Adaptive Pixel-Selection Fractional Chaotic Map Lattices for image cryptography

Jirasak Sittigorn* and Kittipat Paithoonwattanakij

Faculty of Engineering, King Mongkut's Institute of Technology Ladkrabang, Chalongkrung Rd., Ladkrabang, Bangkok, 10520, Thailand.

Received 6 May, 2015; Accepted 20 July, 2015

Chaotic theory has been employed in cryptography application for establishing a sequence of data closest to pseudorandom number. Image cryptography with Chaotic Map Lattices (CML) uses the chaos parameters, the number of iterations and the number of cycles for encryption as secret keys. Amount of secret keys has a great impact on security in cryptography. Adaptive Pixel-Selection Fractional Chaotic Map Lattices (APFCML) enhances the encryption security by introducing a novel non-integer fractional order concept as secret keys. Fractional chaos is modified chaos with a fractional differential equation containing derivatives of non-integer order. A non-integer order has an effect on the range of chaos's parameter. Moreover, the encryption sequence has been adaptively selected based on another chaos generator. In the experiments, the measurement indices of originality preservation, visual inspection, and statistical analysis are used to evaluate the performance of the proposed APFCML compared to that of the original CML.

Key words: Chaotic, fractional logistic, image cryptography, Lyapunov exponent, bifurcation diagram.

INTRODUCTION

In the current trends, the communication is through the public network such as the Internet. The secure communication is crucial for business communication (Pecora and Carroll, 1990; Van Wiggeren and Roy, 1998). Electronic banking and military communication are two sample applications that clearly require a secure communication. The cryptographic algorithm is a method to protect plain text by changing it to data confidentiality. The cryptographic algorithm encrypts the plain text to a ciphered text using a key or keys, and it decrypts the ciphered text back to the plain text (Pareek et al., 2003).

Symmetric-key cryptography is algorithms for cryptography used the same keys for both encryption and decryption while asymmetric cryptography uses different keys for encryption and decryption. Since the symmetric-key cryptography shared keys when transforming a message back and forth, it becomes a target of attacking from an intruder. An attack can simply try different keys until the plain text is found.

The chaotic theory has been applied to the symmetric-key cryptography. It is a field of science that studies behavior of nonlinear dynamic systems that are highly...
sensitive to small variation of an initial condition. The output of a dynamic system is greatly deviated when initial conditions or parameters are changed. Therefore, initial conditions and system parameters are used as keys for the chaotic cryptography. The nature of a chaotic system makes a dictionary attack impractical. Chaotic Map Lattices (CML) (Pisarchik et al., 2006) is a cryptographic algorithm using the chaotic theory. Without knowledge of keys used in an encryption process, the decryption is practically difficult. The keys for the CML are chaotic parameters, number of iterations, and number of cycles. The parameters are variables in a logistic map that is well known chaotic systems. The limitation of a logistic map is the value of the parameter between 3.57 and 4. Therefore, a logistic map was chaos. When CML is applied to image cryptography, it encrypts and decrypts every pixel of an image. The CML algorithm uses an initial condition from the previous pixel in sequence for the current encrypting pixel. As a result, it is possible to decrypt all the sequence of the encrypted pixels if the intruder can guess secret keys and the initial condition of the first pixel. In order to enhance the encryption security, an Adaptive Pixel-Selection Fractional Chaotic Map Lattices (APFCML) algorithm is proposed, where the encryption sequence has been adaptively selected. Even though the intruder can guess the secret keys and the initial condition of the first pixel, it is quite difficult to acquire the whole encryption sequence. Another limitation of the CML algorithm is the amount of secret keys. The presented APFCML algorithm is based on fractional order and a parameter of fractional chaos with fractional-order as a new secret key. The fractional-order system is a dynamical system that can be modeled by a fractional differential equation containing derivatives of non-integer order (Monje et al., 2010). Fractional chaos is the chaotic system when fractional-order and the selected parameters are appropriate. Each fractional-order offers difference boundary of parameter. The remainder of this paper is organized as follows. The methodology section describes the chaotic system, the fractional order logistic model, Lyapunov exponent, bifurcation diagram, fractional chaotic system, and encryption and decryption algorithm using APFCML.

