دوره دهم، شماره دوم، پاییز و زمستان ۱۳۹۶

مجله فناوری اطلاعات در طراحی مهندسی
Information Technology in Engineering Design
http://ited.sinaweb.net

رمزنگاری امن تصویر مبتنی بر جایگشت سطوح بیت و نگاشت‌های آشوب

ابوالفضل یاقوتی نیت*(۱) متینه زوار (۲)

(۱) آموزشکده فنی و حرفه‌ای سما، دانشگاه آزاد اسلامی، واحد قوچان، قوچان، ایران*
(۲) آموزشکده فنی و حرفه‌ای سما، دانشگاه آزاد اسلامی، واحد قوچان، قوچان، ایران

چکیده

امروزه اکثر ارتباطات بین افراد به صورت تصویری است، به طوری که حفاظت از اطلاعات تصویر، به منظور جلوگیری از دستیابی‌های غیر مجاز مورد نیاز است. این مقاله یک طرح نوین رمزنگاری تصویر مبتنی بر تجزیه سطح بیت و نگاشت آشوب را ارائه می‌دهد. در ابتدا تصویر اصلی به سطوح بیتی مختلف گسسته می‌شود. سپس، سطوح بیتی فرد در یک گروه و سطوح بیتی زوج در گروه دیگر قرار می‌گیرند. با استفاده از نگاشت آرنولد بر روی هر یک از گروه‌ها، جایگشت صورت می‌گیرد. روش پیشنهادی موجب می‌شود که گروهی از بیت‌ها از یک سطح بیتی به سطح بیتی دیگر منتقل گردند. در نتیجه، توزیع بیت در هر سطح بیت بسیار یکنواخت خواهد بود و اطلاعات آماری در هر سطح بیتی از تصویر اصلی تغییر می‌یابد. از این رو، مهاجم نمی‌تواند، هنگامی‌که تصویر جایگشت شده را دریافت کند، اطلاعات آماری تصویر اصلی را تجزیه و تحلیل نماید. از سیستم آشوب سه بعدی لجستیک جهت رمزنگاری بهره گرفته‌ایم. نتایج آزمایشی نشان دهنده‌ی امنیت بالای روش پیشنهادی در برابر حملات مختلف، مانند حملات آماری و از دست دادن داده‌ها است.

واژه‌های کلیدی: تجزیه سطح بیت، رمزنگاری تصویر، نگاشت آرنولد، نگاشت سه بعدی لجستیک

* **عهده‌دار مکاتبات:**
نشانی: آموزشکده فنی و حرفه‌ای سما، دانشگاه آزاد اسلامی، واحد قوچان، قوچان، ایران
تلفن: ۰۹۳۷۰۳۶۹۳۴۹ **پست الکترونیکی:**ayaghouti@gmail.com

۱) مقدمه

امروزه تکنولوژی رایانه تأثیر زیادی بر زندگی روزمره ما دارد. ارتباطات تصویری به یکی از مهمترین ابزار در استفاده از اطلاعات دیجیتال، تبدیل شده است. به طوری که امنیت تصاویر، هنگام انتقال از طریق یک کانال ارتباطی ناامن، مورد نیاز است. برای این منظور، رمزنگاری تصویر به عنوان یک فناوری مهم در رایانه برای برقراری ارتباط امن مطرح شده است [۱,۲]. برخلاف متون، تصاویر دارای ویژگی‌ها و خصوصیات خاصی هستند، به عنوان مثال تصاویر دارای، افزونگی زیاد، ظرفیت بالای داده و همبستگی قوی میان پیکسل‌های مجاور هستند. در نتیجه، بسیاری از روش‌های سنتی رمزنگاری متن برای رمزنگاری اطلاعات تصویر مناسب نیستند [۳,۷,۸]. با توجه به ویژگی‌های خاص توابع آشوب، مانند حساسیت به شرایط اولیه، رفتارهای پیچیده و تصادفی، غیر قابل پیش بینی بودن، طرح‌های رمزنگاری تصویر مبتنی بر آشوب توجه بیشتری را به خود جلب کرده‌اند [۲۰-۱]. یک الگوریتم رمزنگاری تصویر کلاسیک همیشه شامل یک روش جایگشتی برای تغییر مکان پیکسل‌ها در تصویر اصلی و یک روش انتشار برای تغییر مقدار پیکسل است. جایگشت را می‌توان به دو دسته‌ی جایگشت سطح پیکسل و جایگشت سطح بیت، تقسیم کرد [۹]. در [۱۰] یک الگوریتم رمزنگاری تصویر با استفاده از جایگشت سطح بیت ارائه شده است. در ابتدا تصویر به هشت سطح بیتی تقسیم شده و سپس سطوح بیتی بالا که حاوی اطلاعات بیشتری هستند با استفاده از نگاشت آرنولد بصورت جداگانه جایگشت می‌شوند. همچنین جایگشت سطوح پایین با یکدیگر انجام می‌شود. در [۱۱] بررسی بر روی زمان مصرفی، جابجایی مکان پیکسل‌های تصویر با استفاده از نگاشت‌های آشوب دو بعدی انجام شده است. معمولاً یک نگاشت آشوب دو بعدی برای جایگشت پیکسل‌ها بکار گرفته می‌شود. از جمله نگاشت‌های آشوب دو بعدی که برای این کار مناسب هستند، نگاشت آرنولد، نگاشت استاندارد و نگاشت نانوا است [۱۱,۱۲]. در [۱۳] برخی از ویژگی‌های ذاتی ترکیب بیت در تصویر را در هنگام بررسی در سطح بیت، کشف کرده‌اند. آن‌ها متوجه شدند که سطوح بیت بالاتر در تصویر اصلی، دارای مقادیر متضاد هستند. همبستگی قوی بین سطوح بیتی بالا، به ویژه میان سطوح هفتم و هشتم وجود دارد. در [۱٤] یک الگوریتم رمزنگاری تصویر سطح بیت مبتنی بر آشوب تلفیقی و خود تطبیقی ارائه شده است. ایده اساسی خود تطبیقی تقسیم تصویر به دو بخش مساوی است و از اطلاعات یک بخش جهت رمزنگاری بخش دیگر استفاده می‌شود. در [۱۵] یک الگوریتم رمزنگاری تصویر با جایگشت سطح بیت با سه نوع تکنولوژی متفاوت گسسته‌سازی سطوح بیتی، گسسته‌سازی سطوح بیت به روش کدگری و گسسته‌سازی سطوح بیت به روش فیبوناچی، ارائه شده است [۱٦,۱۷]. نویسندگان در [۱۸] نشان دادند که تفاوت قابل توجهی از اطلاعات میان سطوح بیتی موجود است. در [۱۹] یک الگوریتم نوین رمزنگاری تصویر مبتنی بر بلاک و سیستم آشوب ارائه شده است. نویسندگان [۱۹] نشان دادند که نگاشت آرنولد برای جایگشت تصویر بسیار سریع است، از این جهت، آن برای انتقال داده بلا درنگ مهم است. در [۲۰] یک الگوریتم رمزنگاری تصویر رنگی مبتنی بر جایگشت داخلی ارائه شده است. روش جایگشت پیشنهادی در [۲۰] مبتنی بر توسعه و ادغام است. در [۲۱] نشان داده‌اند که الگوریتم‌های رمزنگاری که فقط دارای گام جایگشت تصویر هستند، برخی از آنها شاید دارای پیچیدگی محاسباتی کمتری باشند، اما با توجه به اینکه آنها فقط موقعیت پیکسل‌ها را جابجا می‌کنند و مقدار پیکسل را تغییر نمی‌دهند، دارای مشکلات امنیتی هستند.

