IMAGE ENCRYPTION BASED ON THE NOVEL 5D HYPER-CHAOTIC SYSTEM VIA IMPROVED AES ALGORITHM

Sadiq A. Mehdi
Computer Science Department, Collage of Education, Mustansiriyah University, Baghdad-Iraq

Khalid Kadhim Jabbar
Computer Science Department, Collage of Education, Mustansiriyah University, Baghdad-Iraq

Fadhil Hanoon Abbood
Computer Science Department, Collage of Education, Mustansiriyah University, Baghdad-Iraq

ABSTRACT

The extensive use of digital images in various areas, such as military, commercial and other, requires that the security of images transmitted through communication networks and on the Internet be well preserved. One of the safest algorithms is the Advanced Encryption Standard AES algorithm. However, this algorithm has a number of drawbacks, such as the problem of the appearance of the model and very slow when used directly to encrypt images. This paper proposes a new improved of AES using a novel hyper-chaotic system with five-dimensional (5D) to be suitable for image cryptography. The sequence for a chaotic that generated by the novel hyper-chaotic system was used as a key in the improved an AES to overcome the key problem without changes in the entire cryptographic process in the original AES and the operation Mix Columns was eliminated, since it consumes a lot of time compared to other operations, with the consequent great reduction in the time of encryption and decryption and the improvement in AES algorithm according to its security levels as observed in the experimental results, where proposed algorithm has a very large key space indicates that the algorithm has more capacity for lessen the prospect of intended attack with high sensitivity to minimal manipulation though it was simple in the key, and our proposed method has the ability to resist the statistical attack because of the histogram of the encrypted image is completely uniform and the correlation analysis values are very small and close to zero, the entropy analysis of the information shows that the results experimental are very important with the theoretical value (8), the proposed algorithm has also demonstrated its ability to
thwart differential attacks in which the number of pixels changes the speed (NPCR) and the analysis of the intensity of unified average variation (UACI) fall within the theoretical intervals.

**Keywords:** AES algorithm, chaos, 5D chaotic system, image encryption, chaotic key.

**Cite this Article:** Sadiq A. Mehdi, Khalid Kadhim Jabbar and Fadhil Hanoon Abbood, Image Encryption Based on the Novel 5d Hyper-Chaotic System Via Improved Aes Algorithm, International Journal of Civil Engineering and Technology, 9(10), 2018, pp. 1841–1855.

1. **INTRODUCTION**

Recently, there are many algorithms has been used for encryption image process such as: AES and Data Encryption Standard DES algorithms with chaotic systems [1]. The small key length of DES makes it more vulnerable to various attacks. Besides security issue, DES is a low efficiency encryption algorithm because of its slowness. AES algorithm is the winner of encryption competition standard held by the National Institute of Standard and Technology NIST as an alternative of DES [2]. However, there are a number of drawbacks in AES, such as high computation, pattern appearance issue and so slow when used directly for encrypting images because of intrinsic features of images which are large volumes, high redundancy and high correlations among image pixels. Consequently, there is a need to propose new encryption algorithms [3]. Chaos has been presented to cryptography thanks to its randomness, initial conditions and parameters sensibility, mixing property and periodicity that are close to diffusion and confusion in cryptography. These features make chaos an excellent choice for building cryptographic systems and approved chaotic systems to be promising alternate for the conventional cryptographic algorithms [4].

2. **THE RELATED WORKS**

Several attempts have been made in literature toward the AES algorithm enhancement based on chaos. While [5], introduced a modify AES to enhances the performance of AES to be appropriate for image encryption, especially if the host is large. Besides the Mix Columns transformation is swapped by using 3D chaotic system and XOR operation in order to reduce the high computation in Mix Columns transformation. The proposed method offers a low correlation coefficient and providing better enciphering speed and acceptable security, but the method that present in [6] that amended AES algorithm according to 2D Henon and Chebyshev chaotic map that has ability to produce an independent round key randomly, the two sets of chaotic key stream are produced from each of Henon map and Chebyshev plan, and the four groups of key stream that produced from Henon and Chebyshev plan perform an XOR process respectively to produce the two middling keys then produce a base key by using the XOR process of the middling key, and this is an AES key. This proposed algorithm beat the weak point in the primary key without any change in the encryption process when using the original AES.

