رمزگذاری تصویر با استفاده از دنباله های t-پیل و تعمیم آن

منصور هاشمی[۱]، الهه مهربان[۲]، محمد جواد بذرافشان دلیجانی [۳,*]

۱- دانشیار دانشکده علوم ریاضی، دانشگاه گیلان ، گیلان، رشت

۲- دکتری ریاضی محض، دانشکده ریاضی، دانشگاه گیلان ، گیلان، رشت

۳- کارشناسی ارشد مهندسی برق مخابرات(رمز)، دانشگاه شهید ستاری ، تهران

چکیده

امنیت و محرمانه بودن در سطوح مختلف ارتباط مانند هنگام برقراری ارتباط محرمانه داده های شخصی ، داده های پزشکی ، اطلاعات دفاعی و غیره همواره مورد توجه بوده است. در این مقاله ما دو مدل رمزگذاری تصویر بر اساس دنباله t-پیل و فیبوناتچی را پیشنهاد می کنیم.

کلمات کلیدی: تصویر دیجیتال، دنباله t-پیل، دنباله فیبوناتچی، ماتریس، دوره تناوب.

۱- مقدمه

با توجه به نیاز جامعه به امنیت و محرمانه بودن داده ها ، روش های مختلفی برای این کار وجود دارد. یکی از این روش ها درهم آمیزی تصویر است. در طول چهار دهه اخیر به عنوان استانداردهای رمزنگاری محبوب ظاهر شده است. ابتدایی ترین این روش توسط ولادیمیر آرنولد (Vladimir Arnold)در سال ۱۹۶۰ ارایه شد. که به شرح زیر است:

$\tau : T^2 \to T^2$، تبدیل آرنولد نامیده می شود اگر

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \pmod N, \qquad (1)$$

که $x, y \in \{0,1,\cdots, N-1\}$ و N سایز تصویر دیجیتال است.

تصویر جدید وقتی پدید می آید که همه نقاط به وسیله (۱) منتقل شده باشند. برای مطالعه بیشتر به [1] و [2] مراجعه نمایید.این تبدیل ساده اما قدرتمند است که ماهیت تناوبی دارد و برای برنامه های کاربردی از جمله پنهانگاری مفید است. فرض کنید p دوره تناوب تبدیل یک تصویر دیجیتال l، NxN باشد. اعمال (۱) برای تکرار تصادفی t بار که $t \in [1, p]$، یک تصویر در هم ریخته l' به دست می آید که کاملا آشفته است وبا l متفاوت است. کانال های ارتباطی بدون افشای هیچ اطلاعاتی به گیرنده یا شنودهای غیرمجاز در انتهای دریافت این فرآیند برای $p-t$ بار تکرار می شود تصویر اصلی به دست می آید. توجه داشته باشید می توانیم این تبدیل از یک بار به n بار تعمیم دهیم که $p-n \pmod N$ را برابر با تبدیل آرنولد انجام دهیم.

در سال ۲۰۰۴، الگوریتم تبدیل آرنولد را گسترش داد([3]). Hong و همکاران در [4]، آرنولد دو بعدی را به سه بعدی گسترش داداند همچنین دوره تناوب تبدیل آرنولد (AT) را مورد مطالعه قرار دادند. Wang در مقاله خود مطالعه ای روی دوره تبدیل ماتریس تصادفی دو بعدی انجام داد و از آن برای پنهان کردن تصویر استفاده کرد([5]). در [6]روش فوق را بصورت زیر گسترش دادند و دوره تناوب را برای بهبود امنیت در هم تعمیم دادند.

* **Email: javadomhdnd@gmail.com**

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} k+1 & k \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \pmod N, \qquad (2)$$

یا

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} k & k+1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \pmod N, \qquad (3)$$

که $x, y \in \{0,1,\cdots, N-1\}$ ، $k \geq 0$ و N سایز تصویر دیجیتال است.

همان طور که مشاهده می شود در هر مورد دو ماتریس $2x2$ و دوره تناوب دارند. تصویر مربعی را در قالبی غیرقابل تشخیص در هم می ریزند. برخلاف (۱) که نقشه واحد وجود دارد در (۲) و (۳) تعدادی نقشه برای مقادیر مختلف k وجود دارد. از این رو سطح امنیتی پیام درهم شده را در برابر رمزگشایی ضربه ای و آزمایشی افزایش می دهد. توجه داشته باشید به ازای $k=1$ تساوی (۲) همان (۱) است.