۲) ابزار و روشها

a) نگاشت آشوب

نگاشت لجستیک یک بعدی، در الگوریتم‌های رمزنگاری تصویر، به دلیل ساختار ساده آن با رفتار آشوبی خوب، به طور گسترده‌ای مورد استفاده قرار گرفته است [۷]. با این حال، تنها یک پارامتر کنترل و یک شرایط اولیه دارد. دارای

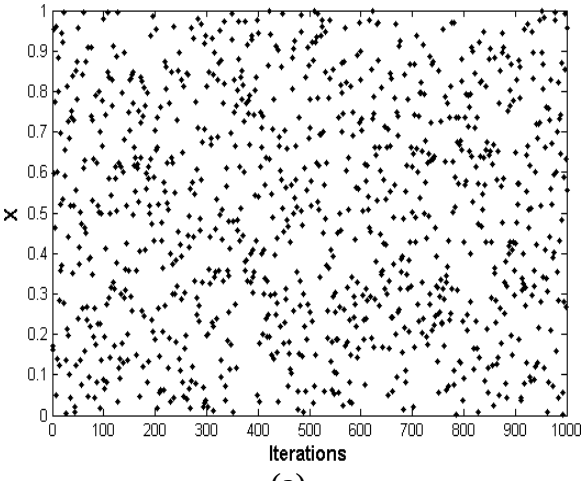
برخی از نقاط ضعف مانند روزنه‌های خالی، توزیع ناهموار توالی‌های تکرار شده است، که کلیدهای ضعیف را تولید می‌کند. به‌طوری‌که در [۲۲] مورد تجزیه و تحلیل واقع شده است. بنابراین، برای رفع این نقاط ضعف، نگاشت لجستیک سه بعدی در [۲۲] طراحی شده است که دارای پارامترهای کنترل بیشتر و شرایط اولیه بیشتری است. این نگاشت لجستیک سه بعدی بصورت زیر تشریح شده است.

$$\begin{bmatrix} \lambda & (1-x_i)+z_i] \\ z & (x \quad \text{n}(z_i)] \end{bmatrix} \frac{}{(1+} \text{mo} \qquad (1$$

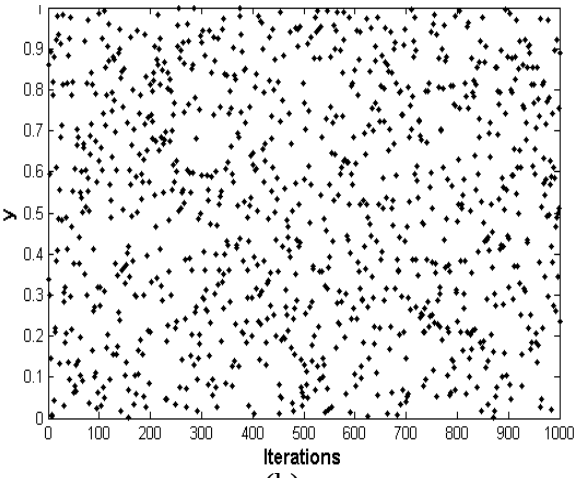
به طوری‌که

$$,|k_1|>33.5,|k_2|>37.9,|k_3|>$$

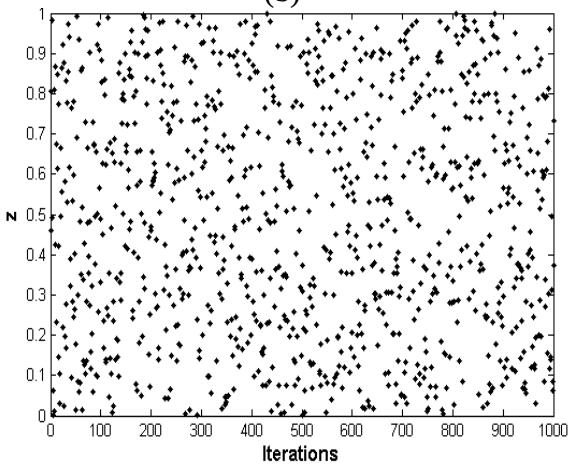
نگاشت لجستیک سه بعدی، دارای رفتار آشوبی برجسته، بدون ضعف‌های معمول روزنه‌های خالی، روزنه پایدار و توزیع ناهموار توالی‌های تکرار شده است، بنابراین می‌تواند کلیدهای قوی‌تر تولید کند [۱,۲۲]. شکل ۱ رفتار نگاشت آشوب لجستیک سه بعدی را در مختصات x، y و z را با شرایط اولیه زیر نشان می‌دهد.