3. **AES**

AES is a symmetric block cipher, which has ability for encryption and decryption data in blocks with size of (128) bits by using a several key range of (128) bits, (192) bits or (256) bits respectively, which indicate as: AES-128, AES-192 or AES-256 according to the key range. AES operations are carried out in two dimension array with size of 4×4 bytes known
as the states that converted at every stage of encryption or decryption process. On the other hand, the key is appeared as a square array of with several bytes, where any key is inclusive into a matrix of keys that scheduled words. Each word with size of four bytes, so; when using 128-bits, the whole key schedule is 44 words. Furthermore, the AES contains a number of round N, where each round depend on the key size such as: 10 rounds for a 16 bytes key, 12 rounds for a 24 bytes key, and 14 rounds for a 32 bytes key. The first rounds (N-1) include 4 transformations which are begin with the Sub Bytes then perform Shift Rows, and Mix Columns, finally perform Add Round Key. While the final round encloses N just 3 transformations; the initial transform which is Add Round Key exists before the first round that could be considered as Round 0. In the decryption process, the three operations that begin with Sub Bytes then perform Shift Rows finally apply Mix Columns in the side of encryption process that are inverse in the decryption process. The XOR process used to inverse Add Round Key stage, and an exact round key to the block.

3.1. Sub Bytes/ Inverse Sub Bytes Transformation
In this operation that illustrated in the following figure, all the bytes in the State are changed with other different bytes by using S-box (table of 8-bits). On the other hands, the confusion requirement in the encryption process will be provides from the nonlinear step in AES algorithm Sub Bytes operation. In the decryption process, to implementing Inverse Sub-Byte operation; the Inverse S-box table will be used instead of S-box [8].

![Figure 1 Sub Bytes transformation](image)

3.2. Shift Rows and Inverse Shift Rows Transformation
In the row, each byte of State will be shifted as circular to the left side by different amount of displacement. The 1st row in the State is not shifted, while the 2nd row is shifted by (1) byte, and the 3rd row is shifted by (2) bytes; finally, the 4th row is shifted by (3) bytes, during decryption process. On the other hand, the inverse Shift Rows transformation applying the circular shifting to the right side for each of the last three rows by a (1) byte rotating to the right for the 2nd row and so on [7]. The following figure shows this operation.
3.3. Mix Columns and Inverse Mix Columns Transformation

The Mix Columns transformation deal with each column as a four-terms polynomial, where each column are considered as polynomials over Galois field GF($2^8$), every column which include of four bytes is multiplied by a special $4 \times 4$ array. The multiplication apply on this array isn’t a normal multiplication, rather than the multiplication is performed over GF. The Shift Rows and Mix Columns transformation provides diffusion in AES. Inverse Mix Columns is achieved by using multiplication of the whole GF by another known matrix [9]. The following figure illustrates the Mix Columns operation:

![Figure 3 Mix Columns Transformation](image)

3.4. Add Round Key and Inverse Add Round Key Transformation

In the State array, each byte will be added to the corresponding one in the round key. This addition is simply an XOR operation that completed bitwise between the key and the State. The State is added with the sub key corresponding to the current round which had been already produced via key expansion and make another State. The process of round key inverse is exactly the same operation [7]. Add Round Key transformation is shown in the next figure.

![Figure 4 Add Round Key Transformations](image)
3.5. AES Key Expansion

Each round that used in the Add Round Key transformation, Number of sub-keys from the initial key that generated via the key expansion operation, such as: AES-128, equal to 44 words, where each word equal (4) bytes. When every word are indexed as: \( W_{[\text{index}]} = \{0, \ldots, 43\} \). The first \( (W_0, W_1, W_2, W_3) \) are full off with the given cipher key and columns in locations that are a multiple of four \( (W_4, W_8, W_{12}, \ldots, W_{40}) \) will be generated by three operations which are [7]:

- Rot Word: Rot Word apply one rotating permutation to the left on a word.
- Sub Word: Sub Word substitutes individual bytes of a word by using S-box.
- XOR the result from Rot Word and Sub Word operations with word \( W_i \) and with a defined constant from Recon matrix.