**METHODOLOGY**

**Chaotic system**

A logistic map is the well known chaotic systems, which is a polynomial mapping of degree two, and is given by:

\[ x_{n+1} = rx_n(1-x_n) \]  \hspace{1cm} (1)

Where \( x_n \) is the system variable, \( r \) is the parameter, \( n \) is the number of iterations and \( x_0 \) is an initial condition. The system variable and parameter lead to chaotic system when \( x_{\text{min}} < x < x_{\text{max}} \).

\[ x_{\text{max}}, \ 3.57 < r < 4, \ x_{\text{max}} = \frac{r}{4} \text{ and } x_{\text{min}} = \frac{r^2}{4} \left(1 - \frac{r}{4}\right). \]

**Fractional order logistic model**

The fractional order logistic model was the mathematical form accomplished by integral and derivative of fractional order (Podlubny, 1999). This mathematical field may be considered as old topic since it is been developed for more than a century (Podlubny, 1999). Recently, this mathematical theory has applied to many modem applications in physics and engineer (Petras, 2006; Sabatier et al., 2007). The fractional order logistic equation is obtained by apply the fractional operator to the logistic equation as follow:

\[
\frac{d^\alpha x}{dx^\alpha} = \frac{\Gamma(\mu+1)}{\Gamma(\mu-n+1)} x^{\alpha-n}
\]  \hspace{1cm} (2)

Where \( \Gamma(\ ) \) is the Gamma function. The Gamma function is defined as \( n! = \Gamma(n+1) \).

The fractional order logistic model is operated by fractional derivative of logistic equation. The model is initially published by Pierre Verhulst (Pastijn, 2006). First order ordinary differential equation describes the continuous model. The discrete model discloses the chaotic property in certain regions (Alligood et al., 1996). The logistic Equation (1) is written as the sigmoid function as \( f(x) = rx(1-x) \).

The fractional order logistic equation is obtained by applies the fractional operator to the logistic equation as follows:

\[
D^\alpha f(x) = \frac{rx^{1+\alpha}}{\Gamma(\alpha+2)} \left(1 - \frac{2x}{\alpha+2}\right)
\]  \hspace{1cm} (3)

Where \( D^\alpha f(x) \) is the \( \alpha \)-order derivative of a function \( f(x) \), \( r \) is parameter, \( \alpha \) is fractional order when \( -\infty < \alpha < \infty \).

The result of the fractional logistic equation becomes chaotic at some of parameter. Figures 1 and 2 illustrate the results with the number of iterations \( n=1-6 \). It can be seen that the chaotic behavior trends of fractional logistic equation arises at parameter \( r=6 \) for order \( \alpha = \frac{1}{2} \) and parameter \( r=5 \) for order \( \alpha = \frac{1}{4} \). The Lyapunov exponent and bifurcation diagram are tools for indicating chaos system.

**Lyapunov exponent**

In mathematics, the Lyapunov exponent is quantified the average stability for describing the discrete dynamical system which can compute from the result of numerical simulation or a physical experiment (Alligood et al., 1996; Moon, 2004). The characteristics of Lyapunov exponents are analyzed by the linear stability of non periodic system. An indicator is the typical rate of exponential divergence of nearby trajectories (Alligood et al., 1996; Suansook and Paithoonwattanakij, 2014). This quantity characterizes the rate of separation of nearby close trajectories. The differences of initial condition and trajectories are provided the different in rate of separation. The dynamic system predictability is determined by the largest Lyapunov exponent. The positive value of Lyapunov...
The Lyapunov exponent or exponential rate of divergence per iteration is defined as follow:

\[ \lambda = \lim_{N \to \infty} \frac{1}{N} \sum_{n=1}^{N} \ln \left| \frac{df(x_i)}{dx} \right| \]

(4)

Where \( \frac{df(x_i)}{dx} \) is the derivative of a function \( f(x_i) \), \( \lambda \) is the Lyapunov exponent.

