On the Periods of Some Transformations Used in Digital Image Scrambling

Shaochuan Fu¹,²  Chengxian Xu¹
(¹ Xi’an Jiaotong University ² Beijing Jiaotong University)

Abstract: In this paper, the authors have analyzed several transformations used in digital image scrambling, giving some results on the periods of that transformation. Some notes on the transformation when it is used have been proposed and the fast calculation method to these reverse transforms. The results of this paper can make the computing complexity lower when the scrambling image is deciphered.

Key words: linear transformation, affine transformation, integral residue rings, period, digital image scrambling

1. Foreword:
With the rapid development of multimedia technology, more and more digital images are transferring on the network, these image information possibly involves with national security or company benefits, its value is invaluable, so it is extremely important for the security of image transmission on the network and image encryption has become a vigorous research direction.

During the process of digital image scrambling, generally the original image is pretreated, and the common method for pretreatment is to make proper transformation to original image. There are many methods for image transformation, such as Arnold transformation [1], alignment transformation [2], Fibonacci transformation [3], affine transformation [4]. Above-mentioned transformation

Above-mentioned change periods is one of the current unsettled problems, this thesis presents the estimation method for these changes, thus the period estimation problem to all kinds of image size by affine transformation which presented in text [5] is settled; all the reverse transformation for above-mentioned changes is the second currently unsettled problem, because reverse transformation is needed during the process of image information decryption, for instance, the
period for Aronld change is 192, lots of unnecessary computation is added during decryption process of Aronld change, for these problems, this thesis gives a method that can finish all the changes in all kinds of above-mentioned decryption change process, no complicated computation is existed. For the convenience of application, we assume that $N=2^e$ permanently.

2. Polynomial and its property on the ring

First let’s have a look of polynomial [5] on the ring of $\mathbb{Z}/2^e$.

$$f(x) = x^n + \sum_{j=0}^{n-1} c_j x^j,$$

among which,

$$c_j = \sum_{i=0}^{2^e-1} c_{j,i} 2^i,$$

f(x) also has binary dissociation :

$$f(x) = \sum_{i=0}^{2^e-1} f_i(x) 2^i, \quad f_i = \sum_{j=0}^n c_{j,i} x^j,$$

among which

3. Period for all kinds of changes

(1) Aronld change

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \mod N,$$

$x, y \in \{0, 1, 2, \ldots, N-1\}$

of which. N is the pixel number of image height and width.
\[ T = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}, \quad |T - Ix| = \begin{vmatrix} 1 - x & 1 \\ 1 & 2 - x \end{vmatrix} = x^2 - 3x + 1 \]

Keeps

Then \( |T - Ix| \mod 2 = x^2 + x + 1 \), while \( x^2 + x + 1 \) is \( F_2 \)'s 2-order origin polynomial. But \( x^3 - 1 = (x - 1)(x^2 + x + 1) \), so now \( q(x) = x - 1, r(x) = 0 \). Again in \( x^2 + x + 1, f_1 = 0 \), so \( h_2(\Lambda) = 0 \), namely \( \triangle_1 = 0 \). Thus the maximum period of \( x^3 - 3x + 1 \) is \( 2^6 \times 3 = 192 \), T's change tendency is as follows:

<table>
<thead>
<tr>
<th>( T )</th>
<th>( T^2 )</th>
<th>( T^3 )</th>
<th>( T^{64} )</th>
<th>( T^{128} )</th>
<th>( T^{192} )</th>
<th>( T^{384} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \begin{pmatrix} 1 &amp; 1 \ 1 &amp; 2 \end{pmatrix} )</td>
<td>( \begin{pmatrix} 2 &amp; 3 \ 3 &amp; 5 \end{pmatrix} )</td>
<td>( \begin{pmatrix} 13 &amp; 21 \ 21 &amp; 34 \end{pmatrix} )</td>
<td>( \begin{pmatrix} 29 &amp; 197 \ 197 &amp; 226 \end{pmatrix} )</td>
<td>( \begin{pmatrix} 226 &amp; 59 \ 59 &amp; 29 \end{pmatrix} )</td>
<td>( \begin{pmatrix} 1 &amp; 0 \ 0 &amp; 1 \end{pmatrix} )</td>
<td>( \begin{pmatrix} 1 &amp; 0 \ 0 &amp; 1 \end{pmatrix} )</td>
</tr>
</tbody>
</table>

(2) Arrangement transformation

\[
\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \mod N,
\]

\( x, y \in \{0, 1, 2, \ldots, N-1\} \) (7)

of which, \( \{ad-bc=\pm 1, a, b, c, d \in \mathbb{Z}\} \). When \( a=b=c=1, d=2 \), arrangement transformation is Arnold transformation. When \( a=b=c=1, d=0 \), arrangement transformation is Fibonacci transformation.