4. CONSTRUCTION OF A NOVEL 5D CHAOTIC SYSTEM

A chaotic is a special dynamical nonlinear system; the 5D chaotic system has more complex dynamic properties than lower dimensional chaotic systems. Lyapunov Exponent is a numerical indicator to judge if the system is chaotic. A positive Lyapunov Exponent means chaos and positive Lyapunov Exponents more than one means hyper chaotic [10]. The following differential equations are used to construct our proposed novel algorithm:

\[
\begin{align*}
\frac{dx}{dt} &= ay - bx + u + w - c\sin(z) \\
\frac{dy}{dt} &= dx - xz - y \\
\frac{dz}{dt} &= xy - ez \\
\frac{du}{dt} &= -fxz + gu \\
\frac{dw}{dt} &= hx + i\cos(n)
\end{align*}
\]

Where \((x, y, z, u, w \text{ and } t) \in \mathbb{R}\) and called the system states, where \(a, b, c, d, e, f, g, h, i\) are positive constant parameters. When the values of \(a=6, b=10, c=0.02, d=23, e=2.2, f=1.1, g=1.3, h=2.5\) and \(i=4\) and the initial state are \( x(0) = 4, y(0) = 0.8, z(0) = 0.7, u(0) = 1.5\) and \( w(0) = 0.6\), the system shows a chaotic behaviour and the Lyapunov Exponents are obtained as: \( LE1 = 0.315207, LE2 = 0.135137\) and \( LE3 = -0.082011, LE4 = -0.275085, LE5 = -11.9927\). The next figure shows our chaotic attractors:
5. PROPOSED ALGORITHM

Our proposed algorithm, an original image \( O_i \) is passed through the transformations that already exist in the original AES \( O_A \), which are: Sub-Bytes, Shift Rows and Add Round Key; there are two Add Round Keys in our proposed algorithm named, First Add Round key and Second Add Round key. A First Add Round key is applied by using the chaotic sequences that produced from the chaotic system 1 \( C_{s1} \), and Second Add Round key is applied using a normal cipher key. In First Add Round key, each block of the \( O_i \) is encrypted with completely different chaotic key while in Second Add Round key the initial normal key is unmodified during the encryption process as in the \( O_A \). The Mix Columns transformation is removed because it consumes very long time in comparison to the other operations. Chaotic masks will be generated from the chaotic sequences of \( C_{s1} \), where each mask will be divided into blocks of size 4×4 bytes to be used as changing key in modified AES. Finally, encryption process applied as invers order in the side of decryption process. The general structure and the general algorithm of the encryption process are illustrated in figure 6 and Algorithm 1 respectively:

![Figure 5 Phase portrait of the new chaotic system](image)

(a), (b) (c) two-dimensional view, and (d) (e) (f), are three-dimensional view
Figure 6 General Diagram for Encryption process of Our proposed algorithm
6. EXPERIMENT RESULTS
A series of experiments are performed using the proposed algorithm in order to encrypt two color images of JPEG format with size of 256×256 bytes. These images are shown in Figure 7 with their color components. Also, a comparison is made between the O' and O_A:

![Image](http://www.iaeme.com/IJCIET/index.asp)

**Figure 7** (a) Rose image with its RGB components (b) Baboon image with its RGB components

6.1. Key Space Analysis
The size of key must be greater than $2^{100} (\text{Key}_{\text{size}} < 2^{100})$, in order to prevent from the intended attack, which is a process of the break a cryptosystem via exhaustively seeking all probable keys [11]. The key size in our proposed algorithm is calculated according to the parameters
and $I_c$ of the $C_{i,j}$, and if the accuracy of each one is $10^{14}$ then the key size would be $10^{126}$ which are equal to $2^{398}$, in addition to the key range of $O_A$. Thus, the intended attack is impractical in the proposed algorithm.

6.2. Key Sensitivity Analysis

A secure encryption algorithm has sensitivity toward the encryption key in both encryption and decryption processes. When encrypting an $O$, a small change of keys obtains two different $O'$ and when decrypting an $O'$, if an incorrect key is used, different image is obtained [12]. The test of key sensitivity of our proposed algorithm is applied on each of the $O$, where the value of $I_c=0$ of $C_{i,j}$ is slightly changed from $x(0)=\{4, \ldots, 4.00000000000001\}$. Table 1 illustrates that the $O'$ by using a tiny changed key is completely different from the $O$ even with a tenuous difference of $10^{14}$, which means that the proposed algorithm has high sensitive when any change may occur in the key.