در [7]، تعمیمی از تبدیل فیبوناتچی مورد بررسی شد. در این مقاله، با استفاده از ماتریس دنباله های t-پیل ، رمزگذاری تصویر مورد بررسی قرار می دهیم.

۲- دنباله های t-پیل و برخی خواص آن

به ازای $t \geq 2$، دنباله عددی t-پیل که آن را p_n^t نشان می دهیم بصورت

$$p_n^t = tp_{n-1}^t + p_{n-2}^t, \quad n \geq 0,$$

با شرایط اولیه $p_0^t = 0$ ، $p_1^t = 1$ تعریف می شود. بعنوان مثال، داریم:

$$t=3, \quad p_n^3 = 3p_{n-1}^3 + p_{n-2}^3 = \{0,1,3,10,\cdots\},$$

$$t=5, \quad p_n^5 = 5p_{n-1}^5 + p_{n-2}^5 = \{0,1,5,26,\cdots\}.$$

لم ۲-۱. ماتریس دنباله عددی t-پیل را که با $Q\left(t, p_n^t\right)$ نشان می دهیم و با استقرا می توان ثابت کرد

$$Q\left(t, p_n^t\right) = \begin{bmatrix} p_{n+1}^t & p_n^t \\ p_n^t & p_{n-1}^t \end{bmatrix}.$$

در جدول ۱ برخی مقادیر $1 \leq n \leq 10$ را به ازای $t \in \{2,3,4\}$ و $1 \leq i \leq 10$ را بدست آمده است.

جدول ۱. $Q\left(t, p_i^t\right)$ به ازای $t \in \{2,3,4\}$ و $1 \leq i \leq 10$

i	$Q(2, p_i^2)$	$Q(3, p_i^3)$	$Q(4, p_i^4)$
1	$\begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 3 & 1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 4 & 1 \\ 1 & 0 \end{bmatrix}$
2	$\begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix}$	$\begin{bmatrix} 10 & 3 \\ 3 & 1 \end{bmatrix}$	$\begin{bmatrix} 17 & 4 \\ 4 & 1 \end{bmatrix}$

3	$\begin{bmatrix}12 & 5\\5 & 2\end{bmatrix}$	$\begin{bmatrix}33 & 10\\10 & 3\end{bmatrix}$	$\begin{bmatrix}72 & 17\\17 & 4\end{bmatrix}$
4	$\begin{bmatrix}29 & 12\\12 & 5\end{bmatrix}$	$\begin{bmatrix}109 & 33\\33 & 10\end{bmatrix}$	$\begin{bmatrix}305 & 72\\72 & 17\end{bmatrix}$
5	$\begin{bmatrix}70 & 29\\29 & 12\end{bmatrix}$	$\begin{bmatrix}360 & 109\\109 & 33\end{bmatrix}$	$\begin{bmatrix}1292 & 305\\305 & 72\end{bmatrix}$
6	$\begin{bmatrix}169 & 70\\70 & 29\end{bmatrix}$	$\begin{bmatrix}1189 & 360\\360 & 109\end{bmatrix}$	$\begin{bmatrix}5473 & 1292\\1292 & 305\end{bmatrix}$
7	$\begin{bmatrix}408 & 169\\169 & 70\end{bmatrix}$	$\begin{bmatrix}3927 & 1189\\1189 & 360\end{bmatrix}$	$\begin{bmatrix}23184 & 5473\\5473 & 1292\end{bmatrix}$
8	$\begin{bmatrix}985 & 408\\408 & 169\end{bmatrix}$	$\begin{bmatrix}12970 & 3927\\3927 & 1189\end{bmatrix}$	$\begin{bmatrix}98209 & 23184\\23184 & 5473\end{bmatrix}$
9	$\begin{bmatrix}2375 & 985\\985 & 408\end{bmatrix}$	$\begin{bmatrix}42837 & 12970\\12970 & 3927\end{bmatrix}$	$\begin{bmatrix}416020 & 98209\\98209 & 23184\end{bmatrix}$
10	$\begin{bmatrix}5741 & 2375\\2375 & 985\end{bmatrix}$	$\begin{bmatrix}141481 & 42837\\42837 & 12970\end{bmatrix}$	$\begin{bmatrix}1762289 & 416020\\416020 & 98209\end{bmatrix}$

لم۲-۲. دترمینان $Q\left(t,p_n^t\right)$ برابر با $(-1)^n$است.

