فصلنامه پژوهش‌های حفاظتی ـ امنیتی دانشگاه جامع امام حسین(علیه‌السلام)
سال سوم، شماره‌ی ۱۳ (بهار ۱۳۹۴): صص ۹۱ – ۱۰۷

الگوریتم جدید درهم‌ریزی تصاویر خاکستری با استفاده از شبکه‌های اتصالی امگا

فریبا دهقانی فیروزآبادی[۱]
علی‌محمد لطیف[۲]

تاریخ دریافت: ۱۳۹۳/۱۰/۲۸
تاریخ پذیرش: ۱۳۹۳/۱۲/۱۵

چکیده

رمزنگاری، یکی از روش‌های تأمین امنیت است که با استفاده از یک رابطه ریاضی برگشت‌پذیر انجام می‌گیرد. تصویر، به‌عنوان یکی از پراستفاده‌ترین محصولات دیجیتالی – به دلیل ماهیت خاص خود – دارای الگوریتم‌های رمزنگاری ویژه است. در این مقاله یک الگوریتم رمزنگاری جدید برای تصاویر دیجیتال خاکستری با استفاده از شبکه‌های اتصالی امگا – که یکی از ابزارهای پردازنده موازی محسوب می‌شود – پیشنهاد شده است. در این الگوریتم ابتدا تصویر، قالب‌بندی می‌شود و با استفاده از فن جاگذاری و یک شبکه امگا، پیکسل‌های هر قالب درهم‌ریخته می‌شود. در سال‌های اخیر، روش‌های گوناگونی برای رمزنگاری تصویر ارائه شده است. برای ارزیابی الگوریتم‌های مختلف از معیارهای آزمون بصری، تحلیل همبستگی، معیارهای خطا و تحلیل هیستوگرام استفاده می‌شود. نتایج آزمایش‌ها نشان می‌دهد روش پیشنهادی علاوه بر داشتن کیفیت بصری مناسب، معیارهای خطای NPCR، MAE و UACI را به طور متوسط به ترتیب در حد ۴۶/۷۶۰۱ ، ۳۹/۰۱۲۴ و ۱۷/۷۶۲۵ کاهش داده است. همچنین الگوریتم پیشنهادی توانسته است معیار همبستگی پیکسل‌ها در سه راستای افقی، عمودی و قطری به طور متوسط در حد ۰/۱۷۲۵، ۰/۱۷۸۹ و ۰/۱۷۴۳ کاهش دهد.

کلید واژه‌ها: *تصویر دیجیتال، درهم‌ریزی، شبکه‌های اتصالی درونی، شبکه امگا*

۱- دانشجوی کارشناسی ارشد، گروه کامپیوتر، واحد میبد، دانشگاه آزاد اسلامی، میبد، ایران، Fdehghani200@gmail.com
۲- استادیار، دانشکده برق و کامپیوتر، دانشگاه یزد، یزد، ایران، alatif@yazd.ac.ir

۱- مقدمه

امنیت اطلاعات یک امر مهم و حیاتی برای حریم اطلاعات افراد و سازمان‌ها است. یکی از ابزارهای پرقدرت برای ارضای این نیاز «رمزنگاری» است. امروزه رمزنگاری بیش‌تر به‌عنوان مطالعه روش‌ها و الگوریتم‌های رمزنگاری تلقی می‌شود که در پس این روش‌ها، مسائل ریاضیاتی موجود است. بسیاری افراد، از رمزنگاری برای محرمانه نگه‌داشتن اطلاعاتشان استفاده می‌کنند. رمزگذاری یعنی تبدیل داده به شکلی که خواندن آن بدون دانش مناسب و کلید، غیرممکن باشد.

وابستگی سطوح خاکستری پیکسل‌های مجاور در تصویر باعث شده است تا الگوریتم‌های رمزنگاری متن بر روی تصویر قابل استفاده نباشد (Ding, et al,2000:7-14) و (Wei, et al,1999:900-904). این ویژگی باعث شده است تا حوزهٔ رمزنگاری تصویر از بقیه حوزه‌های رمزنگاری جدا شود.

با توجه به حجم بالای دادهٔ تصویری و همچنین ویژگی‌های خاص تصویر، استفاده از الگوریتم‌های کلاسیک رمزنگاری مانند RSA[1] و DES[2] در رمزنگاری تصویر ناکارآمد است؛ زیرا این الگوریتم‌ها، وقت‌گیر بوده و در سامانه‌های بلادرنگ قابل‌استفاده نمی‌باشند. (Pareek, et al, 2006:926-934) و (Kanso, Ghebleh, 2012: 2943-2959).

روش‌هایی که تاکنون برای رمزنگاری تصویر ارائه شده‌اند بر اساس دو فن جاگذاری[3] و درهم‌ریزی[4] کار می‌کنند. در روش جاگذاری با استفاده از روابط ریاضی برگشت‌پذیر، به ازای هر پیکسل تصویر، یک سطح روشنایی جدید جایگزین می‌شود. در روش درهم‌ریزی تصویر، ترتیب پیکسل‌های موجود در تصویر با استفاده از الگوریتم رمزنگاری به‌هم‌ریخته می‌شود. (Che, et al, 2008:495-499).

تاکنون الگوریتم‌های رمزنگاری زیادی برای رمزنگاری تصاویر دیجیتال ارائه شده است. الگوریتم‌های فیبوناچی، تبدیل آرنولد، تبدیل مرتب و کد گری را می‌توان نام برد ؛ اما طبق مطالعه‌های انجام شده الگوریتم فیبوناچی(Jiancheng, et al, 2004:1-10) و تبدیل آرنولد (Ying, et al, 2007:2737-2741) در اولین اجرا به خوبی نمی‌توانند تصویر را درهم بریزند. همچنین الگوریتم کدگری (Wei, et al,1999:900-904)(Wei, 2001: 454-460) و تبدیل مرتب (Xiangdong, et al, 2008:64-68) به تنهایی نمی‌تواند بر روی تصویر اجرا شوند؛ زیرا در بسیاری از قسمت‌های تصویر رمز شده، همبستگی بین پیکسل‌ها همچنان وجود دارد. از شبکه‌های اتصالی امگا[5] در تولید پردازنده‌های چند هسته‌ای استفاده می‌شود و تاکنون از ساختار این شبکه در رمزنگاری تصویر استفاده نشده است.