| Table 1 Key sensitivity result |

<table>
<thead>
<tr>
<th>Original image</th>
<th>Encryption with $x(0)=4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decrypted image using correct key, $x(0)=4$</td>
<td>Decrypted image using incorrect key, $x(0)=4.00000000000001$</td>
</tr>
</tbody>
</table>

6.3. Histogram Analysis

The histogram analysis of $O$ demonstrates the pixel distribution of an image by through the graph representation for each color component, while histogram of the $O'$ must be fairly uniform and different from the corresponding histogram of $O$ and therefore doesn’t give any clue for employing any statistical analysis on the $O'$ [12]. Table 2 obviously illustrates that the histogram analysis of $O'$ by using $O_A$ and the proposed algorithm is nearly the same, and has uniform distribution and different from the histogram of the $O$.

http://www.iaeme.com/IJCIET/index.asp 1849 editor@iaeme.com
6.4. Correlation Coefficients Analysis

Correlation coefficient is a statistical computation in a range between (-1) and (+1), which measures the robustness of the association between two variables of data. The Correlation coefficient measurement is known by the equation below:

$$ r = \frac{\sum_{mn} \sum_{n}(A_{mn} - \bar{A})(B_{mn} - \bar{B})}{\sqrt{(\sum_{mn} \sum_{n}(A_{mn} - \bar{A})^{2})(\sum_{mn} \sum_{n}(B_{mn} - \bar{B})^{2})}} $$

In which A and B are matrices has similar size, where $\bar{A} = mean(A)$, $\bar{B} = mean(B)$ and $mn$ represent the total number of samples. A zero correlation indicates complete independence and -1 or 1 represents complete dependence. A strong encryption system should have a correlation coefficient near to zero [13]. Table 3 illustrates the correlation coefficients of the O' which encrypted by using $O_{a}$ and the directions of our proposed algorithm (horizontal, vertical and diagonal). The observation of table 3, the correlation coefficients of the O' of Rose using our proposed algorithm is more near to zero than the $O_{a}$ in two directions and O' of Baboon using the proposed algorithm is more close to zero than the $O_{a}$ in one direction, figure 8 and 9 shows the correlation coefficients of pixels distribution of O and O' by using $O_{a}$ and proposed algorithm.
Table 3 Correlation coefficients of encrypted images

<table>
<thead>
<tr>
<th>Image</th>
<th>Original AES</th>
<th>Proposed algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Horizontal</td>
<td>Vertical</td>
</tr>
<tr>
<td>Rose</td>
<td>-0.0022</td>
<td>0.0027</td>
</tr>
<tr>
<td>Baboon</td>
<td>0.0012</td>
<td>0.0023</td>
</tr>
</tbody>
</table>

Figure 8 Correlation coefficients of Rose image in horizontal, vertical and diagonal direction: (a) Original image. (b) Cipher image using original AES. (c) Cipher image using proposed algorithm.

Figure 9 Correlation coefficients of Baboon image in horizontal, vertical and diagonal direction: (a) Original image. (b) Cipher image using original AES. (c) Cipher image using proposed algorithm.

6.5. Entropy Analysis

Entropy of a source provides an idea of self-information, i.e., information obtained via a random process about itself, where it represent trait characteristic of randomness. Let $P(x)$ stands for the information source, the formula for computing the entropy information illustrated in the following equation:

$$\text{Entropy} = -\sum_{i=0}^{n-1} p(x_i) \times \log_2 p(x_i)$$  \hspace{1cm} (3)
Where $P(x_i)$ indicates the prospect of $x_i$ occurrence and $\log$ denotes the base 2 logarithm that represented in bits. The theoretical entropy of an $O'$ should be 8 contrary to its $O$ form, which means the cryptic system is secure against entropy attack [14]. The entropy of $O$ that encrypted by using the $O_\lambda$ and proposed algorithm are shown in table 4, where the entropy of $O'$ by using the proposed algorithm is near to the exemplary value, which is 8, than $O_\lambda$.