The Lyapunov exponent of fractional order logistic model can be calculated from the Equations (3) and (4). The numerical results of Lyapunov exponent of fractional logistic model for different order are shown in Figure 3.

**Bifurcation diagram**

Bifurcation theory was studies of changes in the qualitative of periodic point structure of dynamical systems, which is varying with time. The parameters are changed in a dynamical system, the stability of the balance points can change as well as the number of balance points. The values of parameters at which the qualitative or topological nature changes are known as critical or bifurcation values (Baker and Gollub, 1990). This occurs where a linear stability analysis yields an instability which characterized by a growth rate of a perturbation of the base solution. In dynamical system, a bifurcation diagram shows the possible long-term values either fixed points or periodic of a system as a function of a bifurcation parameter. In general, the bifurcation diagram represents stable solutions with solid line and unstable solutions with a dotted line. The theory of bifurcation is to study how the equilibrium points changes with the parameters (Suansook and Paithoonwattanakij, 2006). The bifurcation diagrams of the fractional order logistic equation for different order are illustrated in Figure 4.

Results of Lyapunov exponent and bifurcation diagram for each fractional order are used to describe the chaotic of fractional order logistic equation. The equation become chaotic when Lyapunov exponent value is greater than zero or Bifurcation Diagram are many values at the either fixed point (Table 1).

Image cryptography with regular CML considers the chaos parameters from a logistic map as one of secret keys. A logistic map becomes the chaotic system when the value of the parameter is between 3.57 and 4. However, in the proposed APFCML, the fractional logistic equation is chosen as additional secret keys. With dual sets of the secret keys, the encryption key length is extensive, thus the encryption security can be greatly intensifie.

The Lyapunov exponent and Bifurcation diagrams of fractional order logistic model are presented in Figures 3 and 4 respectively in order to illustrate the possibility of chaotic behavior in each fractional order. Even though the chaotic properties in fractional order logistic model depend on the same parameters as that of the logistic map, the order parameter is not restricted. Table 1 presents 10 samples of chaotic behavior cases with the order of fractional up to 9. With other fractional, the chaotic behavior can also be achieved. This leads to extensive selection of the fractional order parameters.
Fractional chaotic system

The fractional logistic equation of order $\alpha$ in Equation (3) is rewritten in a logistic map as followed.

$$x_{n+1} = \frac{rx_n^{1+\alpha}}{\Gamma(\alpha+2)} \left( 1 - \frac{2x_n}{\alpha+2} \right)$$

(5)

Where $x_n$ are the system variable, $r$ is the parameter, $n$ is the number of iterations. $x_0$ is an initial condition and $\alpha$ is fractional order. For all $x \geq 0$ and $\alpha > 0$, $x_{\text{max}}$ and $x_{\text{min}}$ are as following.

$$x_{\text{max}} = \frac{r (1+\alpha)^{1+\alpha}}{2^{1+\alpha} \Gamma(\alpha+2)} \left( 1 - \frac{\alpha+1}{\alpha+2} \right)$$

(6)

$$x_{\text{min}} = \frac{r (1+\alpha)^{1+\alpha}}{2^{1+\alpha} \Gamma(\alpha+2)} \left[ 1 - \left( \frac{r (1+\alpha)^{1+\alpha}}{2^{1+\alpha} \Gamma(\alpha+2)} \left( 1 - \frac{\alpha+1}{\alpha+2} \right) \right)^{\alpha+1} \right]$$

(7)

The image encryption, the image can be represented as a lattice of pixels. The color image is a combination of the three components: red, green, and blue shown as $C = (C_r, C_b, C_g)$. Encryption creates $x_c$ by processing each of color component in parallel

$$x_c = (x_r, x_b, x_g).$$

Normally, value of each component is an integer between 0 and 255. APFCML converts the integer value into the range of chaotic system variable by using the following transformation.

$$x_c = x_{\text{max}} + \delta x (C+1) / (257)$$

(8)

Where $\delta x = x_{\text{max}} - x_{\text{min}}$. To extract the value of color component, the inverse function is applied as followed:

$$C = \text{round}( (x_c - x_{\text{min}}) / \delta x - 1)$$

(9)

Where round is rounding function that replaces a numerical value to integer. With the modified normalization boundary, it results in complete recovery of the original pixel values.

