Mathematical Problems of Computer Science 30, 54--59, 2008.

On an Image Scrambling Method via Fibonacci and Lucas Numbers

Hakob Sarukhanyan, Grigor Petrosyan
Institute for Informatics and Automation Problems of NAS of RA,
hakop@ipia.sci.am

Abstract

The novel digital image scrambling method based on Fibonacci and Lucas numbers is presented. This scrambling transformation has the following advantages: (a) Encoding and decoding are very simple and can by realized in real-time situations. (b) The scrambling effect is very good, the pixels of the image are re-distributed randomly across the whole image. (c) The method can endure common image attacks, such as compression, noise and loss of data packet.

1. Some Properties of Fibonacci and Lucas numbers

The integer sequence 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, ... is called the Fibonacci sequence. It has fascinated both amateurs and professional mathematicians for centuries, and they continue to charm us with their beauty, their abundant applications, and their ubiquitous habit of occurring in totally surprising and unrelated places [1]. Fibonacci numbers can be presented recursively as follows:

$$F_n = F_{n-1} + F_{n-2}, \quad F_1 = F_2 = 1, \quad n = 3,4,... \tag{1}$$

Lucas numbers is given by

$$L_n = L_{n-1} + L_{n-2}, \quad F_1 = 1, L_2 = 3, \quad n = 3,4,... \tag{2}$$

The first ten Lucas numbers are: 1, 3, 4, 7, 11, 18, 29, 47, 76, 123. An important property of Fibonacci sequence is that the ratio of any number to its previous number will eventually lead us to a limit known as the Golden Mean α (1.61804...). Other number, on the other side of 1, known to exhibit similar kind of properties is called the conjugate Golden Mean α^{-1} (0.61804...). Further we define golden mean and outlist some properties of these parameters.

$$\alpha = \tfrac{1+\sqrt{5}}{2}, \quad \alpha^{-1} = -\tfrac{1-\sqrt{5}}{2}. \tag{3}$$

We can check that

$$\begin{array}{lll}
\alpha^1 = \alpha, & \alpha^{-1} = \alpha^{-1}, & \alpha^{-1} = -1+\alpha; \\
\alpha^2 = 1+\alpha, & \alpha^{-2} = 1-\alpha^{-1}, & \alpha^{-2} = 2-\alpha; \\
\alpha^3 = 1+2\alpha, & \alpha^{-3} = -1+2\alpha^{-1}, & \alpha^{-3} = -3+2\alpha; \\
\alpha^4 = 2+3\alpha, & \alpha^{-4} = 2-3\alpha^{-1}, & \alpha^{-4} = 5-3\alpha; \\
\alpha^5 = 3+5\alpha, & \alpha^{-5} = -3+5\alpha^{-1}, & \alpha^{-5} = -8+5\alpha; \\
\alpha^6 = 5+8\alpha, & \alpha^{-6} = 5-8\alpha^{-1}, & \alpha^{-6} = 13-8\alpha.
\end{array} \tag{4}$$

Or more general

$$\alpha^n = F_{n-1} + \alpha F_n,$$
$$\alpha^{-n} = (-1)^n \left[F_{n-1} - \alpha^{-1} F_n\right] \quad n \geq 2. \tag{5}$$

Using the golden mean Lucas numbers can be presented as follows

$$L_n = \alpha^n + (-1)^n \alpha^{-n}, \quad n \geq 2. \tag{6}$$

Now using equations (5) the Lucas numbers represent as

$$L_n = 2F_{n-1} + F_n = F_{n-1} + F_{n+1}. \tag{7}$$

Fibonacci and Lucas numbers also satisfy the following equalities:

$$F_{n-1}F_{n+1} - F_n^2 = (-1)^n,$$
$$L_{n-1}L_{n+1} - L_n^2 = 5(-1)^{n-1}, \quad n \geq 2. \tag{8}$$

Before we give the definitions of Fibonacci and Lucas scrambling transformation, we need the following theorem.

Theorem 1: [1]. If P and Q are relatively prime integers, then the sequence of integers $s_k = kP(\text{mod } Q)$, $k = 0,1,2,\ldots,Q-1$ is the permutation of $\{0,1,2,\ldots,Q-1\}$.