### Table 4 Entropy values of encrypted images

<table>
<thead>
<tr>
<th>Image</th>
<th>Original AES</th>
<th>Proposed algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rose</td>
<td>7.9990</td>
<td>7.9991</td>
</tr>
<tr>
<td>Baboon</td>
<td>7.9998</td>
<td>7.9998</td>
</tr>
</tbody>
</table>

#### 6.6 PSNR Analysis

The Peak Signal to Noise Ratio PSNR: is the ratio that computed between $O$ and $O'$. A signal in this state is the original data, and noise is the ciphered data, PSNR is easily well-defined by Mean Squared Error $MSE$ that described in the following equations:

$$ MSE = \frac{1}{M \times N} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [(I(i,j) - K(i,j))^2] $$

$$ PSNR = 10 \times \log_{10} \left( \frac{\text{MAX}_i^2}{MSE} \right) $$

Where, $I$ is an $m \times n$ signal of $O$, $\text{MAX}_i$ is the maximum component of the signal and $K$ is the noise ($O'$). The lower of the PSNR value is the extra distorted in the host image, which indicates to complexity in retrieving the $O$ from $O'$ image for opponents, thus, the higher security is the cryptosystem [15]. PSNR test measures the changes between each pixel of an $O$ (signal) and its corresponding $O'$ (noise). The PSNR values of $O_\lambda$ and the proposed algorithm are illustrated in table 5. The table illustrates that PSNR values of the proposed algorithm are lower than the $O_\lambda$, which represent better encryption quality and reflect the strong safety of the proposed algorithm.

### Table 5 PSNR results of encrypted images

<table>
<thead>
<tr>
<th>Image</th>
<th>Original AES</th>
<th>Proposed algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>R</td>
<td>G</td>
</tr>
<tr>
<td>Rose</td>
<td>8.7197</td>
<td>8.5978</td>
</tr>
</tbody>
</table>

#### 6.7. NPCR and UACI Analysis

The Number of Pixels Change Rate NPCR: and the Unified Average Changing Intensity UACI: is differential attack measurements utilized for evaluating the sensitiveness to slight
modification in the O. Let’s suppose the O’ before and after modifying one pixel in a O are C1 and C2. NPCR and UACI formulas are expressed as below:

\[ NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \] \hfill (6)

\[ UACI = \frac{1}{M \times N} \left[ \frac{\sum_{i,j} |C(i,j) - C'(i,j)|}{255} \right] \times 100\% \] \hfill (7)

In which D is a two dimensional set and has the equal size of image C1 or C2 and M, N are the image height and width dimensions respectively [15]. The results of NPCR and UACI tests in table 6 denote that values of our proposed algorithm are near to the theoretical value than the OA in most image components.

<table>
<thead>
<tr>
<th>Image</th>
<th>Test</th>
<th>Original AES</th>
<th>Proposed algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>R</td>
<td>G</td>
</tr>
<tr>
<td></td>
<td>UACI</td>
<td>33.2921</td>
<td>33.4890</td>
</tr>
<tr>
<td></td>
<td>UACI</td>
<td>31.6933</td>
<td>33.2615</td>
</tr>
</tbody>
</table>

6.8. Execution Time

The time that required by OA and our proposed algorithm to execute both encryption/decryption process with each test images is shown in table 7. The execution time is calculated in seconds. Obviously, the proposed algorithm is faster than the OA during the encryption and decryption process.

<table>
<thead>
<tr>
<th>Image</th>
<th>Original AES</th>
<th>Proposed algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rose</td>
<td>71.98212</td>
<td>93.3814</td>
</tr>
<tr>
<td>Baboon</td>
<td>287.1232</td>
<td>346.5770</td>
</tr>
</tbody>
</table>

http://www.iaeme.com/IJCIET/index.asp 1853  editor@iaeme.com
7. CONCLUSION

In general, speed and secure cryptosystem are very desirable for multimedia applications. In this paper, an efficient algorithm is introduced for color image encryption\ decryption according to improved AES using a novel 5D chaotic systems, and the results that obtained after applying the proposed algorithm illustrated in figure 1, that shows the attractor of the proposed chaotic system and it clearly displays chaotic behavior. The new chaotic system has two positive Lyapunov Exponents, thus it is hyper chaotic, which adds more unpredictability and randomness to the corresponding system. According to the experimental results, the proposed algorithm provides high key space, high key sensitivity and less time for encryption and decryption process than O\textsuperscript{A\textregistered} as well as offering acceptable resistance against differential and statistical attacks.

ACKNOWLEDGMENTS

The Authors would like to thank Mustansiriyah University (www.uomustansiriyah.edu.iq) Bagdad-Iraq for its support in the present work.

REFERENCES