(a)



(b)



(c)

شکل ۱- رفتار آشوب‌گونه نگاشت سه بعدی لجستیک:
(a) مختصات-x، (b) مختصات -y، (c) مختصات - z

b) تصویر در سطح بیت

در تصاویر خاکستری مقادیر پیکسل‌ها مابین 0 و 255 است به عنوان نمونه تصویر «لنا» با اندازه 256×256 در شکل (۲) نشان داده شده است. هر پیکسل می‌تواند به صورت یک دنباله‌ی باینری هشت بیتی نمایش داده شود. بنابراین همان‌طور که در شکل (۳) نشان داده شده است بر اساس مکان بیت در پیکسل، یک تصویر خاکستری می‌تواند به هشت تصویر باینری تجزیه شود. شکل (۳) نشان دهنده‌ی تصاویر باینری بدست آمده توسط مجموع بیت‌های i ام از همه‌ی پیکسل‌های تصویر اصلی است. با توجه به موقعیت یک بیت در پیکسل، یک بیت می‌تواند شامل مقادیر متفاوتی از اطلاعات باشد. برای مثال "1" در

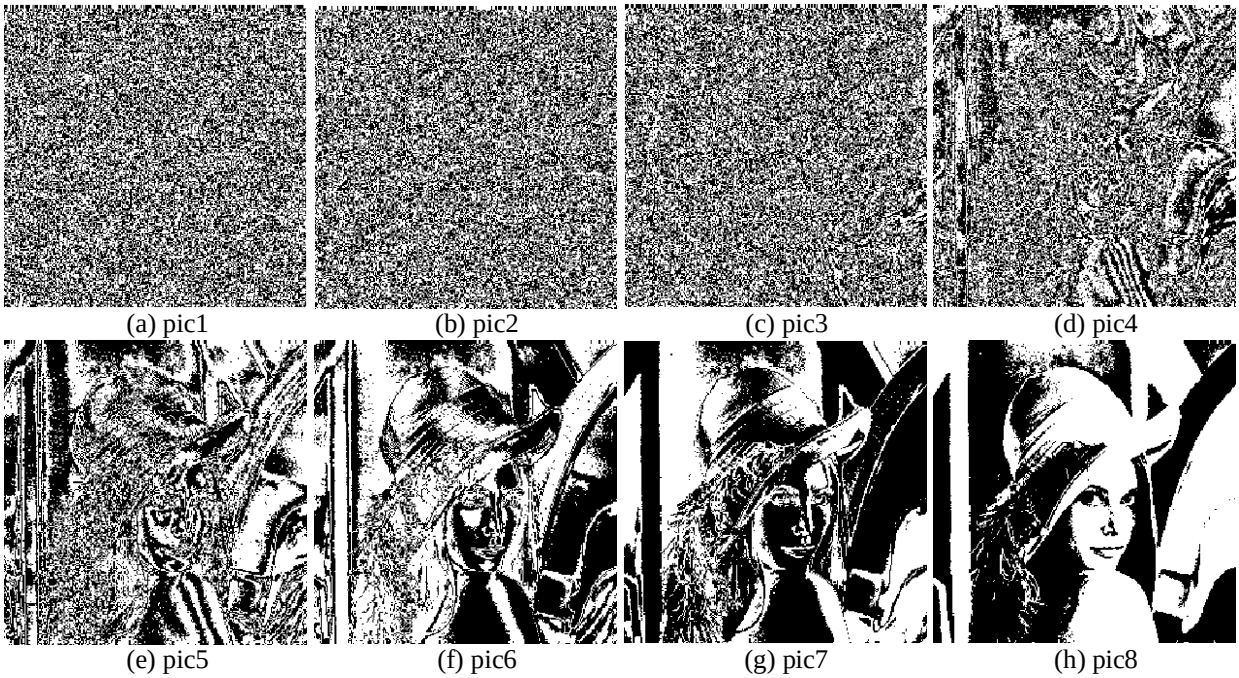
بیت ۸ ام یک پیکسل نشان دهنده‌ی (2^7)128 است، اما آن فقط نشان دهندی (2^0)1 در بیت اول است. مطابق رابطه (۲)، چهار بیت بالایی (8th, 7th, 6th, 5th) حاوی 94.125% از اطلاعات کل تصویر هستند. به عبارت دیگر، چهار بیت پایینی (4th, 3rd, 2nd, 1st) کمتر از 6% از اطلاعات تصویر را دارند. درصد اطلاعات پیکسل در جدول ۱ نشان داده شده است [۲۶-۲۳].

$$p(i) = \frac{}{\sum^{8} \quad i-1}, i = \{1,2, \dots, 8\} \qquad (2)$$

جدول ۱- درصد اطلاعات پیکسل با در نظر گرفتن بیت‌های متفاوت [23]

موقعیت بیت	درصد کل اطلاعات
1	0.3922
2	0.7843
3	1.5686
4	3.137
5	6.275
6	12.55
7	25.10
8	50.20

شکل ۲- تصویر «لنا» با اندازه 256 × 256



(a) pic1 (b) pic2 (c) pic3 (d) pic4

(e) pic5 (f) pic6 (g) pic7 (h) pic8

شکل ۳- هشت سطح بیتی از تصویر «لنا»

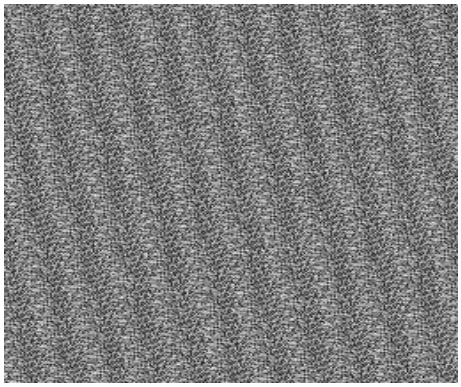
c) نگاشت دو بعدی آرنولد

این نگاشت هنگامی‌که به تصویر اعمال می‌شود، مکان اصلی پیکسل‌ها را بصورت تصادفی تغییر می‌دهد و به صورت رابطه (۳) تعریف می‌شود.

$$\begin{bmatrix} \acute{x} \\ \acute{y} \end{bmatrix} \rightarrow \begin{bmatrix} \quad \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N \quad (۳)$$

به طوری‌که، در اینجا $x, y \in \{1, 2, \dots N-1\}$ و N اندازه

تصویر است، p, q پارامترهای کنترل هستند، $\begin{bmatrix}x\\y\end{bmatrix}$ مکان اصلی پیکسل‌های تصویر اصلی را نشان می‌دهد و $\begin{bmatrix}x'\\y'\end{bmatrix}$ مکان جدید پیکسل‌ها پس از تبدیل نگاشت را نشان می‌دهد [۲۷]. شکل ٤ نگاشت آرنولد اعمال شده بر روی شکل ۲ را نشان می‌دهد. این نگاشت مقادیر پیکسل‌های تصویر را تغییر نمی‌دهد و تنها مکان پیکسل‌های تصویر را جابجا می‌کند.



شکل ٤- تصویر بهم ریخته شده با استفاده از نگاشت آرنولد.