برهان. به [8]مراجعه نمایید.

اعضای دنباله فیبوناتچی که آن را با f_n نشان می دهندبصورت

$$f_n = f_{n-1} + f_{n-2}, \quad n \geq 0,$$

با شرایط اولیه $f_0 = 0, \quad f_1 = 1$ تعریف می شود.

اینک با توجه به تعریف فیبوناتچی میتوان ماتریس فیبوناتچی - t-پیل را بصورت زیر تعریف می کنیم.

تعریف۲-۳. ماتریس دنباله فیبوناتچی - t-پیل را با $FQ\left(t,p_n^t\right)$ نشان میدهیم و به صورت زیر است:

$$FQ\left(t,p_n^t\right)=\begin{bmatrix}f_n & f_{n+1}\\p_n^t & p_{n+1}^t\end{bmatrix}$$

که f_n اعضای دنباله فیبوناتچی و p_n^t اعضای دنباله - t-پیل است.

بعنوان مثال برای $t=3$و $n=4$، داریم:

$$FQ\left(3,p_4^3\right)=\begin{bmatrix}f_4 & f_5\\p_4^3 & p_5^t\end{bmatrix}=\begin{bmatrix}3 & 5\\33 & 109\end{bmatrix}.$$

اگر $t=2$ در نظر بگیریم ماتریس فیبوناتچی - t-پیل را با $FQ(p_n)$ نشان می دهیم. داریم:

$$FQ(p_1)=\begin{bmatrix} f_1 & f_2 \\ p_1 & p_2 \end{bmatrix}.$$

لم۲-۴. به ازای $m\in\mathbb{N}$، داریم:

$$(FQ\ (p_1))^m=\begin{bmatrix} f_{(2m-1)} & f_{(2m)} \\ f_{(2m)} & f_{(2m+1)} \end{bmatrix}.$$

برهان. با استقرا روی m بدست می آوریم. به ازای $m=1$، داریم:

$$FQ(p_1)=\begin{bmatrix} f_1 & f_2 \\ f_2 & f_3 \end{bmatrix}.$$

فرض استقرا برای $m=k$ برقرار باشد. حکم را برای $m=k+1$ ثابت می کنیم. با توجه به خواص دنباله فیبوناتچی داریم:

$$(FQ\ (p_1))^{k+1}=\begin{bmatrix} f_{(2k-1)} & f_{(2k)} \\ f_{(2k)} & f_{(2k+1)} \end{bmatrix}\begin{bmatrix} f_1 & f_2 \\ f_2 & f_3 \end{bmatrix}=\begin{bmatrix} f_{(2k+1)} & f_{(2k+2)} \\ f_{(2k+2)} & f_{(2k+3)} \end{bmatrix}.$$

حکم ثابت شد.

لم۲-۵. دترمینان $(FQ\ (p_1))^m$ برابر است با ۱.

برهان. با توجه به رابطه $f_{(2k-1)}f_{(2k+1)}-f_{(2k)}{}^2=1$ بدست می آید.

در جدول ۲ به ازای $1\le n\le 30$، مقادیر ماتریس $FQ(p_n)$ بدست می آوریم.

در جدول ۲: به ازای $1\le n\le 30$، مقادیر ماتریس $FQ(p_n)$

n	$FQ(p_n)$	n	$FQ(p_n)$
1	$\begin{bmatrix}1 & 1\\ 1 & 2\end{bmatrix}$	11	$\begin{bmatrix}17711 & 28657\\ 28657 & 46368\end{bmatrix}$
2	$\begin{bmatrix}2 & 3\\ 3 & 5\end{bmatrix}$	12	$\begin{bmatrix}46368 & 75025\\ 75025 & 121393\end{bmatrix}$
3	$\begin{bmatrix}5 & 8\\ 8 & 13\end{bmatrix}$	13	$\begin{bmatrix}121393 & 196418\\ 196418 & 317811\end{bmatrix}$
4	$\begin{bmatrix}13 & 21\\ 21 & 34\end{bmatrix}$	14	$\begin{bmatrix}317811 & 514229\\ 514229 & 832040\end{bmatrix}$
5	$\begin{bmatrix}34 & 55\\ 55 & 89\end{bmatrix}$	15	$\begin{bmatrix}832040 & 1346269\\ 1346269 & 1346269\end{bmatrix}$