From (8) it follows that for $m \geq 1$ the following relations take place:

$$\begin{aligned} &(a) \quad F_{2m}^2 + 1 = F_{2m-1}F_{2m+1}, \\ &\qquad F_{2m+1}^2 - 1 = F_{2m}F_{2m+2}; \\ &(b) \quad L_{2m}^2 - 5 = L_{2m-1}L_{2m+1}, \\ &\qquad L_{2m+1}^2 + 5 = L_{2m}L_{2m+2}. \end{aligned} \tag{9}$$

From relations (9) we can deduce the following corollary

Corollary 1. (a) $F_{2m+1}^2 - 1$ can be divided by F_{2m+2} and by F_{2m}; (b) $F_{2m}^2 + 1$ can be divided by F_{2m-1} and by F_{2m+1}; (c) $L_{2m}^2 - 5$ can be divided by L_{2m-1} and by L_{2m+1}; (d) $L_{2m+1}^2 + 5$ can be divided by L_{2m} and by L_{2m+2}.

2. Fibonacci and Lucas Transformations

It is evident that the adjacent pairs of Fibonacci and Lucas numbers are relatively prime numbers. Now we define the Fibonacci and Lucas transformation.

Definition 1. Let (F_n, F_{n+1}) and (L_n, L_{n+1}) be the adjacent pairs of Fibonacci and Lucas numbers, respectively. Then we call the Fibonacci and Lucas scrambling transformations the following transformations, respectively

$$\begin{aligned} &f_n : k \to f_n(k) = kF_n (\text{mod } F_{n+1}), \quad k = 0,1,2,\ldots,F_{n+1} - 1, \\ &l_n : k \to l_n(k) = kL_n (\text{mod } L_{n+1}), \quad k = 0,1,2,\ldots,L_{n+1} - 1. \end{aligned} \tag{10}$$

Above given transforms the input sequences $\{0,1,2,\ldots,F_{n+1}-1\}$ and $\{0,1,2,\ldots,L_{n+1}-1\}$ are transformed to other sequences $\{f_n(0), f_n(1),\ldots,f_n(F_{n+1} \quad 1)\}$ and $\{l_n(0), l_n(1),\ldots,l_n(L_{n+1} \quad 1)\}$, respectively, which are called the pseudo-random permutation of input sequences. These sequences pass one important and relevant property to our applications: they are uniform sequences. They have also some other tests for our applications: they are inexpensive to compute, they are easy to remember, to program, and to analyze.

The "uniformity" for two-dimensional case means that each of the horizontal and vertical directions has uniformity under the distance of pixels coordinates of digital image, defined as follows. Let (x_1, y_1) and (x_2, y_2) be two points, then the distance between them is defined by

$$dist[(x_1, y_1), (x_2, y_2)] = \max\{|x_1 - x_2|, |y_1 - y_2|\}$$

Let $f_n(k) = kF_n \pmod{F_{n+1}}$ then it can be shown that for any $k = 0,1,2,\ldots, F_{n+1} - 1$, take place the following relations [2]:

$$\begin{aligned}
&|f_n(k+1) - f_n(k)| = F_{n-1} \quad or \quad F_n,\\
&|f_n(k+2) - f_n(k)| = F_{n-2} \quad or \quad 2F_{n-1},\\
&|f_n(k+3) - f_n(k)| = F_{n-3} \quad or \quad F_{n-1} - F_{n-3},\\
&|f_n(k+4) - f_n(k)| = F_{n-1} + F_{n-3} \quad or \quad F_n - F_{n-3},\\
&|f_n(k+F_{n-1}) - f_n(k)| = 1.
\end{aligned} \tag{11}$$

The last relation of (11) shows that F_{n-1} is the smallest distance that numbers at random the sequences mapped as neighbors.