در [۱۱]، بررسی بر روی زمان مصرفی، جابجایی مکان پیکسل‌های تصویر با استفاده از نگاشت‌های آشوب دو بعدی انجام شده است. معمولاً یک نگاشت آشوب دو بعدی برای جایگشت پیکسل‌ها بکار گرفته می‌شود. از جمله نگاشت‌های آشوب دو بعدی که برای این کار مناسب هستند، نگاشت آرنولد، نگاشت استاندارد و نگاشت نانوا است.

یک نگاشت آشوب دو بعدی، یک قانون نگاشت از یک مکان مشخص در تصویر اصلی، به یک مکان تصادفی در تصویر بهم ریخته شده، تعریف می‌کند. برای هر پیکسل در تصویر اصلی، دو نوع عملیات نیازمند است که انجام شود: محاسبه موقعیت جدید پیکسل و انتقال پیکسل از موقعیت اصلی به موقعیت جدید. فرایند جایگشت برای یک تصویر با اندازه 512×512 را در نظر بگیرید، به طور کلی دارای 262,144 پیکسل است. از آنجا که جهت انتقال پیکسل به مکان جدید، نیازمند محاسبه دو موقعیت x, y هستیم، در نتیجه نیازمند محاسبه 262144×2=524288 عدد تصادفی خواهیم بود و محاسبه هر یک از اعداد شامل عملیات پیچیده (ضرب و تقسیم) خواهد بود. با این حال، نوع دوم عملیات، فقط لازم است تا یک بایت از حافظه به آدرس دیگری در حافظه منتقل شود. زمان محاسبه این نوع عملیات در جدول ۲ برای تصویر "لنا" با اندازه 512×512 آورده شده است. مطابق جدول ۲، میانگین زمان مصرفی نوع اول عملیات، بیشتر از نوع دوم است [۱۱].

جدول ۲- زمان اجرای دو نوع عملیات در گام جایگشت [۱۱].

نگاشت	زمان مصرفی نوع اول عملیات (میلی ثانیه)	زمان مصرفی نوع دوم عملیات (میلی ثانیه)
نگاشت آرنولد (Cat map)	3.1	3.1
نگاشت استاندارد (Standard map)	50	3.1
نگاشت نانوا (Baker map)	31	3.1

با توجه به بررسی‌های انجام گرفته در مرجع [۱۱]، بر روی زمان مصرفی نگاشت‌های آشوب دو بعدی، برای جایگشت پیکسل‌های تصویر، بطوری‌که نتایج در جدول ۲ نشان داده شده است، واضح است که نگاشت دو بعدی آرنولد، برای جایگشت تصویر بسیار سریع است، به طوری‌که، برای انتقال داده بصورت بلادرنگ، دارای اهمیت است. از طرفی، برای تصاویری که دارای اندازه‌های بزرگی هستند، نگاشت آرنولد می‌تواند برای جایگشت تصویر، بسیار سریع عمل کند، که منجر به افزایش سرعت الگوریتم رمزنگاری می‌گردد.

۳) روش پیشنهادی

a) جایگشت سطح بیتی

الگوریتم‌های جایگشت نقش مهمی را در رمزنگاری تصویر ایفا می‌کنند. بطوری‌که همواره اولین گام در سیستم

رمزنگاری جابجایی همه‌ی پیکسل‌ها و یا بیت‌ها است. در ابتدا، تصویر اصلی به هشت تصویر باینری گسسته می‌شود و سپس تصاویر باینری سطوح بیتی فرد، شکل ۵ (a) (pic1, pic3, pic5, pic7) در یک گروه و تصاویر باینری سطوح بیتی زوج، شکل ۵ (b) (pic2, pic4, pic6, pic8) در گروه دیگر قرار می‌گیرند. در گام بعدی، با استفاده از نگاشت دو بعدی آرنولد مکان بیت‌های هر یک از گروه‌ها را جابجا می‌کنیم. نتیجه جایگشت سطح بیتی، در شکل (۵) (c) نشان داده شده است. روش پیشنهادی موجب می‌شود که گروهی از بیت‌ها از یک سطح بیت به سطح بیت دیگر منتقل گردند. در هر یک از سطوح بیتی تصویر جایگشت شده، اکثر بیت‌ها از سطوح بیتی دیگر هستند. در نتیجه، اطلاعات آماری تمامی سطوح بیتی تغییر می‌یابد. همانطور که قابل ملاحظه است اثرات زیر می‌تواند در جایگشت سطح بیتی بدست آید.

۱- توزیع بیت در هر سطح بیت یکنواخت‌تر است.

۲- همبستگی بین سطوح بیتی بالایی می‌تواند کاهش یابد.

۳- نه تنها موقعیت، بلکه مقادیر پیکسل‌ها نیز تغییر می‌یابد.

شکل ۵ (a): قرار گرفتن سطوح بیتی فرد در یک گروه.

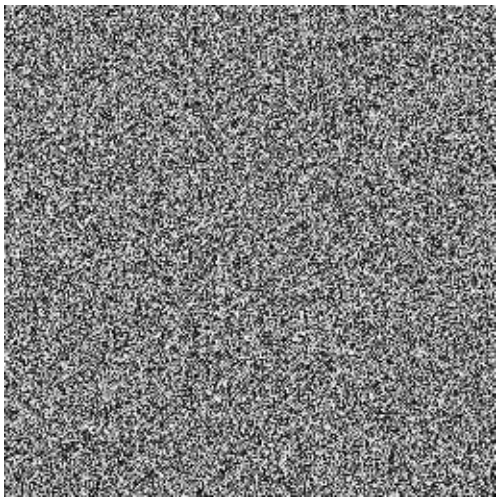
شکل ۵ (b): قرار گرفتن سطوح بیتی زوج در یک گروه

b) رمزنگاری

گام‌های روش ارائه شده بصورت زیر است.

گام ۱: ورودی یک تصویر خاکستری بنام P(N, N) است.

گام ۲: تصویر خاکستری به هشت تصویر باینری گسسته می‌شود. سطوح بیتی فرد در یک گروه و سطوح بیتی زوج در گروه دیگر قرار می‌گیرند. بطوری‌که اندازه بخش جدید مشابه شکل (۵) (a,b) برابر 2N×2N خواهد بود. سپس، جایگشت سطح بیت، با استفاده از نگاشت دو بعدی آرنولد همانطور که در بخش قبل شرح داده شد، اعمال می‌گردد. آنگاه، سطوح بیتی جایگشت شده با یکدیگر ترکیب شده و ما می‌توانیم تصویر جایگشت شده را دریافت نماییم. در نتیجه، اندازه تصویر جایگشت شده N×N خواهد بود.