Now keeps \( T_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \), then

\[
|T_1 - Ix| = \begin{vmatrix} a - x & b \\ c & d - x \end{vmatrix} = x^2 - (a + d)x + (ad - bc) = x^2 - (a + d)x + 1
\]

(8)

So, when \( a+d \) is an odd number, the maximum period of \( T_1 \) on the ring \( F_2^8 \) is 384. When \( a+d \) is an even number, \( |T_1 - Ix| \mod 2 = x^2 + 1 \), then the period of \( T_1 \) on the ring \( F_2^8 \) is the multiplier of 256.

Example 1. in arrangement transformation, when assumes \( a=c=d=1, b=0 \),

\[
T^{256} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I
\]

. Degradation is occurred for T's period. When assumes

\[
T = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix},
\]

\( T^{128} = I \), when assumes \( T^{64} = I \), \( \ldots \); Assumes \( T = \begin{pmatrix} 1 & 0 \\ 128 & 0 \end{pmatrix}, T^2 = I \). While above-mentioned T are all satisfied with conditions \( ad-bc=1 \). \( (0, 0) \) is their common stationary
Example 1 shows that, in arrangement transformation, the selection of a, b, c, d is conditioned, we suggest that when a, d is selected, it should be satisfied with \(a + d = 1 \mod 2\). 

(3) Fibonacci transformation

In Fibonacci transformation, transformation matrix

\[
T = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix},
\]

then \(|T - Ix| = \begin{vmatrix} 1 - x & 1 \\ 1 & -x \end{vmatrix} = x^2 - x + 1\), so \(|T - Ix| \mod 2 = x^2 + x + 1\), while \(\triangle f = 0\), so, the period (when \(N = 2^e\)) of Fibonacci transformation is the multiplier of \(3 \times 2^e\), when \(e = 8\), its period is not bigger than 192.

(4) Affine transformation

The general form of affine transformation is:

\[
\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} e \\ f \end{pmatrix},
\]

(9)

The affine transformation is used in text [4] is:

\[
\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & N - 1 \\ N - 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \end{pmatrix} \mod N, x, y \in \{0, 1, 2, \ldots, N - 1\}
\]

(10)

This affine transformation is combined by two parts, they are marked as \(T(1)\), \(T(2)\) respectively, namely:

\[
\begin{pmatrix} x' \\ y' \end{pmatrix} = T^{(1)} \begin{pmatrix} x \\ y \end{pmatrix} + T^{(2)} \begin{pmatrix} x \\ y \end{pmatrix}
\]

Here

\[
T^{(1)} = \begin{pmatrix} 1 & N - 1 \\ N - 1 & 0 \end{pmatrix}, \quad T^{(2)} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}.
\]

Within \(F_2^8\), the period of \(T(2)\) is 256, while

\[
|T^{(1)} - Ix| = \begin{vmatrix} 1 - x & N - 1 \\ N - 1 & -x \end{vmatrix} = x^2 - x - (N - 1)^2 = x^2 - x - 255^2.
\]

Thus \(|T^{(1)} - Ix| \mod 2 = x^2 + x + 1\). Since \(\triangle f \neq 0\), the period of \(T^{(1)}\) is \((\text{within } F_2^8)\)384. Known from the following conclusion, for the affine transformation given by formulation (10), its period is 384, thus the problem of the period of affine transformation is smaller than the period of Aronld transformation doesn’t exist. Of course, we also settle the period estimation problem of affine transformation to all kinds of image size that presented by text [4].
In affine transformation

\[
P \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} e \\ f \end{bmatrix} \mod N
\]

(11)

\[
A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}
\]

assumes the period of \( N_0 \) is \( N_0 \). \( B = A^N_0 + A^{N_0-1} + \cdots + A^1 + A^0 \) then

\[
AB = A^{N_0} + A^{N_0-1} + \cdots + A^2 + A = I + A^{N_0-1} + A^{N_0-2} + \cdots + A^2 + A = B
\]