1. Rivest-Shamir-Adleman (RSA)
2. Data Encryption Standard (DES)
3. Inserting
4. Scrambling
5. Omega

در این مقاله ابتدا مختصری در مورد شبکه‌های اتصالی درونی بحث شده است؛ پس از آن، ضمن معرفی شبکه‌ی اتصالی امگا، سعی شده است از ابزار شبکه‌های اتصالی امگا برای رمزنگاری تصاویر خاکستری استفاده شود و محاسن و معایب این ابزار با سایر روش‌های قبلی مقایسه شود.

۲- شبکه اتصالی درونی بین پردازنده و حافظه

واژه‌ی پردازنده موازی برای یک رایانه با بیش از یک پردازنده تعریف می‌شود. سامانه‌هایی با هزاران پردازنده از این قبیل به نام سامانه‌های شدیداً موازی[1] نامیده می‌شوند.

پردازنده‌های چندهسته‌ای اخیر برای ایجاد سامانه‌های موازی، بسیار مناسب هستند؛ در نتیجه، پردازنده‌های موازی وجود دارند که به آن‌ها ذرات بزرگ در مقابل ذرات کوچک گفته می‌شود. این تقسیم-بندی به اندازه پردازنده برمی‌گردد (Tachmazidis, et al, 2014:1-8).

انواع مختلفی از پردازنده‌های موازی وجود دارد. وجه تمایز آنها، نوع اتصال داخلی بین پردازنده‌ها و یا اتصال بین پردازنده‌ها و حافظه‌ها است؛ هم‌چنین پردازنده‌های موازی به متقارن[2] و نامتقارن[3] تقسیم می‌شوند. در سامانه چند پردازنده‌ای نامتقارن، یک پردازنده برای اجرای سامانهٔ عامل و پردازنده‌های دیگر برای اجرای برنامه‌های کاربران استفاده می‌شود. در سامانه چند پردازنده‌ای متقارن، سامانهٔ عامل می‌تواند روی هر یک از پردازنده‌های آزاد یا روی تمام پردازنده‌ها به‌صورت هم‌زمان اجرا شود. طراحی و ساخت‌های متنوعی برای پردازش موازی انجام گرفته است که شبکه اتصالی امگا یکی از نمونه‌های آن است.

خواص ازدحام حافظه، به مالتی پروسسورها و ویژگی شبکه اتصالی درونی بین پردازنده و حافظه بستگی دارد. حافظه اشتراکی داخل بخش‌های چندگانه به نحو زیادی ازدحام حافظه را کاهش می‌دهد؛ اما تراکم و انباشتگی ممکن است در ارتباطهای سخت‌افزاری حتی هنگامی که پردازنده‌ها به بخش‌های متفاوتی رجوع می‌کنند، اتفاق افتد.

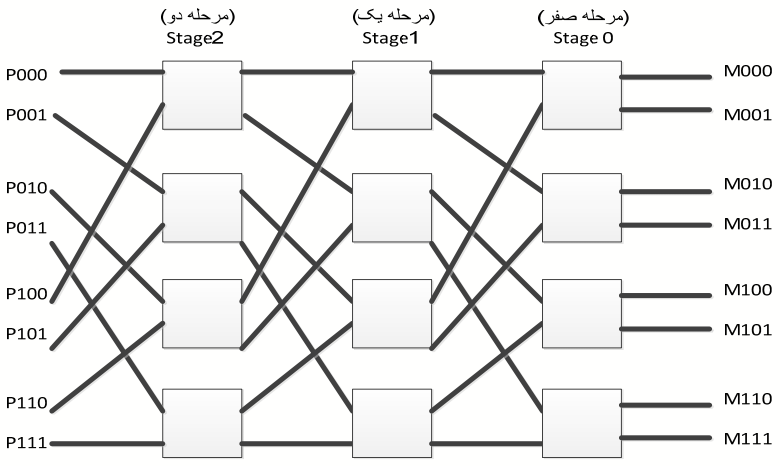
یک شبکه عرضی ارتباطی بین ۸ پردازنده و ۸ پودمان حافظه را در نظر بگیرید؛ هر پودمان حافظه می‌تواند در یک لحظه، تنها به یک درخواست سرویس دهد؛ بنابراین درخواست‌های هم‌زمان به یک پودمان حافظه توسط چندین پردازنده منجر به ازدحام حافظه خواهد شد. شبکه عرضی دارای خواص مهمی است که باعث می‌شود ازدحام در شبکه اتصالی درونی هرگز روی ندهد. شبکه عرضی می‌تواند همه پردازنده را به

1. Massively Parallel
2. Symmetric Multi-Processing
3. Asymmetric Multi Processing

طور هم‌زمان به حافظه‌های مختلف متصل کند. سوییچ‌ها می‌توانند به گونه ای تنظیم شوند تا اجـازه دهنـد که هر الگوی ممکن از ارتباطات پردازنده و حافظه، به طور هم‌زمان اتفاق افتند.

برای n پردازنـده از n پودمـان حافظـه شـبکه‌ی عرضـی، نیـاز بـه n^2 سـوئیچ اسـت؛ بنـابراین دارای هزینه $O(n^2)$ است. اگر تعداد پردازنده‌ها زیاد باشد، هزینه $O(n^2)$ مقرون به‌صرفه نیست. بـرای کـاهش این هزینه، شبکه‌های بسیاری با هزینه $O(n \log n)$ توسعه داده شده‌اند که از جمله آن‌ها می‌توان به شـبکه امگا – که در شکل ۱ نشان داده شده است – اشاره کرد.