شکل ۵ (c): جایگشت شکل ۲ به روش پیشنهادی.

گام ۳: برای اینکه طرح پیشنهادی در مقابل حمله‌ی تفاضلی مقاوم باشد مقادیر اولیه سیستم لجستیک سه بعدی X_0, Y_0, Z_0 با استفاده از رابطه ٤ بروزرسانی می‌شوند.

$$\begin{matrix} d((X & 1), \\ d((Y & 1), \\ d((Z & \end{matrix} \quad \frac{\left(\sum\sum P_{(i,j)}, 256\right)}{} \qquad (4)$$

گام ٤: جهت اجتناب از اثر ناپایداری، سیستم لجستیک سه بعدی ۲۰۰ بار تکرار می‌شود، به طوری‌که اعداد تولید شده در نظرگرفته نمی‌شود، سپس تکرار نگاشت ادامه می‌یابد.

گام ٥: تکرار سیستم لجستیک سه بعدی، N×N بار جهت تولید دنباله‌های آشوبی، ادامه می‌یابد. آنگاه، با استفاده از رابطه (٥) دنباله‌های آشوبی تولید شده را به دنباله‌های صحیح، به عنوان کلید، جهت رمزنگاری، تبدیل می‌کنیم. در نتیجه مقادیر k1, k2, k3 در بازه [255، 0] قرار دارند.

$$\begin{matrix} \left(X_i \times (10^{14})\right)\text{mo} \\ \left(Y_i \times (10^{14})\right)\text{mod } 256 \\ \left(Z_i \times (10^{14})\right)\text{mo} \end{matrix} \qquad (5$$

گام ٦: عملگر Xor را برای هر پیکسل از تصویر اصلی جایگشت شده، با یک متغیر انتخابی از سه متغیر $k_i\ i = 1, 2, 3$ اعمال می‌نماییم، به طوری‌که یک متغیر بصورت تصادفی با رابطه (٦) انتخاب می‌شود.

$$d(X \qquad (6$$

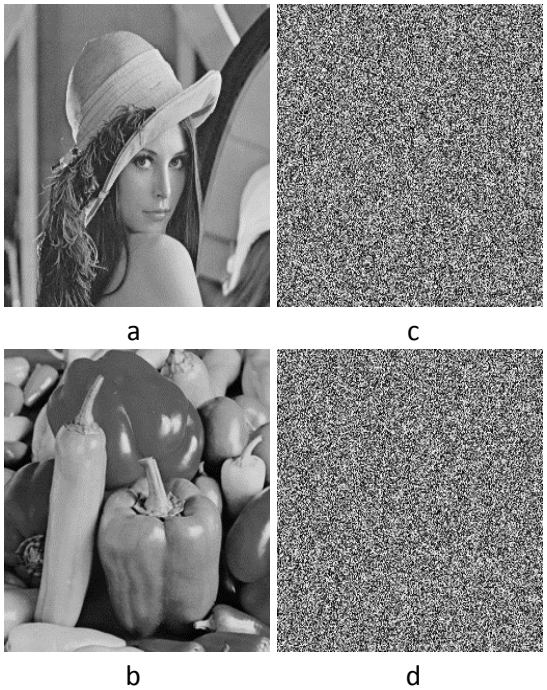
مقدار key حاصل از رابطه (٦) عدد صحیح موجود در بازه [۳, ۱] است. با استفاده از مقدار key به عنوان شماره اندیس می‌توانیم از سه متغیر حاصل از سیستم آشوبی k1, k2, k3 ایجاد شده در مراحل قبل، یک متغیر را بصورت تصادفی جهت رمزنگاری انتخاب نماییم.

$$C(i \qquad p(i,j) \oplus key, \quad key \in [k1, k2, k3] \qquad (7$$

بطوری‌که $i = 1, 2, \ldots, N;\ j = 1, 2, \ldots, N$ است. علامت $\oplus$ نشان دهنده‌ی عملگر XOR است. C تصویر رمزنگاری شده است. گام‌های فوق برای رمزنگاری تصویر ارائه شده‌اند، بدیهی است برای رمزگشایی تصویر گام‌های مذکور را باید بالعکس انجام داد.

٤) نتیجه شبیه سازی و تجزیه و تحلیل

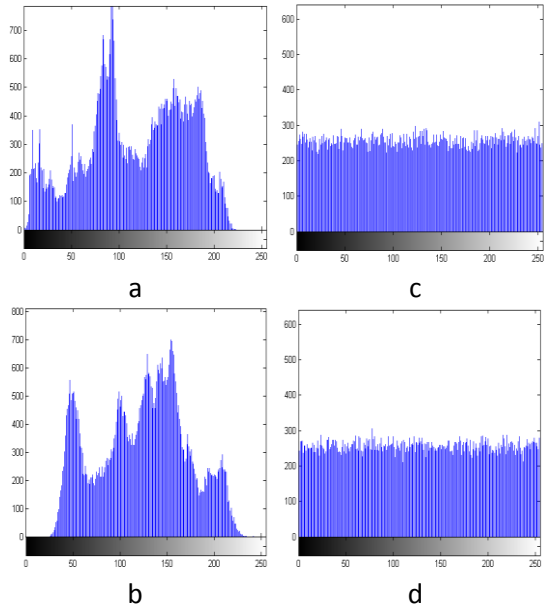
در این بخش جهت ارزیابی روش پیشنهادی، از برخی تصاویر استاندارد، با اندازه 256 × 256 به عنوان تصویر ورودی استفاده کرده‌ایم. شکل ٦ (a, b) تصاویر اصلی «لنا» و «فلفل‌ها» را نشان می‌دهد. با استفاده از الگوریتم پیشنهادی، تصاویر رمزنگاری مربوطه به ترتیب، در شکل ٦ (c, d) نمایش داده شده است. بدیهی است، از نقطه نظر بصری، هیچ ارتباطی بین تصاویر اصلی و تصاویر رمزنگاری شده وجود ندارد. این نشان می‌دهد که الگوریتم پیشنهادی می‌تواند اثر رمزنگاری خوبی داشته باشد.