Example 1. For n=7 Fibonacci transform $f_7(k) = 13k \pmod{21}$ for $k = \overline{1,20}$ gives the following sequence {13, 5,18,10, 2,15,7,20,12,4,17,9,1,14,6,19,11,3,16, 8}. We can see that for this sequence the relations (11), i.e.

$$|f_7(k+1) - f_7(k)| = \begin{cases} F_6 = 8 & for \quad k = 1,3,4,6,8,9,11,12,14,16,17,19,20, \\ F_7 = 13 & for \quad k = 2,5,7,10,13,15,18; \end{cases}$$

$$|f_7(k+2) - f_7(k)| = \begin{cases} F_5 = 5 & for \quad k = 1,2,4,5,6,7,9,10,12,13,14,15,17,18, \\ 2F_6 = 16 & for \quad k = 3,8,11,16,19; \end{cases}$$

$$|f_7(k+3) - f_7(k)| = \begin{cases} F_4 = 3 & for \quad k = 1,2,3,4,6,7,8,9,10,11,12,14,15,16,17,18, \\ F_8 - F_4 = 18 & for \quad k = 5,13; \end{cases}$$

$$|f_7(k+4) - f_7(k)| = \begin{cases} F_6 + F_4 = 11 & for \quad k = 1,3,6,8,9,11,14,16,17, \\ F_7 - F_4 = 10 & for \quad k = 2,4,5,7,10,12,13,15; \end{cases}$$

$$|f_7(k+8) - f_7(k)| = 1.$$

are really satisfied.

The Fibonacci transform of input sequences of lengths 4, 7, 12, and 20 are given in the following table

0

Fib. Transform	Resulting sequence
$f_4(k) = 3k \pmod 5$	3, 1, 4, 2
$f_5(k) = 5k \pmod 8$	5, 2, 7, 4, 1, 6, 3
$f_6(k) = 8k \pmod{13}$	8, 3, 11, 6, 1, 9, 4, 12, 7, 2, 10, 5
$f_7(k) = 13k \pmod{21}$	13, 5, 18, 10, 2, 15, 7, 20, 12, 4, 17, 9, 1, 14, 6, 19, 11, 3, 16, 8

Now consider the Lucas transform. Let $l_n(k) = kL_n \pmod{L_{n+1}}$, then, as in the case of Fibonacci transform, we can show that for any $k = 0,1,2,\ldots, L_{n+1} - 1$, the following relations take place [3]:

$$
\begin{aligned}
&|l_n(k+1)-l_n(k)| = L_{n-1} \quad or \quad L_n,\\
&|l_n(k+2)-l_n(k)| = L_{n-2} \quad or \quad 2L_{n-1},\\
&|l_n(k+3)-l_n(k)| = L_{n-3} \quad or \quad L_{n+1}-L_{n-3},\\
&|l_n(k+4)-l_n(k)| = L_{n-1}+L_{n-3} \quad or \quad L_n \quad L_{n-3}.
\end{aligned} \tag{12}
$$

Example 2. For n=5 Lucas transform $l_5(k) = 11k \pmod{18}$ for $k = \overline{1,17}$ gives the following sequence {11, 4,15,8,1,12,5,16,9,2,13,6,17,10,3,14,7}. We can see that for this sequence the relations (12), i.e.

$$
|l_5(k+1)-l_5(k)| = \begin{cases} L_4 = 7 & for \quad k = 1,3,4,6,8,9,11,13,14,16, \\ L_5 = 11, & for \quad k = 2,5,7,10,12,15; \end{cases}
$$

$$
|l_5(k+2)-l_5(k)| = \begin{cases} L_3 = 4 & for \quad k = 1,2,3,4,\ 5,6,7,9,10,11,12,14,15, \\ 2L_4 = 14, & for \quad k = 3,8,13; \end{cases}
$$

$$
|l_5(k+3)-l_5(k)| = \begin{cases} L_2 = 3 & for \quad k = 1,2,3,4,\ 6,7,8,9,11,12,14, \\ L_6 - L_2 = 15, & for \quad k = 5,10; \end{cases}
$$

$$
|l_5(k+4)-l_5(k)| = \begin{cases} L_4 + L_2 = 10 & for \quad k = 1,2,6,8,11,13, \\ L_5 - L_2 = 8, & for \quad k = 2,4,5,7,9,10,12; \end{cases}
$$

are really satisfied.