شبکه‌ی اتصالی امگا یک شبکه‌ی چند مرحله‌ای است که در آن P پردازنده به P حافظه متصـل شـده است. در شبکه‌ی امگا $\frac{p}{2}\log(p)$ سوییچ قرار داد. بعد از هر مرحله، تابع شافل[1] روی خروجی‌های آن اعمال می‌شود به طور مثال در شکل۱– ۸ پردازنده به ۸ واحد حافظـه متصـل شـده اسـت. بـدیهی اسـت در ایـن شبکه $\frac{8}{2}\log(8) = 12$ سوییچ وجود خواهد داشت. پردازنده‌ها از صفر تا ۸ شماره‌گذاری مـی‌شـوند و در تـابع شافل از سه بیت استفاده می‌شود. در داخل هر مرحله مسیریابی انجام می‌شود و اطلاعات از یک حافظـه‌ی مشخص به یک پردازنده‌ی مشخص فرستاده می‌شود.



شکل۱– شبکه‌ی اتصالی امگا

1. Shuffle

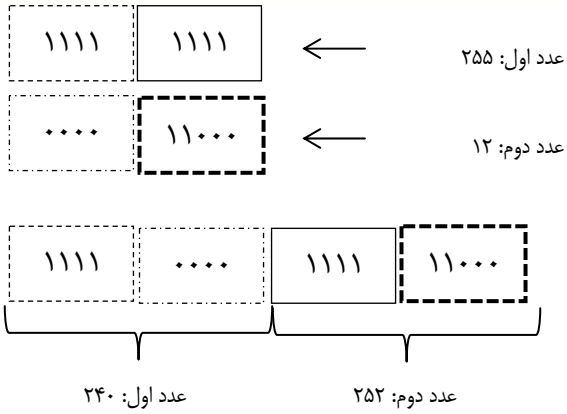
۳- الگوریتم پیشنهادی

در این مطالعه، از ساختار شبکه‌ی اتصالی امگا برای جاگذاری محتوای پیکسل‌های تصویر استفاده می‌شود. اندازه‌ی تصویر استفاده شده ۲۵۶×۲۵۶ است؛ بنابراین کل تصویر به $(256 \times 256) / 8 = 8192$ قالب با اندازه‌ی ۸×۱ تقسیم می‌شود. در ادامه اعداد ۱ تا ۸۱۹۲ به صورت تصادفی در یک ماتریس قرار داده می‌شود. این ماتریس «جعبه جانشانی» نامیده می‌شود. در این ماتریس، عنصر تکراری وجود نخواهد داشت. این ماتریس که به صورت تصادفی پُر شده است، شماره قالب‌هایی که باید به شبکه اتصالی امگا ارسال شوند را در بردارد. در این مقاله از یک شبکه اتصالی امگا با $p=8$ و شماره پردازنده‌های سه بیتی با هشت ردیف استفاده شده است. هشت عدد متوالی از ماتریس جعبه جانشانی خوانده می‌شود و به شبکه اتصالی امگا ارسال می‌شوند.

برای درک بهتر، ادامه‌ی الگوریتم با ذکر مثال شرح داده خواهد شد. انتخاب اعداد بر اساس خطوط رسم شده‌ی شافل در شبکه‌ی امگا خواهد بود. پیکسل‌های $C(2,1)=255$ و $C(3,2)=12$ را در نظر بگیرید؛ محتوای پیکسل‌ها، اعداد ۲۵۵ و ۱۲ به صورت دو دویی نوشته می‌شوند، چهار بیت پر ارزش دو دویی ۲۵۵ یادداشت می‌شود. سپس چهار بیت پر ارزش ۱۲ در کنار چهار بیت قبلی نوشته می‌شود؛ هم‌چنین چهار بیت باقی‌مانده ۲۵۵ و چهار بیت باقی‌مانده‌ی ۱۲ پشت سرهم یادداشت می‌شود و در پایان معادل هشت بیتی نتیجه به صورت ده‌دهی نمایش داده می‌شود. برای درک بهتر این قسمت به شکل‌های ۲ و ۳ مراجعه شود. حال باید اعداد به دست آمده با محتوای اصلی پیکسل‌ها جایگزین شوند؛ بنابراین محتوای پیکسل $C(2,1)$ با عدد ۲۴۰ و محتوای پیکسل $C(3,2)$ با عدد ۲۵۲ جایگزین خواهند شد. این روند طبق خطوط رسم شده‌ی شافل برای تمام پیکسل‌های ستون‌های یک با دو، سه با چهار و پنج با ششِ ماتریس C انجام می‌شود. این فرآیند طبق خطوط رسم شده‌ی ستون هفت با هشت پیاده خواهد شد و ماتریس D به‌دست می‌آید.

۲۵۴	۲۵۰	۱۰۶	۴۵	۲۰۰	۱۰	۲۵۰	۱۰
۲۵۵	۸	۴۸	۵۵	۲۱۵	۱۵	۲۱۶	۱۶۶
۱۶	۱۲	۲۵۴	۷۵	۴۵	۳۳	۲۱۵	۴۱
۱۱۸	۱۰۰	۲۵۵	۶۱	۶۴	۷۲	۲۰۰	۲۱۰
۵۰	۲۵۵	۲۵۵	۲۵	۲۱۰	۴۱	۱۰۶	۲۳
۲۵۴	۲۰۰	۲۱۰	۲۰۵	۲۵۴	۲۵۴	۵۰	۱۴
۲۴۰	۲۱۰	۲۰۰	۷۳	۷۰	۲۵۵	۲۳۴	۶۲
۱۹	۸۰	۱۶۷	۱۷۹	۶۰	۲۵۵	۱۱۴	۷۰