شکل(٦): (a,b): تصاویر اصلی و (c, d): بترتیب رمزنگاری تصاویر اصلی به روش پیشهادی.

a) تحلیل هیستوگرام

هیستوگرام توزیع پیکسل‌ها را برای یک تصویر نشان می‌دهد. هیستوگرام برای تصویر رمزنگاری شده باید توزیع یکنواختی در مقایسه با تصویر اصلی داشته باشد [1]. به عنوان یک آزمون، شکل ۷ (a, b) هیستوگرام را برای تصاویر اصلی «لنا» و «فلفل‌ها» نشان می‌دهد. هیستوگرام مربوط به تصاویر رمزنگاری شده به ترتیب در شکل ۷ (c, d) نشان داده شده است. قابل مشاهده است که پیکسل‌ها در تصاویر رمزنگاری شده، یکنواخت توزیع شده‌اند. در نتیجه، الگوریتم پیشنهادی توانایی مقاومت در برابر حملات آماری را دارد.



شکل(۷): بترتیب هیستوگرام تصاویر اصلی «لنا»، «فلفل‌ها» (a,b): قبل از رمزنگاری و (c, d): پس از رمزنگاری

b) تجزیه و تحلیل ضریب همبستگی

به خوبی شناخته شده است که ضریب همبستگی کم میان پیکسل‌های مجاور در تصویر رمزنگاری شده، مقاومت بیشتری در برابر حملات آماری دارد. در این بخش، ضریب همبستگی پیکسل‌های مجاور در تصویر اصلی و تصویر رمزنگاری شده مطالعه شده است. از روابط زیر، برای بررسی همبستگی بین دو پیکسل مجاور، در راستای افقی، عمودی و قطری استفاده می‌شود [27].

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i,\ D(x) = \frac{1}{N}\sum_{i=1}^{N}(x - E(x))^2$$

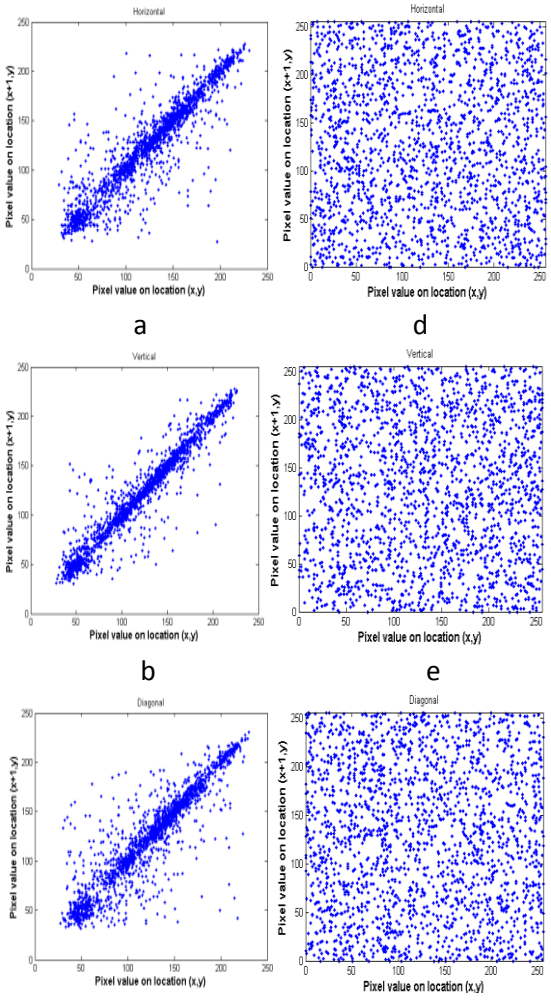
$$Cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x - E(x))(y_i - E(y)) \quad (8$$

$$\frac{v(x}{\sqrt{D(x)} \times \sqrt{D(}}$$

که در آن x و y مقادیر دو پیکسل همجوار در تصویر هستند و N تعداد پیکسل‌های همجوار انتخاب شده از تصویر است. شکل ۸ همبستگی پیکسل‌های همجوار، تصویر رمزنگاری شده «لنا» را در سه جهت افقی و عمودی و قطری قبل از رمزنگاری و پس از رمزنگاری نشان می‌دهد. در جدول ۳ ضریب همبستگی روش پیشنهادی با مراجع مختلف مقایسه شده است. بنابراین، مقادیر ضریب همبستگی و شکل ۸ (d, e, f) نشان دهنده‌ی این است که ضریب همبستگی تصویر رمزنگاری شده بسیار کاهش پیدا کرده است و طرح رمزنگاری ارائه شده مؤثر است.

جدول ۳- مقایسه ضریب همبستگی و آنتروپی با مراجع مختلف

Algorithm	Correlation coefficients			entropy
	Horizontal	Vertical	Diagonal	
Our algorithm (Lena)	-0.0054	-0.0062	0.0005	7.9971
Our algorithm (Peppers)	-0.0038	-0.0039	-0.0062	7.9975
Our algorithm (Baboon)	-0.0060	-0.0013	0.0082	7.9972
Ref. [14]	0.0241	-0.0194	0.0243	7.9974
Ref. [23]	-0.0035	-0.0574	0.0578	7.9881
Ref. [24]	-0.0098	-0.0050	-0.0013	7.9972
Ref. [25]	-0.0230	0.0019	-0.0034	7.9974



شکل(۸): توزیع همبستگی تصویر اصلی «لنا» در سه جهت افقی و عمودی و قطری. (a, b, c): قبل از رمزنگاری و (d, e, f): پس از رمزنگاری.

c) آنتروپی اطلاعات

آنتروپی اطلاعات می‌تواند به عنوان معیاری برای به دست آوردن میزان آشفتگی سطوح خاکستری پیکسل‌ها استفاده شود. در تصویر رمزنگاری‌شده مقدار آنتروپی باید نزدیک به مقدار ایده‌آل ۸ باشد. آنتروپی یک تصویر از رابطه (۹) محاسبه می‌شود:

$$H(m)=\sum_{i=1}^{2^N-1} p(m_i)\log_2\frac{1}{p(mi}} \quad (9)$$

در این رابطه $p(m_i)$ احتمال وقوع سطح خاکستری و تعداد سطوح خاکستری ممکن است. در جدول ۳، آنتروپی اطلاعات مربوط به رمزنگاری تصاویر مختلف با مراجع مختلف نیز مورد مقایسه قرار گرفته است.

d) حملات تفاضلی

تأثیر تغیر یک پیکسل در تصویر اصلی بر روی تصویر رمزنگاری شده متناظر آن، با دو معیار NPCR (مقدار نرخ تغییر پیکسل‌ها) و UACI (میانگین شدت تغییرات) استفاده می‌شود که از طریق روابط زیر قابل محاسبه است [۱,۳].

$$\left(\sum_{i=1}^{W}\sum \quad D\,(i,j)/(W \qquad 100\%\right) \quad (10$$

$$\left(\sum \sum \frac{|\acute{C}(i,j)-C(i,j)|}{H}\right) \quad (W$$

$$(10$$

بطوری که، H,W بترتیب طول و عرض تصاویر هستند. و ً دو تصویر رمزنگاری شده‌اند که از دو تصویر با یک پیکسل اختلاف گرفته شده‌اند و $D(i,j)$ از رابطه زیر محاسبه می‌شود.

$$\begin{cases} \acute{C} \\ \acute{C} \end{cases} \quad (11$$

جدول ٤ نتایج و میانگین NPCR و UACI را برای تصاویر اصلی مختلف، بر اساس روش پیشنهادی نشان می‌دهد. در جدول ۵، NPCR و UACI روش پیشنهادی با مراجع مختلف مقایسه شده است. واضح است که طرح رمزنگاری به تغییر کوچک در تصویر اصلی بسیار حساس است و می‌تواند مقاومت خوبی داشته باشد.