(12)

\[
P^2 \begin{bmatrix} x \\ y \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} e \\ f \end{bmatrix} + \begin{bmatrix} e \\ f \end{bmatrix}
\]

\[
= A^2 \begin{bmatrix} x \\ y \end{bmatrix} + A \begin{bmatrix} e \\ f \end{bmatrix} + \begin{bmatrix} e \\ f \end{bmatrix}
\]

(13)

\[
P^T \begin{bmatrix} x \\ y \end{bmatrix} = A^T \begin{bmatrix} x \\ y \end{bmatrix} + A^{T-1} \begin{bmatrix} e \\ f \end{bmatrix} + A^{T-2} \begin{bmatrix} e \\ f \end{bmatrix} + \cdots + A \begin{bmatrix} e \\ f \end{bmatrix} + \begin{bmatrix} e \\ f \end{bmatrix}
\]

\[
= A^T \begin{bmatrix} x \\ y \end{bmatrix} + [A^{T-1} + A^{T-2} + \cdots + A + I] \begin{bmatrix} e \\ f \end{bmatrix}
\]

(14)

\[
P^{N_0} \begin{bmatrix} x \\ y \end{bmatrix} = A^{N_0} \begin{bmatrix} x \\ y \end{bmatrix} + B \begin{bmatrix} e \\ f \end{bmatrix} = \begin{bmatrix} x \\ y \end{bmatrix} + B \begin{bmatrix} e \\ f \end{bmatrix}
\]

(15)

\[
P^{N_0+1} \begin{bmatrix} x \\ y \end{bmatrix} = A^{N_0+1} \begin{bmatrix} x \\ y \end{bmatrix} + B \begin{bmatrix} e \\ f \end{bmatrix} + \begin{bmatrix} e \\ f \end{bmatrix}
\]

(16)

\[
P^{N_0+2} \begin{bmatrix} x \\ y \end{bmatrix} = A^{N_0+2} \begin{bmatrix} x \\ y \end{bmatrix} + B \begin{bmatrix} e \\ f \end{bmatrix} + \begin{bmatrix} e \\ f \end{bmatrix}
\]

(17)

\[
P^{2N_0} \begin{bmatrix} x \\ y \end{bmatrix} = A^{2N_0} \begin{bmatrix} x \\ y \end{bmatrix} + B \begin{bmatrix} e \\ f \end{bmatrix} + \begin{bmatrix} e \\ f \end{bmatrix}
\]

(18)

\[
= A^{N_0} \begin{bmatrix} x \\ y \end{bmatrix} + 2B \begin{bmatrix} e \\ f \end{bmatrix} = \begin{bmatrix} x \\ y \end{bmatrix} + 2B \begin{bmatrix} e \\ f \end{bmatrix}
\]

(19)

in a similar way, for \( \forall k \in \mathbb{Z} \), there is

\[
P^{kn_0} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x \\ y \end{bmatrix} + kB \begin{bmatrix} e \\ f \end{bmatrix}
\]

(20)
\[ B \begin{pmatrix} e \\ f \end{pmatrix} = \begin{pmatrix} e' \\ f' \end{pmatrix} \]  \hspace{1cm} (21)

Keeps \( \min\{\gcd(e',N), \gcd(f',N)\} = k' \). then when \( k^0 = N/k' \), \( k_0 B \begin{pmatrix} e \\ f \end{pmatrix} = \begin{pmatrix} k_0 e' \\ k_0 f' \end{pmatrix} \mod N = 0 \),

Thus \( N_0 k_0 \) is one of the P's periods.

Let's prove \( N_0 k_0 \) is P's minimum period.

Assumes the minimum period of P is \( T=N_1 K_1 \), then

\[
\begin{pmatrix} x \\ y \end{pmatrix} = p^T \begin{pmatrix} x \\ y \end{pmatrix} + (A^{T-1} + A^{T-2} + \cdots + A + I) \begin{pmatrix} e \\ d \end{pmatrix}, \hspace{0.5cm} \forall x, y \in \{1,2,\ldots,N\}
\]

Since \( x, y \) is random, it should be

\[ A^T = I \mod N, \]  \hspace{1cm} (22)

\[ (A^{T-1} + A^{T-2} + \cdots + A + I) \begin{pmatrix} e \\ f \end{pmatrix} = 0 \mod N \]

Keeps \( T=N_0 K_0 \), and then there is

\[ [A^{T-1} + A^{T-2} + \cdots + A + I] \begin{pmatrix} e \\ f \end{pmatrix} = k_1 [A^{N_0-1} + \cdots + A + I] \begin{pmatrix} e \\ d \end{pmatrix} = k_1 \begin{pmatrix} e'_1 \\ f'_1 \end{pmatrix} = 0 \]

so, \( k_1 \geq k_0 \), hence \( T \geq N_0 K_0 \). Namely \( N_0 K_0 \) is P's minimum period. Especially if there is reverse for A-I, \( B=0 \mod N \), now, P's period equals to A's period. When A –I is reversible, \( B=0 \mod N \).

Because

\[ (A^{T-1} + A^{T-2} + \cdots + A + I)(A - I) = (I + A^{T-1} + \cdots + A^2 + A) - (A^{T-1} + A^{T-2} + \cdots + A + I) = 0 \]

hence, when \( (A-I) \mod N \) is reversible, there must be

\[ \sum_{i=0}^{T-1} A^i = 0 \]

In this case, P’s period is A’s period.

If \( (A-I) \) is not reversible, then, for

\[ B \begin{pmatrix} e \\ f \end{pmatrix} = \begin{pmatrix} e' \\ f' \end{pmatrix} \]

\( e', f' \) must be even numbers.

P’ period is the multiplier of \( 3 \times 2^{2e-2} \). When \( e=8 \), P’s period is the multiplier of \( 3 \times 2^{14} \). for the affine transformation given by formulation (10), when \( N=2^8 \), since \( N_0=384 \), \( (1) -I \) is reversible,
hence the period of $T$ defined by formulation (10) is 384.

4. Rapid calculation method of transformation

For affine transformation (11), there is following relational expression

$$ P^{T_1+T_2} \begin{bmatrix} X \\ Y \end{bmatrix} = A^{T_1+T_2} \begin{bmatrix} X \\ Y \end{bmatrix} + A^{T_1} \begin{bmatrix} e_2 \\ f_2 \end{bmatrix} + \begin{bmatrix} e_1 \\ f_1 \end{bmatrix}, $$

of which, $\begin{bmatrix} e_2 \\ f_2 \end{bmatrix}$, $\begin{bmatrix} e_1 \\ f_1 \end{bmatrix}$ satisfies

$$ P^{T_1} \begin{bmatrix} x \\ y \end{bmatrix} = A^{T_1} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} e_1 \\ f_1 \end{bmatrix}, $$

$$ P^{T_2} \begin{bmatrix} x \\ y \end{bmatrix} = A^{T_2} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} e_2 \\ f_2 \end{bmatrix}. $$

For Aronld transformation, arrangement transformation and Fibonacci transformation, when one of the $A$’s periods is known, reverse calculation of $A$ can be done within one step. Assumes that one of the transformation periods is $N_0$, $A^{-1}$ can be obtained by pre-calculating $A^{N_0-1}$. For the calculation of $A^{N_0-1}$, the method is as follows:

$$ N_0 - 1 = \sum_{i=0}^{j} a_i, a_i = 0, 1 \quad (\text{Assumes}) $$

Let $T_0 = A, \ldots , T_i = T_{i-1}, \ldots , T_i = T_{i-2}^{2^{-2}}$.

Then

$$ A^{N_0-1} = \prod_{i=0}^{N_0-1} T_i. $$

For instance: during image treatment, when the pixel number of the image height and width is 256, $t \leq 7$. So the calculation of $A^{N_0-1}$ is fairly easy. During decryption, $A^{N_0-1}$ is directly employed in cryptograph image, it is not necessary to continuously function $N_0-1$ times by using $A$. In a similar way, when affine transformation (11) is used, $P^{N_0-1}$ can be pre-calculated, at this time $N_0$ is $P$’s period.

5. Conclusion

In this thesis, we talked about the period problem of Aronld transformation, arrangement transformation, Fibonacci transformation and affine transformation as well the fast calculation method of transformation, especially the reverse calculation for various transformations can be completed by only one step, these results not only has the great usage to image restore, but also
effectively reduces the computational complexity during image restore. For practical application, assumes $N=2^e$.

References

Shaochuan Fu, male, Ph. D. Post Ph. D of Xian jiaotong University. Associate professor of Beijing Jiaotong University. Communication Address: the economy and management school, Beijing Jiaotong University, China. Post Code: 100044. Tel: 010-51686725, 13811554779. E-mail: fushaochuan@263.net

Chengxian Xu, male, professor of xian Jiaotong University. Communication Address: the Science school, Xian Jiaotong University, China. Post Code: 710049. Tel: 029-2668744