryption techniques.

REFERENCES


453


Lili Liu, Qiang Zhang, Xiaopeng Wei, 2012. A RGB image encryption algorithm based on DNA encoding and chaos map, Computers and Electrical Engineering, Accepted 10 (Available online).