جدول ٤- نتایج و میانگین NPCR و UACI برای تصاویر مختلف

Image	NPCR (%)	UACI (%)
Lena	99.6261	33.5810
Peppers	99.5849	33.3832
Baboon	99.6145	33.4161
Average for all images	99.6085	33.4601

جدول ۵- مقایسه NPCR و UACIبا مراجع مختلف

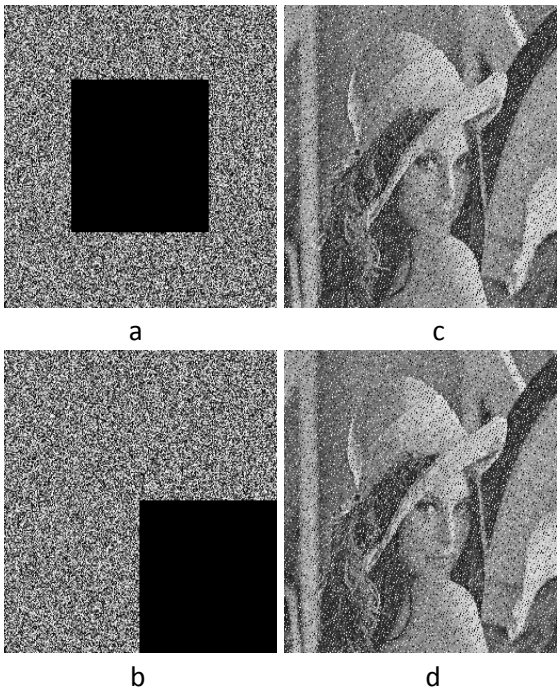
Algorithm	NPCR (%)	UACI (%)
Our algorithm	99.6085	33.4601
Ref. [14]	93.6768	33.3364
Ref. [19]	99.5864	33.2533
Ref. [24]	99.6163	33.4893
Ref. [25]	99.6200	33.5100
Ref. [28]	99.6096	33.4574

e) حمله از دست دادن داده‌ها

یک سیستم رمزنگاری خوب باید در برابر اثرکاهش داده‌ها ایمن باشد. بخشی ازتصویر رمزنگاری شده ممکن است در طول انتقال مفقود شود و یا تغییر یابد [۳,۲۶]. ما برخی از داده‌ها را با اندازه‌های مختلف، از تصویر رمزنگاری شده حذف کرده‌ایم. و با این روش، تصویر رمزنگاری شده را مورد حمله‌ی از دست دادن داده‌ها قرار داده‌ایم. به طوری‌که این داده‌های از دست رفته در شکل ۹(a, b) نشان داده شده است. سپس، تصاویر رمزنگاری شده که مورد حمله واقع شده‌اند را رمزگشایی کرده‌ایم. همانطور که در شکل (۹) (c, d) نشان داده شده است، در حالی که 50% از داده‌های کل تصویر از دست رفته‌اند، تصویر رمزگشایی شده هنوز هم می‌تواند تشخیص داده شود.

f) تجزیه و تحلیل فضای کلید

برای یک الگوریتم رمزنگاری تصویر با امنیت بالا، فضای کلید، باید حداقل $10^{30} \approx 2^{100}$ باشد [۱]. در نگاشت سه بعدی لجستیک، سه کلید اولیه، x0، y0 و z0، به عنوان کلیدهای مخفی در الگوریتم رمزنگاری استفاده می‌شوند. فضای کلید آن، اگر دقت 10^{-14} باشد، می‌تواند به 10^{42} برسد که می‌تواند به طور مؤثر در برابر حمله‌ی جستجوی جامع، مقاومت کند.



شکل(۹): مفقود شدن داده ها (a,b): 50% از داده‌ها از دست رفته‌اند. (c, d): بازیابی داده‌های از دست رفته به روش پیشنهادی.

۵) نتیجه‌گیری

در این مقاله یک روش نوین جهت رمزنگاری تصاویر مبتنی بر تجزیه سطح بیت و توابع آشوب ارائه گردید. در این روش ابتدا تصویر به سطوح بیتی مختلف تقسیم گردید و آنگاه، سطوح بیتی فرد در یک گروه و سطوح بیتی زوج در گروه دیگر قرار گرفتند. سپس، با استفاده از نگاشت دو بعدی آرنولد جایگشت را در سطح بیت بر روی هر یک از گروه‌ها انجام دادیم، در نتیجه توزیع بیت در هر یک از سطوح بیتی یکنواخت گردید و نه تنها موقعیت بیت در پیکسل، بلکه مقادیر پیکسل‌ها نیز تغییر یافت. و از طرفی منجر به تغییر اطلاعات آماری تصویر گردید. مزیت این روش در این است که، اگر مهاجم تصویر جایگشت شده را به دست آورد، نمی‌تواند اطلاعت آماری تصویر را مورد تجزیه و تحلیل قرار دهد. همچنین از قابلیت‌ها و خصوصیات توابع آشوب شامل حساسیت به مقادیر اولیه، رفتار تصادفی، غیر تناوبی بودن و قطعی بودن، بهره گرفته‌ایم و با استفاده از نگاشت آشوب لجستیک سه بعدی

که دارای فضای کلید بزرگی است، عمل رمزنگاری انجام گردید. از طریق نتیجه آزمایش و تجزیه و تحلیل امنیت، مشاهده می‌شود، هیستوگرام تصویر رمزنگاری شده توزیع بسیار یکنواختی دارد. در تصاویر رمزنگاری شده به مقدار آنتروپی ۷.۹۹۷۵ دست یافته‌ایم، که به مقدار ایده‌آل، یعنی ۸ بسیار نزدیک است. همبستگی بین پیکسل‌های تصویر رمزنگاری شده کاهش یافته است. الگوریتم اثر رمزگذاری خوب و فضای کلید مخفی بزرگتر دارد. علاوه بر این، الگوریتم پیشنهادی می‌تواند در برابر، حملات شناخته شده، مانند مقاومت در برابر تجزیه و تحلیل آماری، حملات جستجوی جامع و حمله‌ی تفاضلی را داشته باشد. همچنین روش پیشنهادی، مقاومت بسیار مناسبی در برابر داده‌های از دست رفته‌ی احتمالی، دارد. و می‌تواند داده‌های از دست رفته را بازسازی نماید. همه‌ی این ویژگی‌ها نشان می‌دهد که الگوریتم ارائه شده برای رمزنگاری تصویر دیجیتال بسیار مناسب است.