Encryption and decryption algorithm

The revised encryption algorithm composes of the following steps.

Encryption algorithm

(1) Define secret keys as number of iteration ($N$), number of cycle ($J$). Define the new secret keys as fractional order $\alpha$, parameter of fractional order $r$, chaotic parameters $r_i$ and initial condition $x_{i,n0}$.
(2) Convert two image containing two dimensional pixels \((Row \times Column = m \text{ pixels})\) into a sequential pixel of size \(m\) \((l = 1, 2, 3, \ldots, m)\), which its value is calculated in terms of variable \(C\).

(3) Calculate sequential data \(m\) from the equation (1) with new secret keys \((r_i\) and \(x_{c0})\) in step 1). Sort sequential data as sequential pixels for encryption.

(4) Calculate \(x_c\) with Equation (8) of pixel \(l\) with new secret keys \((\alpha\) and \(r\)).

(5) Use the value of the last first element in sequential pixel in step 4) \((x_{cfirst})\) as the initial condition for the first element in sequential pixel \((x_{0first})\).

(6) Obtain the mapping variable \(x_{nfirst}\) by iterating \(N\) times of the first element in sequential pixel from Equation (10). Add the mapping variable \(x_{nfirst}\) and the value of pixel \((x_{cfirst})\). The sum of value is applied as the initial condition for the subsequent order. Sometime, sum of value is over range of chaos system \((x_{\text{max}})\). We used the condition in Equation (12) to solve the problem. Iterate all maps subsequently starting from the first element in sequential pixel and going through encrypt image pixels, pixel by pixel, toward the last element in sequential pixel. The new \(x_c\) is the latest result of this cycle.

Figure 4. Bifurcation Diagram of fractional order logistic model at fractional order \(\alpha\).
Table 1. The rank of parameter for chaos system.

<table>
<thead>
<tr>
<th>Fractional order</th>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1</td>
<td>7.85-8.72</td>
</tr>
<tr>
<td>1/2</td>
<td>5.61-6.35</td>
</tr>
<tr>
<td>1/3</td>
<td>4.90-5.5</td>
</tr>
<tr>
<td>1/4</td>
<td>4.55-5.15</td>
</tr>
<tr>
<td>1/5</td>
<td>4.35-4.92</td>
</tr>
<tr>
<td>1/6</td>
<td>4.22-4.77</td>
</tr>
<tr>
<td>1/7</td>
<td>4.13-4.65</td>
</tr>
<tr>
<td>1/8</td>
<td>4.05-4.57</td>
</tr>
<tr>
<td>1/9</td>
<td>4.00-4.51</td>
</tr>
</tbody>
</table>

(7) Use the last element in sequential pixel \( x^1_{\text{last}} \) of previous cycle in step 7) as an initial condition for the first element in sequential pixel in the new cycle. Repeat step 6) overall the number of cycles \( J \).

(8) Convert the sequence of encrypted data \( x_c \) back to the image containing two dimensional.

The encryption algorithm can be summarized as following Equations (10) to (12).

\[
x^0_1(j) = x^\text{last}_1(j-1) \quad \text{if} \quad i = 1^a \quad (10)
\]

\[
x^0_j(j) = x^{-1}_1(j) \quad \text{if} \quad i \neq 1^a \quad (11)
\]

\[
x(j) = \begin{cases} 
  x^0_j(j-1) + x^0_j(j) & \text{if} \quad x^0_j(j-1) + x^{-1}_1(j-1) \leq x_{\text{max}} \\
  x^0_j(j-1) + x^{-1}_1(j-1) - \delta x & \text{if} \quad x_{\text{min}} < x^0_j(j-1) + x^{-1}_1(j-1) \leq 2x_{\text{max}} - 2x_{\text{min}} \\
  x^0_j(j-1) + x^{-1}_1(j-1) - 2\delta x & \text{if} \quad 2x_{\text{min}} - 2x_{\text{max}} < x^0_j(j-1) + x^{-1}_1(j-1)
\end{cases} \quad (12)
\]

Decryption algorithm

The revised decryption algorithm is as follows.