6	$\begin{bmatrix} 89 & 144 \\ 144 & 233 \end{bmatrix}$	16	$\begin{bmatrix} 1346269 & 3524578 \\ 3524578 & 5702887 \end{bmatrix}$
7	$\begin{bmatrix} 233 & 377 \\ 377 & 610 \end{bmatrix}$	17	$\begin{bmatrix} 1346269 & 3524578 \\ 3524578 & 5702887 \end{bmatrix}$
8	$\begin{bmatrix} 610 & 1597 \\ 1597 & 2584 \end{bmatrix}$	18	$\begin{bmatrix} 5702887 & 9227465 \\ 9227465 & 14930352 \end{bmatrix}$
9	$\begin{bmatrix} 2584 & 4181 \\ 4181 & 6765 \end{bmatrix}$	19	$\begin{bmatrix} 14930352 & 24157817 \\ 24157817 & 39088169 \end{bmatrix}$
10	$\begin{bmatrix} 6765 & 10946 \\ 10946 & 17711 \end{bmatrix}$	20	$\begin{bmatrix} 39088169 & 63245986 \\ 63245986 & 102334155 \end{bmatrix}$

۳. رمزگذاری تصاویر با تبدیلات ماتریس t-پیل و فیبوناتچی

در اینجا، ابتدا تبدیلات ماتریس های t-پیل و فیبوناتچی را تعریف کرده و سپس دوره تناوب آن ها را بدست می آوریم. در انتها با چند مثال توانایی در هم رمزگذاری را نشان می دهیم.

۳-۱. تبدیل ماتریس های t-پیل

$\tau : T^2 \to T^2$، تبدیل ماتریس های t-پیل نامیده می شود اگر

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} p_{i+1}^t & p_i^t \\ p_i^t & p_{i-1}^t \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \pmod N, \qquad (4)$$

که $x, y \in \{0,1,\cdots, N-1\}$، $i \geq 0$ و N سایز تصویر دیجیتال است.

۳-۲. تبدیل ماتریس فیبوناتچی--پیل

$\tau : T^2 \to T^2$، تبدیل ماتریس فیبوناتچی--پیل نامیده می شود اگر

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} f_{(2i-1)} & f_{(2i)} \\ f_{(2i)} & f_{(2i+1)} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \pmod N, \qquad (5)$$

که $x, y \in \{0,1,\cdots, N-1\}$، $i \geq 1$ و N سایز تصویر دیجیتال است.

۳-۳. دوره تناوب

با توجه به تعریف دوره تناوب یک تبدیل نگاشت می توان در نظر گرفت که p دوره تناوب تبدیل یک تصویر دیجیتال l ، NxN باشد. اعمال (۴) یا (۵) برای تکرار تصادفی t بار که $t \in [1, p]$، یک تصویر در هم ریخته l' به دست می آید که کاملا آشفته است وبا l متفاوت است. دریافت این فرآیند برای $p-t$ بار تکرار می شود تصویر اصلی به دست می آید. توجه داشته باشید می توانیم این تبدیل از یک بار به n بار تعمیم دهیم که $p-n \pmod N$ را برابر با تبدیل

نگاشت مورد نظر خواهد بود. همچنین، دوره تناوب این تبدیلات حداکثر N^2-1 است. در جدول ۳و۴، دوره تناوب برخی از مقادیر ماتریس دنباله t-پیل و فیبوناتچی- پیل برای تصویر دیجیتال384x384 بدست آوردیم.

جدول۳. دوره تناوب تبدیل ماتریس t-پیل برای تصویر دیجیتال 384x384

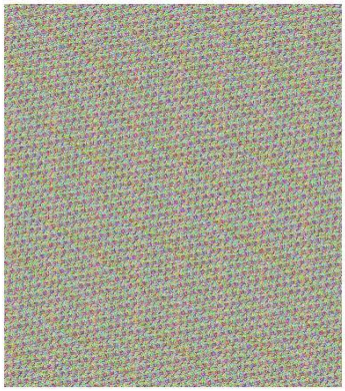
i	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰
$Q(2,p_i^2)$	۱۲۷	۶۳	۱۲۷	۳۱	۱۲۷	۶۳	۱۲۷	۱۵	۱۲۷	۶۳
$Q(3,p_i^3)$	۱۹۱	۹۵	۶۳	۴۷	۱۹۱	۳۱	۱۹۱	۲۳	۶۳	۹۵
$Q(4,p_i^4)$	۶۳	۳۱	۶۳	۱۵	۶۳	۳۱	۶۳	۷	۶۳	۳۱
$Q(5,p_i^5)$	۱۹۱	۹۵	۶۳	۴۷	۱۹۱	۳۱	۱۹۱	۲۳	۶۳	۹۵
$Q(10,p_i^{10})$	۱۲۷	۶۳	۱۲۷	۳۱	۱۲۷	۶۳	۱۲۷	۱۵	۱۲۷	۶۳