٦) مراجع

[1] Guodong Ye, Xiaoling Huang, An efficient symmetric image encryption algorithm based on an intertwining logistic map, Neurocomputing (2017), doi: 10.1016/j.neucom.2017.04.016.

[2] Laiphrakpam Dolendro Singh, Khumanthem Manglem Singh, Medical image encryption based on improved ElGamal encryption technique, Optik - International Journal for Light and Electron Optics (2017), http://dx.doi.org/10.1016/j.ijleo.2017.08.028.

[3] Abolfazl Yaghouti Niyat, Mohammad Hossein Moattar, Masood Niazi Torshiz, Color image encryption based on hybrid hyper-chaotic system and cellular automata, Optics and Lasers in Engineering 90 (2017) 225–237.

[4] Q. Zhang, L. Liu, X. Wei, "Improved algorithm for image encryption based on DNA encoding and multi-chaotic maps", Int. J.Electron. Commun. (AEÜ) 68 (3) (2014) 186–192.

[5] Zhang Q, Guo L, Wei, "Image encryption using DNA addition combining with chaotic maps", Mathematical and Computer Modelling, 52, (2010) 2028-2035.

[6] Liu L, Zhang Q, Wei, "A RGB image encryption algorithm based on DNA encoding and chaos map", Computers and Electrical Engineering, 38(2012) 1240-1248.

[7] R. Enayatifar, A.H. Abdullah, I.F. Isnin, "Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence", Opt. Lasers Eng. 56 (2014) 83–93.

[8] R. Enayatifar, H.J. Sadaei, A.H. Abdullah, M. Lee, I.F. Isnin, "A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata", Opt. Lasers Eng. 71(2015) 33–41.

[9] Hegui Zhu, Cheng Zhao, Xiangde Zhang, Lianping Yang, "An image encryption scheme using generalized Arnold map and affine cipher", Optik 125 (2014) 6672–6677.

[10] Zhi-liang Zhu, Wei Zhang, Kwok-wo Wong, Hai Yu, "A chaos-based symmetric image encryption scheme using a bit-level permutation", Information Sciences 181 (2011) 1171–1186.

[11] Wei Zhang, Kwok-wo Wong, Hai Yu, Zhi-liang Zhu, "An image encryption scheme using lightweight bit-level confusion and cascade cross circular diffusion", Optics Communications 285 (2012) 2343–2354.

[12] Jiri Fridrich, International Journal of Bifurcation and Chaos 8 (6) (1998) 1259.

[13] Wei Zhang, Kwok-wo Wong, Hai Yu, Zhi-liang Zhu, "A symmetric color image encryption algorithm using the intrinsic features of bit distributions", Commun Nonlinear Sci Numer Simulat 18 (2013) 584–600.

[14] Lin Teng, Xingyuan Wang, "A bit-level image encryption algorithm based on spatiotemporal chaotic system and self-adaptive" Optics Communications 285 (2012) 4048–4054.

[15] Yicong Zhou, Weijia Cao, C.L. Philip Chen, Image encryption using binary bitplane, Signal Processing 100 (2014) 197–207.
[16] Y. Zhou, K. Panetta, S. Agaian, C.L.P. Chen, Image encryption using p-Fibonacci transform and decomposition, Opt. Commun. 285 (5) (2012) 594–608.
[17] R.C. Gonzalez, R.E. Woods, Digital Image Processing, 3rd edition, Pearson Prentice Hall, Upper Saddle River, New Jersey, 2008 ISBN 9780131687288.
[18] Zhang Ying-Qian, Wang Xing-Yuan, "A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice", Inform. Sci. (2014), http://dx.doi.org/10.1016/j.ins.2014.02.156.
[19] Xingyuan Wang, Lintao Liu, Yingqian Zhang, "A novel chaotic block image encryption algorithm based on dynamic random growth technique", Optics and Lasers in Engineering 66 (2015) 10–18.
[20] Wei Zhang, Hai Yu, Zhi-liang Zhu, "Color image encryption based on paired interpermuting planes", Communications.
[21] Chong Fu, Bin-bin Lin, Yu-sheng Miao, Xiao Liu, Jun-jie Chen, "A novel chaos-based bit-level permutation scheme for digital image encryption", Optics Communications 284 (2011) 5415–5423.
[22] I. S. Sam, P. Devaraj, R.S. Bhuvaneswaran, An intertwining chaotic maps based image encryption scheme, Nonlinear Dynamics, 2012, 69(4): 1995-2007.
[23] Hongjun Liu, Xingyuan Wang, Color image encryption using spatial bit-level permutation and high-dimension chaotic system, Optics Communications 284 (2011) 3895–3903.
[24] Xingyuan Wang, Hui-li Zhang, A color image encryption with heterogeneous bit-permutation and correlated chaos, Optics Communications 342 (2015) 51–60.
[25] Lu Xu, ZhiLi, JianLi, WeiHua, A novel bit-level image encryption algorithm based on chaotic maps, Optics and Lasers in Engineering 78 (2016) 17–25.
[26] Zhenjun Tang, Juan Song, Xianquan Zhang, Ronghai Sun, Multiple-image encryption with bit-plane decomposition and chaotic maps, Optics and Lasers in Engineering 80(2016)1–11.
[27] Laiphrakpam Dolendro Singh, Khumanthem Manglem Singh, Medical image encryption based on improved ElGamal encryption technique, Optik - International Journal for Light and Electron Optics (2017), http://dx.doi.org/10.1016/j.ijleo.2017.08.028.
[28] Chun Cao, Kehui Sun, Wenhao Liu, A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map, Signal Processing (2017), doi:10.1016/j. sigpro.2017.08.020.