شکل ۲- ماتریس C



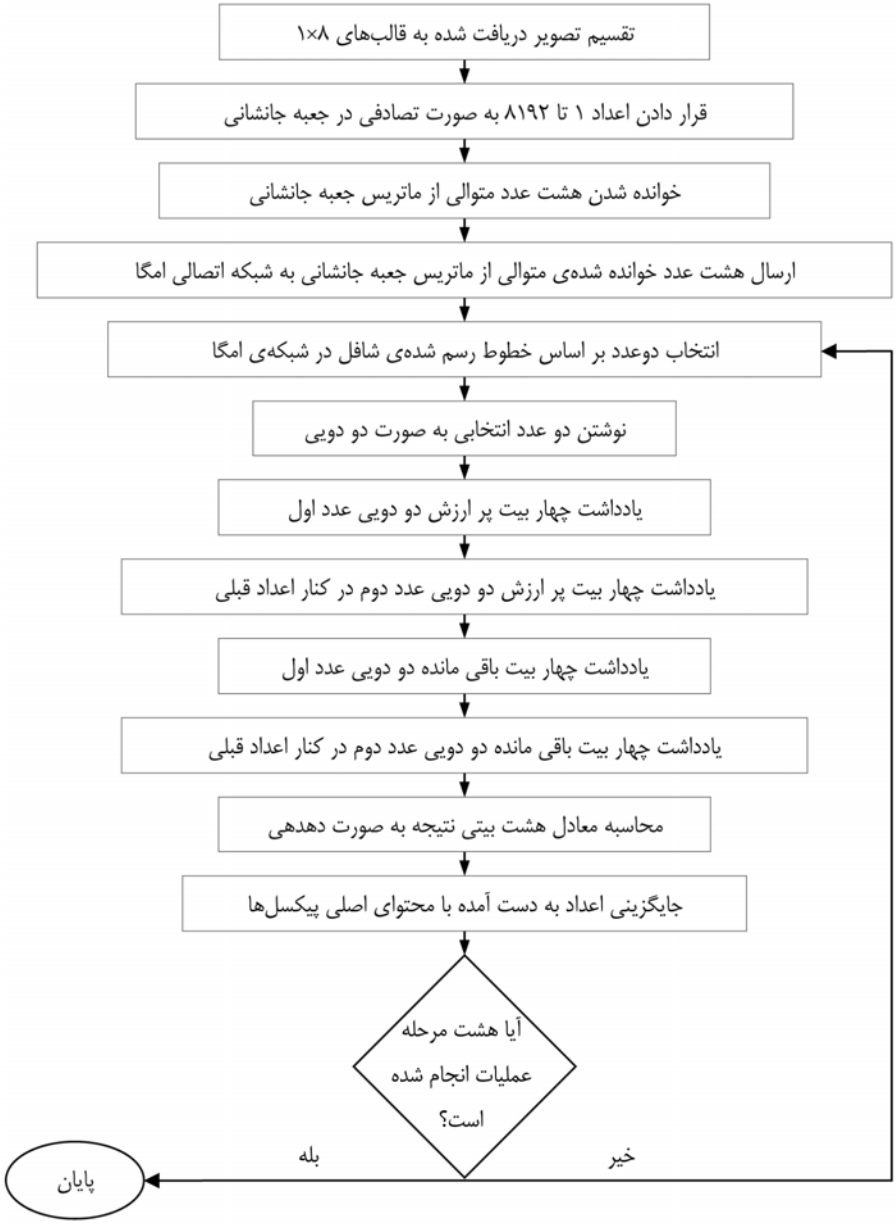
شکل ۳- نحوه‌ی چینش اعداد

طبق شکل ۱ در مرحله‌های صفر، یک و دو، بیت هشتمِ پیکسل‌های ستون‌های دوم، چهارم و ششم مکمل[1] می‌شوند. به طور نمونه اگر بیت هشتمِ D(3,2)=۲۵۲ مکمل شود، حاصل عدد ۱۲۴ خواهد بود. با انجام عملیات فوق یک ماتریس ۸×۸ به دست می‌آید، این ماتریس E نامیده می‌شود. حال سطر اول ماتریس E به جای قالب شماره ۱۴ قرار داده می‌شود؛ هم‌چنین سطر دوم ماتریس E به جای قالب شماره ۵ قرار داده می‌شود. به همین ترتیب محتویات پیکسل‌های قالب‌های شماره ۱۰۱-۵۱۰-۷-۷۶۳-۲۰۰-۱۱۳ با سطرهای سوم تا هشتم ماتریس E جابه‌جا می‌شوند. مراحل فوق تا زمانی که کل قالب‌ها جابه‌جا شوند تکرار می‌شوند. روند نمای الگوریتم پیشنهادی در شکل ۴ نمایش داده شده است.

اگر الگوریتم پیشنهادی بر روی تصویر مرد عکاس اعمال شود، شکل ۵ به‌دست خواهد آمد. همان طور که در شکل ۵ مشخص است برخی از قسمت‌ها به خوبی درهم‌ریخته نشده‌است که برای رفع این مشکل، تصویر به دست آمده را شیفت چرخشی داده و مراحل فوق دوباره اعمال می‌شود. تعداد شیفت‌های چرخشی که به تصویر داده می‌شود دارای اهمیت است، شکل ۵ به ۸ بخش تقسیم شده است. طول تصویر اولیه ۲۵۶ در نظر گرفته شده بود؛ بنابراین برای این تصویر ۳۲ ستون شیفت چرخشی داده می‌شود و مجدداً مراحل الگوریتم بر روی آن اعمال می‌گردد تا تصویر به خوبی درهم‌ریخته شود. پس از اتمام مراحل فوق، سطرها و ستون‌های زوج با یکدیگر جابه‌جا می‌شوند. شکل ۶ نتیجه‌ی به‌دست آمده از اجرای دو بار تکرارِ الگوریتم پیشنهادی بر روی تصویر مرد عکاس را نشان می‌دهد. همان طور که مشاهده می‌شود تصویر به

1. Complement

خوبی درهم‌ریخته شده است. لازم به ذکر است برای رمزگشایی تصویر معکوس، کارهای انجام شده بـرای رمزگذاری انجام می‌شود.