(1) Use secret keys from Encryption Algorithm as parameter, number of iteration, number of cycle and the new secret keys in step 1).

(2) Convert the encrypted image containing two dimensional in terms of sequence encrypted data \( x_c \).

(3) Calculate the encrypted image \( m \) from the Equation (1) with new secret keys in step 1). Sort sequential data as sequential pixel for decryption.

(4) Recover the image of the \( j-1 \) cycle. Start decryption at the last element in sequential pixel by using previous order pixels \( x^{i-1}_1(j) \) as initial condition \( x^0_j(j-1) \). Calculate \( x^0_j(j-1) \) at \( n \) iterations from the Equation (5). Subtract the last element in sequential pixel \( x^0_j(j) \) by \( x^{-1}_1(j-1) \). Continue decryption process to the first element in sequential pixel.

(5) Apply the last element in sequential pixel of \( j-1 \) cycle as the initial condition at the first element in sequential pixel \( x^0_j(j-1) \). After \( n \) iterations from (1) \( x^0_j(j-1) \). Subtract the first order \( x^{i-1}_1(j) \) by \( x^{-1}_1(j-1) \). The subtraction value is used as the initial condition for the next element in sequential pixel. Sometime, the subtraction of value is under range of chaos system \( (x_{\text{new}}) \). We propose the new condition in Equation (14).

(6) Repeat steps (4) to (5) for the next cycles until cycle \( j=0 \).

(7) Convert the decrypted data \( x_c \) back to the image containing two dimensional and then convert to the original image with formula (8) (Figure 5).

The decryption algorithm can be summarized as follows in Equation (13) to (15).

\[
x^0_j(j-1) = x^{i-1}_1(j) \quad \text{if} \quad i \neq 1^a \quad (13)
\]

\[
x^0_j(j-1) = x^{\text{last}}_1(j-1) \quad \text{if} \quad i = 1^a \quad (14)
\]

\[
x^0_j(j) = \begin{cases} 
  x^0_j(j-1) + x^0_j(j) & \text{if} \quad x^0_j(j-1) + x^{-1}_1(j-1) \geq x_{\text{max}} \\
  x^0_j(j-1) + x^{-1}_1(j-1) - \delta x & \text{if} \quad x_{\text{min}} < x^0_j(j-1) + x^{-1}_1(j-1) \leq 2x_{\text{max}} - 2x_{\text{min}} \\
  x^0_j(j-1) + x^{-1}_1(j-1) - 2\delta x & \text{if} \quad 2x_{\text{min}} - 2x_{\text{max}} < x^0_j(j-1) + x^{-1}_1(j-1)
\end{cases} \quad (15)
\]

ANALYSIS AND TEST RESULTS

Visual inspection

The encryption motivates the changes in pixel values without visual perception. Encryption quality is measured on how much changes can be introduced with minimum visual recognition. It can be measured as subjective test or objective tests in terms of statistical analysis such as histogram analysis, correlation analysis, cross-correlation analysis, and Gray Modification Average Value. The employed secret keys for the CML based encryption are the logistic map parameters, the number of iterations, and the number of cycles while fractional order parameters of the logistic model are additionally introduced in the proposed APFCML based encryption. In order to illustrate the comparative encryption quality of both encryption systems, the examples of experimental results obtained from the CML based encryption with \( r = 3.90 \) and those obtained from the proposed APFCML based encryption with \( \alpha = \frac{1}{2} \) and \( r = 5.90 \) are presented in Figure 6. Both encryption systems are compared with the same number of iterations and the number of cycles. Figure 6 shows the encrypted Lena images with ten combination of the number of iterations and the number of cycles of \( J = 1, N = 1-5 \) and \( J = 2, N = 1-5 \).