جدول۴. دوره تناوب تبدیل ماتریس فیبوناتچی--پیل برای تصویر دیجیتال 384x384

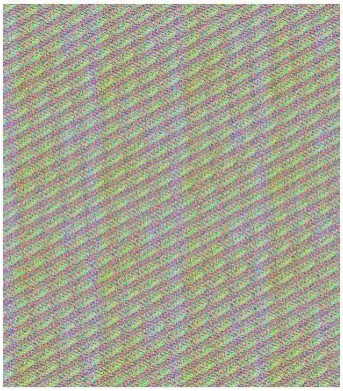
i	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰
$(FQ\ (p_1))^i$	۹۵	۴۷	۳۱	۲۳	۹۵	۱۵	۹۵	۱۱	۳۱	۴۷
i	۱۱	۱۲	۱۳	۱۴	۱۵	۱۶	۱۷	۱۸	۱۹	۲۰
$(FQ\ (p_1))^i$	۹۵	۷	۹۵	۴۷	۳۱	۵	۹۵	۱۵	۹۵	۲۳
i	۲۱	۲۲	۲۳	۲۴	۲۵	۲۶	۲۷	۲۸	۲۹	۳۰
$(FQ\ (p_1))^i$	۳۱	۴۷	۹۵	۳	۹۵	۴۷	۳۱	۲۳	۹۵	۱۵

برای مثال در ادامه، چند تصویر در هم ریخته را به ازای ماتریس ها و دوره تناوب مختلف بدست آوردیم
شکل ۱، تصویر لنا است که آن را با چندین تبدیل نگاشت ماتریسی در نظر گرفته شده به اشکال ۲تا ۵تبدیل شده است. با در نظر گرفتن شکل ۶، و تبدیلات نگاشت شکل های ۷ تا ۱۰ را بدست آوردیم. توجه داشته باشید که تصاویر به دست آمده درهمریختگی بالایی دارند که یکی از کاربردهای آن می تواند در steganographic و watermarking باشد.

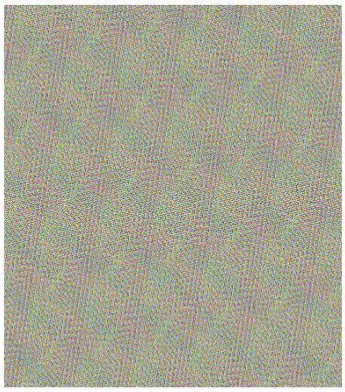
شکل ۱. تصویر اصلی



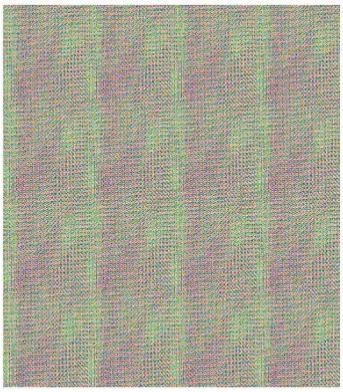
شکل ۲. n=7 و نگاشت ۸۳ برای ماتریس فیبوناتچی



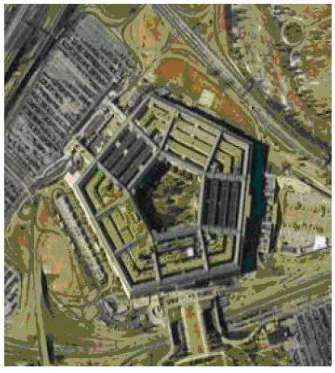
شکل۴. i=7, t=9 نگاشت ۸۳ برای ماتریس پیل



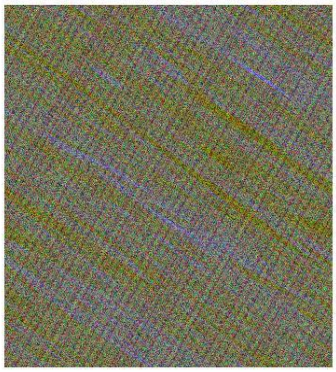
شکل ۳. n=13 و نگاشت 17 برای ماتریس فیبوناتچی