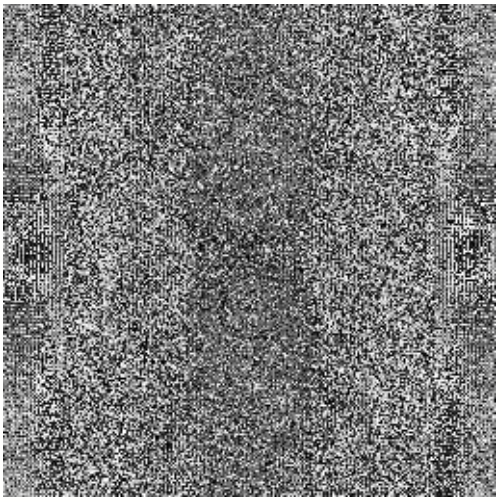
شکل ٤- روند نمای الگوریتم پیشنهادی

٤- تحلیل الگوریتم پیشنهادی با آزمون بصری

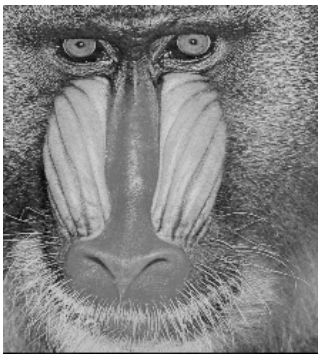
این الگوریتم برای چندین تصویر مانند میمون و فلفل‌ها انجام شد که نتایج خروجی در شکل‌های ۸ الی ۹ دیده می‌شوند. با ملاحظه‌ی این شکل‌ها می‌توان فهمید که تصاویر به‌خوبی رمز شده‌اند.

شکل ٥- تصویر استاندارد مرد عکاس

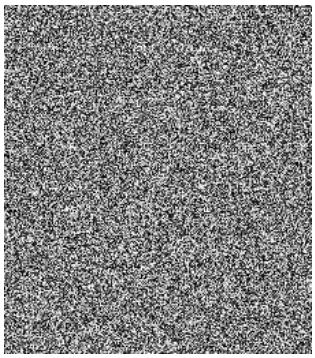
شکل ٦- نتیجه پس از اجرای یک بار تکرارِ الگوریتم



شکل ۷- نتیجه پس از اجرای دو بار تکرارِ الگوریتم



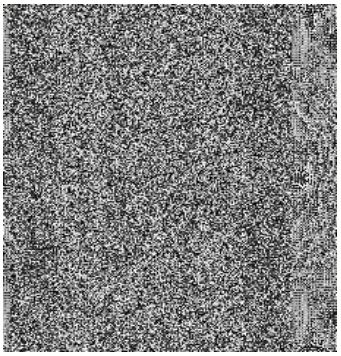
الف: تصویر اصلی



ب: تصویر رمزشده

شکل ۸: تصویر میمون

الف : تصویر اصلی



ب: تصویر رمزشده

شکل ۹: تصویر فلفل‌ها

۵- تحلیل الگوریتم پیشنهادی با آزمون تحلیل همبستگی

در داده‌ی تصویری، هر پیکسل با پیکسل‌های همسایه‌ی خود همبستگی دارد.

یک الگوریتم رمزنگاری فوق العاده باید تصاویر رمز شده‌ای تولید کند که همبستگی بین پیکسل‌های آن کم باشد (Rakesh, et al, 2012:49-57). در جدول ۲ همبستگی بین پیکسل‌ها در سه راستای افقی، عمودی و

قطری بر روی تصویر مرد عکاس (شکل ۵) بررسی شده است. معیار همبستگی در رابطه‌ی ۱ بیان شده است. مقادیر معیارهای اندازه‌گیری برای پنج الگوریتم در جدول ۱ ارائه شده است. بدیهی است توابع ذکر شده، توابع استاندارد برای محاسبه‌ی میزان تشابه دو تصویر هستند (Rakesh, et al,2012:49-57).

$$r_{xy} = \frac{Cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (۱)$$

$$Cov(x,\ y) = \frac{1}{M \times N} \times \sum_{j=1}^{M \times N} ((x_j - \frac{1}{M \times N} \sum_{j=1}^{M \times N} x_j)(y_j - \frac{1}{M \times N} \sum_{j=1}^{M \times N} y_j)) \quad (۲)$$

$$D(x) = \frac{1}{M \times N} \sum_{j=1}^{M \times N} (x_j - \frac{1}{M \times N} \sum_{j=1}^{M \times N} x_j)^2 \quad (۳)$$

$$D(y) = \frac{1}{M \times N} \sum_{j=1}^{M \times N} (y_j - \frac{1}{M \times N} \sum_{j=1}^{M \times N} y_j)^2 \quad (۴)$$

در این روابط x و y روشنایی دو پیکسل همسایه در تصویر و $M \times N$ تعداد پیکسل‌های تصویر است. رابطه‌ی ۵ محاسبه‌ی MAE [1] است که متوسط خطای مطلق است(Jolfaei, Mirghadri,2010:213-220) (Willmott, Matsuura, 2005:79-82) (Hyndman, Koehler,2006:1-8). $C(i,j)$ و $P(i,j)$ به ترتیب مقادیر پیکسل‌های تصویر رمز و تصویر اصلی هستند.

$$MAE = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} |C(i,j) - P(i,j)| \quad (۵)$$

رابطه‌ی ۶ مربوط به محاسبه NPCR [2] است که نرخ پیکسل‌های تغییریافتهٔ تصویر رمز، به ازای یک بیت تغییر در تصویر اصلی است (Wong, Kwok, 2009:2652-2663) (Ye, Zhao, 2012:41-45) (Wu And et al, 2011:1-23). به طور کلی ممکن است کاربرِ غیر مجاز با تغییر یک پیکسل از تصویر رمز شده به یک رابطه معنی‌دار بین تصویر اصلی و تصویر رمزشده برسد، سپس با تغییر یک پیکسل مهم از تصویر رمزشده، رمزگشایی را در طرف گیرنده دچار اختلال کند.