From the results, it can be seen that the CML and the APFCML deliver high encryption quality when the number of cycles is greater than 1. Observing the encrypted images with number of cycles is 2 and the number of iterations is 1 that the CML have Lena image information more than the APFCML. The APFCML is more efficiency than the CML.
Statistical analysis

The statistical analysis was analyzed in image encryption (Pareek et al., 2006; Liu et al., 2009). An encryption result should be robust against any statistical attack. The histograms of the test images and the correlations of two adjacent pixels in the encrypted images are simulated for statistical analysis.

Histogram analysis

It is important to verify that there is no statistical similarity between the encrypted and original images in order to prevent the leakage of information to the attackers. The statistical similarity can be illustrated in term of histograms, which present the distribution of the pixel intensity in images. Histogram of the Lena original image is shown in Figure 7a. Figure 7(b-f) shows histogram of the encrypted image using CML at $r = 3.90$. Figure 7(g-k) shows histogram of the encrypted image using APFCML when $\alpha = \frac{1}{2}, r = 5.90$. The histogram of original image contains large fluctuation while that of the encrypted image is close to the uniform distribution. It is significantly different from the original image. This shows that no statistical similarity appears between the encrypted and the original images.

From the results, the histogram distribution of the CML based encryption is close to the uniform distribution when $J$ is greater than 1 and $J$ is equal to $N$ while that of the proposed APFCML based encryption can accomplish the goal with the $J = 1, N = 2$. It can be seen that the proposed APFCML based encryption can converge to the desired distribution with lower order of the secret key parameters, thus it can allow extensive range of the encryption parameters. This can guarantee that the encryption with the proposed APFCML based system can achieve greater encryption security than that of the CML based system.

Correlation coefficient analysis

The correlation coefficient analysis is one of the important statistical analysis tools, which measures the statistical
Figure 6. The encrypted Lena image with CML $r = 3.90$ and APFCML $\alpha = \frac{1}{2}, r = 5.90$.

Figure 7. Histogram of (a) the original image and the encrypted image (b)-(f) CML $r = 3.90$ (g)-(k) APFCML $\alpha = \frac{1}{2}, r = 5.90$. 
relationship between two horizontally adjacent pixels and
two vertically adjacent pixels in encrypted image (Pareek et al., 2006; Liu et al., 2009). For effective image
cryptography, all the attributes of the original images
should be concealed, and the encrypted images should be
highly uncorrelated. If the original and encrypted
images are uncorrelated or totally different, their
correlation will be very low or close to zero. If they are
identical, their corresponding correlation will be equal to
one. Figure 8 shows the distribution of two vertically
adjacent pixels and two horizontally adjacent pixels.
Figure 8(a) shows the distribution of the original Lena
image. Figure 8 (b, d, f, h, j) show the distribution of the
encrypted Lena image from CML \( r = 3.90 \). The
distributions of the encrypted Lena image from APFCML
\( \alpha = \frac{1}{2}, r = 5.90 \) are shown in Figure 8(c, e, g, l, k).

The determination of how well adjacent pixels are
correlated is to consider the regression line representing
the data. The horizontally and vertically adjacent pixels
are considered highly correlated if the regression line
passes through points on the scatter plot. Otherwise, they
are considered less correlated. The results show that the
distributions obtained from the proposed APFCML based
encryption are greatly dispersed from the scatter line for
all Js and Ns while those of the CML based encryption
are dispersed when J and N are greater than 2. This
means that the APFCML encrypted pixels are greatly
uncorrelated and it results in less visual perception and
higher encryption quality.