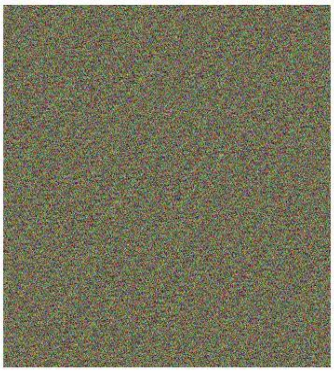
شکل۵. i=13 و t=1 نگاشت 17 برای ماتریس پیل



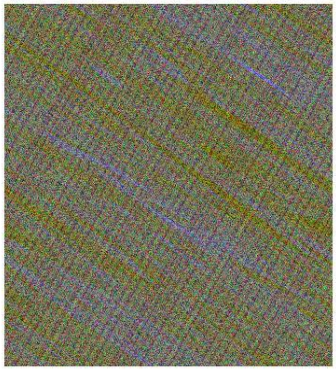
شکل ۶. تصویر اصلی



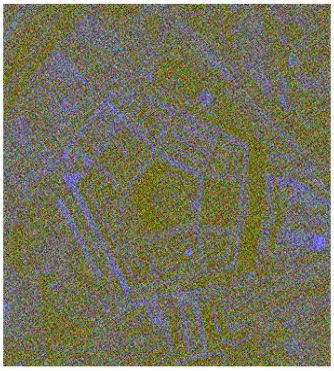
شکل ۷. n=7 و نگاشت ۸۳ برای ماتریس فیبوناتچی



شکل ۹. i=7 و t=7 نگاشت ۸۳ برای ماتریس پیل



شکل ۸. n=13 و نگاشت 17 برای ماتریس فیبوناتچی



شکل ۱۰. i=13 و t=1 نگاشت 17 برای ماتریس پیل

نتیجه گیری:

در این مقاله، دو نوع تبدیل نگاشتی با استفاده از دنباله های t- پیل و فیبوناتچی بدست آوردیم که درهم ریختگی تصاویر قدرتمند است. و می توان از آن در حوزه های تکنیک های مختلف پردازش تصویر و پنهان سازی داده ها و ارتباطات مخفی مانند استگانوگرافی به کار برد و امنیت پیام پنهان را افزایش داد. از دیگر کاربردهای این تبدیلات نگاشتی می توان با توجه به توانایی در هم ریختگی بسیار بالای تصویر، بعنوان کلیدهای قدرتمند به کار برده شود.

اینک، مقاله را با طرح این پرسش ها به پایان می رسانیم.

۱- آیا فرمول یا رابطه مشخصی برای پیداکردن دوره تناوب نگاشت ها ماتریس ها وجود دارد؟

۲- آیا رابطه ای بین دوره تناوب دنباله مورد نظر و دوره تناوب نگاشت ماتریس مورد استفاده از آن دنباله وجود دارد؟

منابع

[۱] V. I. Arnold; A. Avez (1968). Ergodic Problems in Classical Mechanics. New York: Benjamin.
[۲] Ma, Z.G. and S.S. Qiu, 2003. “An image cryptosystem based on general cat map”, J. China Inst.Commun., 24: 51-57.
[3] Kong, T. and Z. Dan, 2004. A new anti-Arnold transform algorithm. J. Software, 15: 1558-1564.
[4] Hong, C.Y. and W.G. Zou, 2005. “Digital image scrambling technology based on three dimensions Arnold transform and its period”, J. Nanchang Univ. Nat. Sci., 29: 619-621.
[5] wang. Z.H., 2006. “On the period of 2D “Random matrix scrambling transform and its application in image hiding”, Chinese J. Comput., 29: 2218-2225.
[6] Minati Mishra, A.R. Routray, Sunit Kumar: “High Security Image Steganography with modified Arnold’s cat map”, IJCA, Vol.37, No.9:16-20, January 2012.
[7] Minati Mishra1, Priyadarsini Mishra**2**, M.C. Adhikary**3** and Sunit Kumar, “IMAGE ENCRYPTION USING FIBONACCI-LUCAS TRANSFORMATION”. International Journal on Cryptography and Information Security (IJCIS),Vol.2, No.3, September 2012.
[8] Hashemi, M., and Mehraban, E. Some New Codes Theory on t- Pell Sequences Matrix.*J. Passive Defence Sci. Technol.*, 1 (2019), 95-106.