از مقادیر UACI [3] و NPCR برای محاسبه‌ی میزان وابستگی بین تصویر اصلی و تصویر رمزشده استفاده می شود. هر چه نتایج به دست آمده از محاسبه‌ی UACI و NPCR بیش‌تر باشد، یعنی وابستگی کم‌تری بین تصویر اصلی و تصویر رمز شده وجود دارد. در رابطه ۷، c و $\bar{c}$ دو تصویر رمز شده

1. Mean Absolute Error (MAE)
2. Number of Pixel Change Rate (NPCR)
3. Unified Average Changing Intensity (UACI)

$$NPCR=\frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}D(i,j)}{M\times N}\times 100\% \quad (۶)$$

$$D(i,j)=\begin{cases}0 & \text{if} \quad C(i,j)=\overline{C}(i,j)\\ 1 & \text{if} \quad C(i,j)\neq\overline{C}(i,j)\end{cases} \quad (۷)$$

هستند که تصاویر اصلی متناظرشان در یک پیکسل متفاوت هستند. نحوه محاسبه‌ی UACI در رابطه ۸ نشان داده شده است (Wu, et al, 2011:1-23) (Wong, Kwok, 2009:2652-2663).

$$UACI=\frac{1}{M\times N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left[\frac{\left|C(i,j)-\overline{C}(i,j)\right|}{255}\right]\times 100\,\% \quad (۸)$$

هر چه مقدار UACI، NPCR و MAE بیش‌تر باشد الگوریتم رمزنگاری، عملکرد بهتری دارد. مقادیر جدول ۱ نشان می‌دهد که معیار UACI، NPCR و MAE روش پیشنهادی از سه روش دیگر بیش‌تر است؛ هم‌چنین تحلیل همبستگی برای مقایسه‌ی بصری در شکل‌های ۱۱ الی ۱۴ نتایج رمزنگاری تصویر با سه دنباله‌ی فوق آشوبی، لجستیک، TD-ERCS و الگوریتم پیشنهادی مشاهده می‌شود. با مشاهده‌ی تصاویر ۱۱ الی ۱۴ مشخص می‌شود الگوریتم پیشنهادی همانند سایر الگوریتم‌ها توانسته است به گونه‌ای تصویر را درهم‌ریزی نماید که محتویات تصویر رمز شده هیچ اطلاعاتی از تصویر اصلی به ما ندهد. هر الگوریتم رمزنگاری دارای یک کلید رمز است. کلید رمز کلیدی است که با استفاده از آن، داده‌ی رمز شده رمزگشایی می‌شود. خوب است که اگر الگوریتم رمزنگاری شناسایی شد، کلید یا کلیدهای رمز، قابل حدس زدن نباشند. برخی از الگوریتم‌های رمزنگاری دارای دوره‌ی تناوب هستند، یعنی بعد از تکرار الگوریتم، تصویر رمزگشایی می‌شود. بدیهی است هر چه طول کلید رمز بزرگ‌تر باشد الگوریتم دارای امنیت بالاتری است.

الگوریتم پیشنهادی دارای سه کلید رمز «اندازه‌ی تصویر اولیه»، «جعبه جانشانی» و «P» در شبکه‌ی امگا است، بنابراین با توجه به بزرگ بودن طول کلید، روش پیشنهادی از امنیت مناسبی برخوردار است.

جدول ۱ـ معیارهای اندازه‌گیری

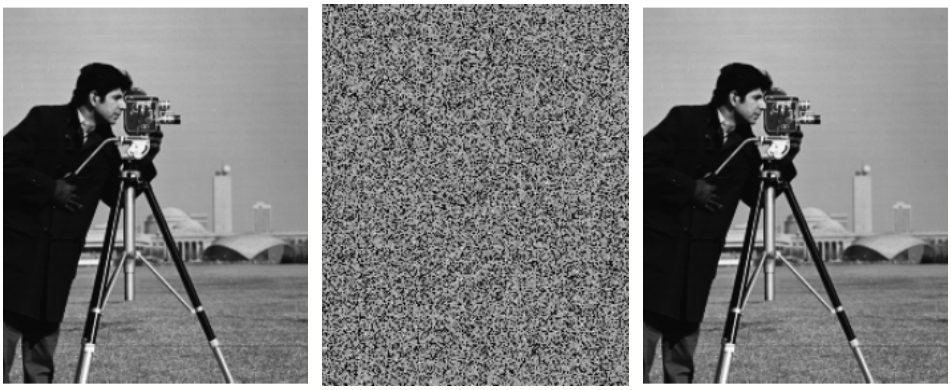
نام الگوریتم ارزیابی شده	UACI	MAE	NPCR
دنباله فوق آشوبی (Gu, Han,2006:3729-3733)	۱۳/۲۴۴۱٪	۴۹/۲۴۱۶ ٪	۳۳/۶۸۵۵٪
دنباله لجستیک (Ye,2010:347-354)	۱۳/۲۳۵۴٪	۴۹/۲۸۷۴٪	۳۳/۶۸۶۹٪
دنباله TD-ERCS (Feng-ying, Cong-xu,2011:186-191)	۱۳/۲۴۲۴٪	۴۹/۵۹۲۶٪	۳۳/۷۰۵۰٪
دنباله الگوریتم ژنتیک (طالبی و لطیف،۱۳۹۳: ۶۹–۷۸)	۱۳/۲۶۷۳٪	۳۳/۹۱۲٪	۴۹/۶۴۹٪
تبدیل آرنولد (Che-S, et al ,2008:495-499)	۱۲/۶۴۴۲٪	۳۲/۲۴۰۴٪	۵۰/۸۷۲۸٪
تبدیل فیبوناچی (Jiancheng ,et al,2004)	۳/۲۱۰۶٪	۸/۱۸۴۷٪	۶۹/۴۵۸۰٪
تبدیل مرتب (Xiangdong, et al ,2008:64-68)	۲۶/۷۸۲۳٪	۶۸/۲۹۲۴٪	۹۸/۹۸۳۸٪
الگوریتم پیشنهادی	۳۱/۴۲۳۴٪	۸۰/۵۴۸۳٪	۹۹/۶۲۳۱٪