The Lucas transform of input sequences of lengths 6, 10, 17, and 28 are given in the following table

Lucas Transform	Resulting sequence
$l_3(k) = 4k \pmod 7$	4, 1, 5, 2, 6, 3
$l_4(k) = 7k \pmod{11}$	7, 3, 10, 6, 2, 9, 5, 1, 8, 4
$l_5(k) = 11k \pmod{18}$	11, 4, 15, 8, 1, 12, 5, 16, 9, 2, 13, 6, 17, 10, 3, 14, 7
$l_6(k) = 18k \pmod{29}$	18,7,25,14,3,21,10,28,17,6,24,13,2,20,9,27,16,5,23,12,1,19,8,26,15,4,22,11

3. The Periodicity of Fibonacci and Lucas Transforms

Definition 2. The number T is called the period of the Fibonacci (Lucas) transform f_n (l_n) (see equation (10)), if for each $k \in \overline{\{1, F_{n+1}-1\}}$ ($k \in \overline{\{1, L_{n+1}-1\}}$),

$$
f_n^T(k) = k \quad (l_n^T(k) = k), \tag{13}
$$

where T is the smallest positive integer that satisfies this condition.

From (10) we have

$$
\begin{aligned}
f_n^T(k) &= f_n^{T-1}(f_n(k)) = f_n^{T-1}(kF_n \pmod{F_{n+1}}) = kF_n^T \pmod{F_{n+1}},\\
l_n^T(k) &= l_n^{T-1}(l_n(k)) = l_n^{T-1}(kL_n \pmod{L_{n+1}}) = kL_n^T \pmod{L_{n+1}},
\end{aligned} \tag{14}
$$

Now we can formulate the following theorem.

Theorem 2. The period of the Fibonacci and Lucas transform is the smallest positive integer T_n satisfying the condition that F_{n+1} divides $F_n^{T_n}-1$ and that L_{n+1} divides $L_n^{T_n}-1$, respectively, i.e. $(F_n^{T_n}-1) \bmod F_{n+1} = 0$ and $(L_n^{T_n}-1) \bmod L_{n+1} = 0$.

The periodicity of Fibonacci transform can be determined from the relations (9). Thus, from $F_{2m+1}^2 - 1 = F_{2m}F_{2m+2}$ we obtain $(F_{2m+1}^2 - 1) \bmod F_{2m+2} = 0$, which means that Fibonacci transform of sequence with length $F_{2m+2} - 1$ for any $m = 1,2,\ldots$ has the period 2.

From the relations (9) we also find $F_{2m}^4 - 1 = F_{2m-1}F_{2m+1}(F_{2m-1}F_{2m+1} - 2)$. That means that Fibonacci transform of sequence with length F_{2m} for any $m = 1,2,\ldots$ has the period 4.

The periods of Lucas transformation we found by computer simulation. In the below table some periods of Lucas transform are given

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
L_n	1	3	4	7	11	18	29	47	76	123	199	322	521	843	1364	2207
T_n	1	2	3	10	6	28	46	18	4	33	66	20	280	30	1103	3570

4. 2D Fibonacci and Lucas Transforms

Two dimensional Fibonacci and Lucas scrambling transformations can be defined as

$$f_{n,m}(i,j) = (iF_n (\bmod F_{n+1}), jF_m (\bmod F_{m+1})), \quad i = \overline{0, F_{n+1} - 1}, \quad j = \overline{0, F_{m+1} - 1}, \tag{15}$$

$$l_{n,m}(i,j) = (iL_n (\bmod L_{n+1}), jL_m (\bmod L_{m+1})), \quad i = \overline{0, L_{n+1} - 1}, \quad j = \overline{0, L_{m+1} - 1}.$$

In other word, 2D Fibonacci (Lucas) transform can be realized by two stages: at first we must apply the 1D transform to all rows of a given image, then we apply the same transform to all columns of image obtained in the first stage.

Introduce the following notation. FibRow(A) is the Fibonacci transformation of all rows of matrix A, FibCol(A) is the Fibonacci transformation of all columns of matrix A, and FibRowCol(A) means the 2D Fibonacci transformation of A.