Cross-correlation equation

The cross-correlation technique is a method to estimate
the displacement information of two consecutive images
by comparing the similarity of a pair of image signals
(Kocarev et al., 2004; Solak and Çokal, 2008). The cross-
correlation between two vertically and two horizontally
adjacent pixels in the original and encrypted images are
calculated using Equation (10) (Pareek et al., 2006; Liu et
al., 2009).

\[
C_i = \frac{N \sum_{j=1}^{N} (x_j \times y_j) - \sum_{j=1}^{N} x_j \sum_{j=1}^{N} y_j}{\sqrt{\left( N \sum_{j=1}^{N} x_j^2 - \left( \sum_{j=1}^{N} x_j \right)^2 \right) \times \left( N \sum_{j=1}^{N} y_j^2 - \left( \sum_{j=1}^{N} y_j \right)^2 \right)}}
\]

(16)

Where \( x_j \) is intensity of pixel at location \((x_j, y_j)\), \( y_j \) is
intensity of pixel at location \((x_j + 1, y_j)\) for the cross-
correlation of two vertically and \( y_j \) is intensity of pixel at
location \((x, y_j + 1)\) for the cross-correlation of two
horizontally.

Figure 9(a) demonstrates correlation coefficient analysis
with CML based encryption for vertical and horizontal
directions with various combinations of N and J
parameters. The correlation coefficient analysis with
APFCML based encryption is shown in Figure 9(b-d). It
can be seen that, to achieve the correlation less than
0.05 for all variations of N, it limits the values of J greater
than 5 for the CML thus greater than 3 for the APFCML.
From the results, it demonstrates that the APFCML
permits larger variation of secret keys with higher
encryption quality for all parameters.

The results from Figure 9(a) and (b) show the correlation coefficient for the CML at J = 1 N = 1 more
than the correlation coefficient for the APFCML that
accords with the results of the visual inspection and the
histogram analysis.

Gray modification average value

The values of pixels in the image encryption have been
changed from the original image. Visual testing can show
contrast between the original image and the image
encryption. The percentage of unchanged point
represents percentage of pixels difference. Gray
modification average value, called GAVE, can measure
the change in value of image encryption. The higher the
GAVE value, the better the encrypted image. GAVE is
defined in Equation (22), where \( G = \left( g_{ij} \right)_{M \times N} \) is the
original image and \( C = \left( c_{ij} \right)_{M \times N} \) is the image encryption (Li
and Wang, 2011).

\[
GAVE(G, C) = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} \left| g_{ij} - c_{ij} \right|}{MN}
\]

(17)

GAVE of all pixels in the image are shown in Figure 10.
For the CML, GAVE will increase when number of cycle
increases and number of iterations is greater than 7. At
J=1, GAVE tends to converge slower. This is supported
by the visual inspection results where the original
information can still be perceived. For the APFCML,
value of GAVE swing at number of cycleless than 3.
Result shown GAVE value of APFCML more than CML.

Conclusion

This paper proposes an adaptive pixel-selection fractional
chaotic map lattices for image cryptography to enhance
the encryption security and overcome the limitation of the
original CML. In the APFCML based encryption, the
fractional logistic equation is applied in cryptography,
which provides new secret keys as fractional order. In
addition, the encryption sequence has been adaptively
Figure 8. The distribution of two vertically adjacent pixels and two horizontally adjacent pixels of the original and encrypted Lena image with CML $r = 3.90$ and APFCML $\alpha = \frac{1}{2}, r = 5.90$. 
Figure 9. Correlation Coefficient Analysis for various combinations of $J$ and $N$ parameters of (a) CML $r = 3.90$ (b) APFCML $\alpha = \frac{1}{2}, r = 5.90$ (c) APFCML $\alpha = \frac{1}{2}, r = 5.97$ and (d) APFCML $\alpha = \frac{1}{4}, r = 4.85$. 

Sittigorn and Paithoonwattanakij 541
selected based on the chaos generator. Even though the intruder can guess the secret keys and the initial condition of the first pixel, it is quite difficult to acquire the whole encryption sequence. In the experiments, the measurement indices of originality preservation, visual inspection, and statistical analysis are used to evaluate the performance of the proposed APFCML compared to that of the original CML.

Conflict of Interest

The authors have not declared any conflict of interest.

REFERENCES