جدول ۲ـ تحلیل همبستگی

تابع همبستگی	افقی	عمودی	قطری
تصویر اصلی مرد عکاس	۰/۹۵۶۲	۰/۹۵۶۴	۰/۹۳۷۳
تصویر رمز فوق آشوبی	۰/۶۶۹۳	۰/۶۷۰۴	۰/۶۶۸۱
تصویر رمز لجستیک	۰/۶۶۵۷	۰/۶۶۷۱	۰/۶۶۶۲
تصویر رمز TD-ERCS	۰/۶۶۸۵	۰/۶۶۶۸	۰/۶۶۵۳
الگوریتم ژنتیک	۰/۶۶۵۸	۰/۶۶۵۵	۰/۶۶۵۸
تبدیل آرنولد	۰/۹۳۷۸	۰/۹۲۲۹	۰/۹۵۵۱
تبدیل فیبوناچی	۰/۹۷۹۵	۰/۹۵۹۸	۰/۹۵۶۳
تبدیل مرتب	۰/۷۱۸۷	۰/۷۳۶۴	۰/۶۶۰۶
الگوریتم پیشنهادی	۰/۶۱۰۱	۰/۶۰۱۷	۰/۵۹۷۵

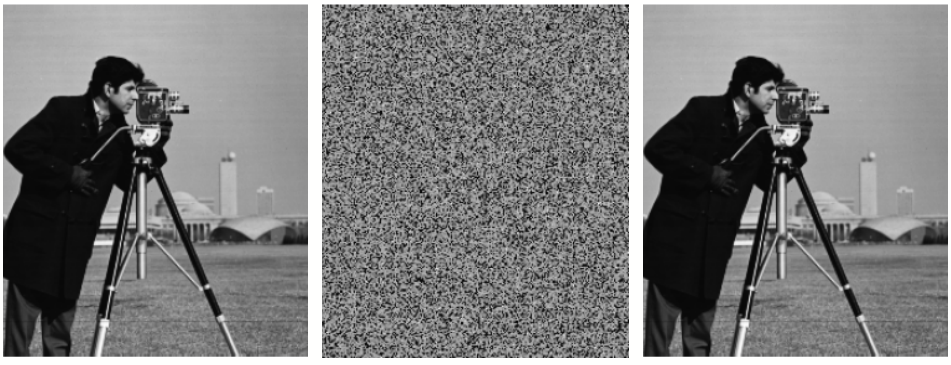
الف: تصویر اصلی ب : تصویر رمز شده ج : تصویر رمزگشایی شده

شکل ۱۰ـ رمزنگاری و رمزگشایی با دنباله فوق آشوبی



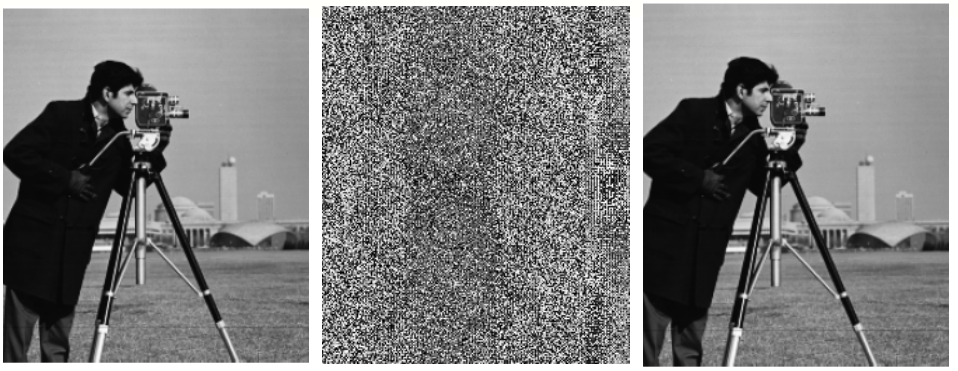
الف: تصویر اصلی ب : تصویر رمز شده ج : تصویر رمزگشایی شده

شکل ۱۱ـ رمزنگاری و رمزگشایی با دنباله‌ی لجستیک



الف: تصویر اصلی ب : تصویر رمز شده ج : تصویر رمزگشایی شده

شکل ۱۲ـ رمزنگاری و رمزگشایی با دنباله‌ی TD-ERCS



الف: تصویر اصلی ب : تصویر رمز شده ج : تصویر رمزگشایی شده

شکل ۱۳ـ رمزنگاری و رمزگشایی با الگوریتم پیشنهادی

٦- نتیجه‌گیری

در این مقاله، یک الگوریتم جدید برای رمزنگاری تصاویر سطوح خاکستری معرفی شد و در این الگوریتم ابتدا تصویر، قالب‌بندی می‌شود؛ سپس با استفاده از شبکه‌ی اتصالی پروانه‌ای، قالب‌ها به‌هم‌ریخته می‌شوند. به منظور ارزیابی، الگوریتم پیشنهادی توسط آزمون‌هایی استاندارد، ارزیابی شد. الگوریتم پیشنهادی توانست تصویر را به گونه‌ای درهم بریزد که تصویر اولیه قابل حدس زدن نباشد. نتایج آزمون تحلیل همبستگی نشان داد که بین پیکسل‌های تصویر رمز شده همبستگی در سه راستای افقی، عمودی و قطری به طور متوسط در حد ۰/۱۷۲۵، ۰/۱۷۸۹ و ۰/۱۷۴۳کاهش داده شده است. برای سنجش میزان تمایز بین تصویر اصلی و تصویر رمز شده، از سه معیار MAE، NPCR و UACI استفاده شد. نتایج آزمایش‌ها نشان می‌دهد روش پیشنهادی علاوه بر داشتن کیفیت بصری مناسب، معیارهای خطای NPCR، MAE و UACI را به طور متوسط به ترتیب در حد ۴۶/۷۶۰۱ ، ۳۹/۰۱۲۴ و ۱۷/۷۶۲۵ کاهش داده است. نتایج عددی به‌دست آمده نشان داد، روش پیشنهادی از مطلوبیت خوبی برخوردار است.

کتابنامه

طالبی نوش آبادی، زهره و لطیف، علی‌محمد، (۱۳۹۳)، ***ارائه روشی نوین برای تولید دنباله بازگشتی در رمزنگاری تصویر با استفاده از الگوریتم ژنتیک*** – *مجله هوش محاسباتی در مهندسی برق*– شماره ۲– صفحات ۶۹–۷۸.

Ding.W, Yan.W & Qi.D. (2000). Digital Image Scrambling. *Progress In Natural Science*,Vol. 11, Pp.7-14.

Wei. D, Wei-Qi.Y & Dong-Xu.Q.(1999). Digital Image Scrambling Technology Based On Gray Code. *The International Conference On Computer Aided Design & Computer Graphics*, Vol. 3. Pp.900-904.

Che.S, Che.Z & Ma.B.(2008). An Improved Image Scrambling Algorithm. *Second International Conference On Genetic And Evolutionary Computing* ,Pp.495-499.

Pareek. N.K, Vinod .P & Sud.K.K.(2006). Image Encryption Using Chaotic Logistic Map. *The Journal Of Image And Vision Computing*, Vol .24, Pp. 926-934.

Kanso. A & Ghebleh.M.(2012). A Novel Image Encryption Algorithm Based On A 3D Chaotic Map. *Nonlinear Science And Numerical Simulation*, Vol .17, Pp. 2943-2959.

Rakesh. S, Ajitkumar. A .Kaller, Shadakshari. B. C & Annappa .B.(2012). Image Encryption Using Block Based Uniform Scrambling And Chaotic Logistic Mapping. *International Journal On Cryptography And Information Security*, Vol .2, Pp. 49-57.

Jolfaei. A & Mirghadri .A. (2010). Survey: Image Encryption Using Salsa20. *International Journal Of Computer Science Issues*, Vol. 5, Pp. 213-220.

Hyndman.R. J. & Koehler. A. B. (2006). Another Look At Measures Of Forecast Accuracy, *International Journal Of Forecasting*.

Willmott.C.J & Matsuura.K .(2005). Advantages Of The Mean Absolute Error (MAE) Over The Root Mean Square Error (RMSE) In Assessing Average Model Performance. *Climate Research Clim Res*,Vol .30, Pp.79-82.

Ye. R & Zhao. H. (2012) . An Efficient Chaos Based Image Encryption Scheme Using Affine Modular Maps. *International Journal Of Computer Network And Information Security*,Vol .4, Pp.41-45.

Wong.K.W & Kwok.B.S.H .(2009). An Efficient Diffusion Approach For Chaos-Based Image Encryption .*Chaos Solitons & Fractals*,Vol.41,Pp. 2652-2663.

Wu.Y , Noonan.J.P & Agaian.S.(2011). Shannon Entropy Based Randomness Measurement And Test For Image Encryption . *Journal Of Information Sciences*.Pp.1-23.

Gu. G.S. & Han. G.Q.(2006). The Application Of Chaos And DWT In Image Scrambling. *IEEE Conference On Industrial Electronics And Applications*, Pp. 3729 – 3733.

Ye. G.(2010). Image Scrambling Encryption Algorithm Of Pixel Bit Based On Chaos Map. *Pattern Recognition Letters*, Vol .31, Pp.347-354.

Feng-Ying. H & Cong-Xu .Z.(2011). An Novel Chaotic Image Encryption Algorithm Based On Tangent-Delay Ellipse Reflecting Cavity Map System. *Procedia Engineering*, Vol. 23, Pp. 186-191.

Tachmazidis.I, Cheng.L, Kotoulas.S, Antoniou.G & Ward.T.E.(2014). Massively Parallel Reasoning Under The Well-Founded Semantics Using X10. *In Submission.*

Jiancheng. Z, Ward. R.K. & Dongxu.Q.(2004). A New Digital Image Scrambling Method Based On Fibonacci Numbers, *In Proceedings Of The International Symposium On Circuits And Systems*,Vol 3.

Ying.W, Zhao.Z & Lelin. Z.(2007). A Fault-Tolerable Encryption Algorithm For Two-Dimensional Digital Image, *IEEE Conference On Industrial Electronics And Applications*, P.2737 - 2741.

Wei. D, Wei-Qi.Y & Dong-Xu.Q.(1999). Digital image scrambling technology based on gray code, *the International Conference on Computer Aided Design & Computer Graphics, Wen Hui Publishers*, Vol 3. p.900-904.

Wei. D.(2001). Digital Image Scrambling, *Progress In Natural Science Journal*, Vol 11, P.454-460.

Xiangdong. L, Junxing.Z, Jinhai.Z & Xiqin.H.(2008). Image Scrambling Algorithm Based On Chaos Theory And Sorting Transformation, *International Journal Of Computer Science And Network Security*, Vol 8, P. 64-68.

Che.S, Che.Z & Ma.B.(2008), An Improved Image Scrambling Algorithm, *Second International Conference on Genetic and Evolutionary Computing*, p.495-499.

Jiancheng. Z, Ward. R.K. & Dongxu.Q.(2004), A new digital image scrambling method based on Fibonacci numbers, *in Proceedings of the International Symposium on Circuits and Systems,*Vol 3.

Xiangdong. L, Junxing.Z, Jinhai.Z & Xiqin.H.(2008), Image scrambling algorithm based on chaos theory and sorting transformation, *International Journal of Computer Science and Network Security*, Vol 8, p. 64-68.