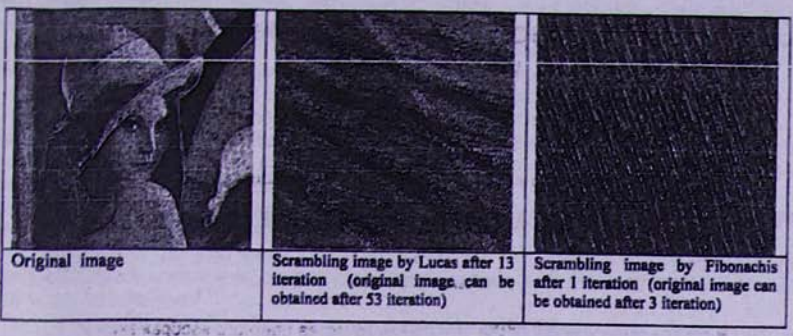
Now let $A = (a_{ij})$ be the input image of size 8×8. For this image 2D Fibonacci transformation has the form $f_{5,5}(i,j) = (5i (\bmod 8), 5j (\bmod 8)), \quad i,j = \overline{0,7}$. Using above given notations we obtain

$$B = FibRow(A) = \begin{bmatrix} 00 & 05 & 02 & 07 & 04 & 01 & 06 & 03 \\ 10 & 15 & 12 & 17 & 14 & 11 & 16 & 13 \\ 20 & 25 & 22 & 27 & 24 & 21 & 26 & 23 \\ 30 & 35 & 32 & 37 & 34 & 31 & 36 & 33 \\ 40 & 45 & 42 & 47 & 44 & 41 & 46 & 43 \\ 50 & 55 & 52 & 57 & 54 & 51 & 56 & 53 \\ 60 & 65 & 62 & 67 & 64 & 61 & 66 & 63 \\ 70 & 75 & 72 & 77 & 74 & 71 & 76 & 73 \end{bmatrix} \quad FibCol(B) = \begin{bmatrix} 00 & 05 & 02 & 07 & 04 & 01 & 06 & 03 \\ 50 & 55 & 52 & 57 & 54 & 51 & 56 & 53 \\ 20 & 25 & 22 & 27 & 24 & 21 & 26 & 23 \\ 70 & 75 & 72 & 77 & 74 & 71 & 76 & 73 \\ 40 & 45 & 42 & 47 & 44 & 41 & 46 & 43 \\ 10 & 15 & 12 & 17 & 14 & 11 & 16 & 13 \\ 60 & 65 & 62 & 67 & 64 & 61 & 66 & 63 \\ 30 & 35 & 32 & 37 & 34 & 31 & 36 & 33 \end{bmatrix}$$

5. Experimental Results

In the presented above paragraphs we have seen that Fibonacci's and Lucas transforms have a periodicity. Also we have seen that those transforms can be used in scrambling algorithms. We can use those properties for mixing the indexes of image pixels, otherwise stated we can randomly choose the set of mixed indexes and change the places of pixel values. This algorithm gives to the bitmap some properties of protection as we have to try at least T (where the T is the periodicity of Lucas and Fibonacci's functions) set of indexes for recovering the original image. Hence, we can see that the amount of protection directly depends on periodicity of Lucas and

Fibonacci's functions. The bitmaps presented bellow show the experimental results of implementation of Lucas and Fibonacci's transforms in image **Lena.bmp** of size 198x198.



Original image	Scrambling image by Lucas after 13 iteration (original image can be obtained after 53 iteration)	Scrambling image by Fibonachis after 1 iteration (original image can be obtained after 3 iteration)

This work has been partially fulfilled owing to the ISTC Grant (Project A-1451).

References

[1] G. E. Bergum et al (eds.) Applications of Fibonacci Numbers. Vol. 4, 1991.

[2] J. Zou, R. K. Ward, D. Qi. A New Digital Image Scrambling Method Based on Fibonacci Numbers. IEEE, 2004.

[3] J. Zou, R. K. Ward, D. Qi. The Generalized Fibonacci Transforms and Application to Image Scrambling. Proc. ICASSP 2004, pp. 385-388.

Ֆիբոնաչիի և Լուկասի թվերի միջոցով պատկերների տարրերի տեղափոխությունների մի մեթոդի մասին

Հ. Սարուխանյան, Գ.Պետրոսյան

Ամփոփում

Հոդվածում ներկայացված է Ֆիբոնաչիի և Լուկասի թվերի օգնությամբ թվային պատկերների տարրերի տեղափոխությունների մեթոդ: Ներկայացված ձևափոխությունները ա/ բավականաչափ պարզ են և իրականացնելի են իրական ժամանակում, բ/ պատկերների տարրերը վերաբաշխվում են ողջ պատկերով համարյա պատահական, գ/ կարելի է կիրառել նաև որոշակի տեղեկություններ թաքցնելու նպատակով: