تاریخ دریافت مقاله: ۹۷/۰۳/۳۱
تاریخ پذیرش مقاله: ۹۷/۰۷/۲۹

رمزگذاری تصویر با استفاده از فشرده‌سازی فرکتالی و نگاشت هنون

دلاور زارعی*
مدرس مرکز علمی کاربردی شهرداری اردبیل،اردبیل،ایران
پست الکترونیکی: zareai@ardabilcity.ir

محمد قربانی اشرف
کارشناس حفاظت فناوری اطلاعات بانک کشاورزی استان اردبیل، اردبیل، ایران
پست الکترونیکی: mg_223460@yahoo.com

چکیده

در ایـــن مقاله یک طرح جدید برای حفظ امنیت داده‌های تصویری توســـط رمزگذاری تصویر با استفاده از روش فشرده‌سازی فرکتالی تصویر و نگاشت هنون برای حفاظت از تبـــادل تصاویر دیجیتال به طریقـــی کارآمد و امن ارائه شده است. به منظور بررســـی میزان کارآمدی طرح ارائه شـــده آن را با استفاده از یکســـری آزمون‌ها و مقایسه‌ها می‌سنجیم. این آزمون‌ها عبارتند از: آزمون بصری، تحلیل فضـــای کلید، تحلیل نمودار پیشـــینه‌نما، آنتروپی اطلاعات و تحلیل حساســـیت نســـبت به کلید. این روش با استفاده از فشرده‌ســـازی فرکتالی تصویر ابتدا تصویر را فشرده می‌کنـــد. پارامترهای حاصل از این فشرده‌ســـازی در یک ماتریس ذخیره می‌شود. با اســـتفاده از نگاشت هنون این پارامترها رمزگذاری می‌شود. نتیجه به‌صورت یک تصویر رمزگذاری شـــده نمایش داده می‌شـــود. نتایج آزمایش‌ها، کارایی روش پیشـــنهادی را در بالا بـــردن امنیت داده‌های تصویری نشـــان می‌دهند. کیفیت تصویر رمزگشایی شده نیز با محاســـبه حداکثر نســـبت ســـیگنال به نوفه به‌دست می‌آید. در روش پیشنهادی این عدد برابر۳٤/۲٤۷ به‌دست آمده است که در مقایسه با مرجع[۱۵] که برابر عدد۳۳/۱۵٦ می‌باشد، ۱/۰۹۱ رشد داشته است.

واژه‌هـــای کلیـــدی: امنیـــت، رمزگـــذاری، فرکتـــال، فشرده‌سازی تصویر، نگاشت

مقدمه

رمزنگاری دانش تغییـــر دادن متن پیام به کمک کلید و الگوریتم رمزگذاری است، به‌صورتی که تنها شخصی که از کلید و الگوریتم مطلع است قادر به استخراج متن اصلی از متن رمزشده باشد و شخصی که از یک یا هردوی آن‌ها اطلاعی ندارد، نتواند به محتوای پیام دسترســـی پیدا کند. رمزگذاری ازطریق پنهان نگاه داشـــتن الگوریتم، منســـوخ اســـت. در روش‌های جدید رمزگذاری فرض بر آن اســـت که همگان الگوریتم را می‌دانند؛ آنچه پنهان است فقط کلید است[۱]. رمزنگاری علمی اســـت که به وسیله آن می‌توان اطلاعات را به‌صورتی امن منتقل کرد حتی اگر مسیر انتقال اطلاعـــات (کانال‌های ارتباطی) ناامن باشـــد. دریافت کننده اطلاعات آن‌ها را از حالت رمـــز خارج می‌کند. به این عمل در واقع رمزگشائی گفته می‌شود.

فرکتال درباره اشـــکال یا فرآیندهایی بحث می‌کند که

* نویسندهٔ مسئول

دارای خواص مقیاس‌پذیر باشند. شکل‌های فرکتال دارای این خاصیت هستند که اگر مقیاس را در مورد آن‌ها تغییردهیم شکلی مشابه حاصل خواهدشد. نمونه‌های طبیعی و واقعی از فرکتال‌ها مانند شش‌های انسان، درختان، ابرها، کوه‌ها، یا برگ برخی از درختان مانند برگ سرخس واز آن قبیل می‌توان ارائه کرد. اصطلاح فرکتال نخستین بار توسط مندلبرات در سال ۱۹۷۰ ابداع گردید. مندلبرات وقتی که بر روی تحقیقی پیرامون طول سواحل انگلیس مطالعه می‌کرد به این نتیجه رسید که این طول هرگاه با مقیاس بزرگ اندازه گرفته شود بیشتر از حالتی است که از مقیاس کوچک‌تر استفاده شود. از لحاظ واژه، مندلبرات اصطلاح فرکتال[1] را از واژه لاتین fractus به معنای سنگی که به شکل نامنظم شکسته شده باشد گرفت تا بر ماهیت بی‌نظمی و قطعه قطعه شونده که از مشخصه اصلی این فرم است، تاکید داشته باشد.

فرهنگستان زبان فارسی واژه برخال را برای فرکتال جایگزین نموده است. در این هندسه اشکالی مورد بررسی قرار می‌گیرند که بسیار نامنظم به نظر می‌رسند. اما اگر با دقت به شکل نگاه کنیم متوجه می‌شویم که تکه‌های کوچک آن کم و بیش شبیه به کل هستند. به عبارتی جزء در این اشکال، نماینده‌ای از کل است، به چنین اشکالی نام خودمتشابه[2] نیز می‌دهند.

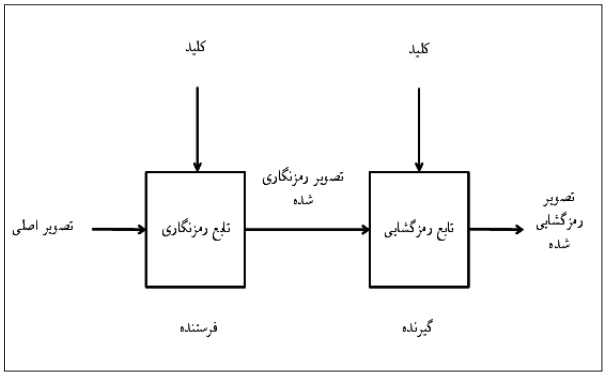
هدف از فشرده‌سازی تصاویر، کاهش افزونگی[3] محتویات عکس می‌باشد. به زبان دیگر، فشرده‌سازی تصویر یعنی ذخیره‌سازی آن به‌صورت مجموعه‌ای از تبدیلات. میزان کاهش ظرفیت یک فایل به عوامل متعددی نظیر نوع فایل، اندازه فایل، روش و الگوریتم استفاده شده توسط برنامه فشرده‌سازی بستگی دارد. فشرده‌سازی عکس می‌تواند به‌صورت بدون اتلاف و پر اتلاف (اتلافی، با فقدان، با زیان، ضایعاتی) صورت گیرد.

در سال‌های اخیر الگوریتم‌های متنوعی در زمینه رمزگذاری تصویر، پیشنهاد شده‌اند. دو نکته اساسی در الگوریتم‌های رمزگذاری تصویر، سرعت و امنیت می‌باشد. با رشد سریع تولیدات چندرسانه‌ای و پخش گسترده محصولات دیجیتالی بر روی اینترنت محافظت از اطلاعات دیجیتالی در برابر کپی و توزیع غیرمجاز، هر روز اهمیت بیشتری پیدا می‌کند. برای رسیدن به این هدف الگوریتم‌های گوناگونی برای رمزگذاری تصویر پیشنهاد شده است.

امنیت یکی از ارکان حیاتی موجودات زنده و احساس امنیت یکی از اساسی‌ترین نیازهای نوع بشر است. امروزه با گسترش وسایل ارتباطی و حجم اطلاعات مبادله شده در شبکه‌های رایانه‌ای که از آن به‌عنوان انفجار اطلاعات یاد شده است، بر لبه یک انقلاب بزرگ در زمینه امنیت اطلاعات چند رسانه‌ای قرار گرفته‌ایم. امنیت رسانه‌های دیجیتال یکی از مسائل مهم و مطرح جامعه رمزگذاری در دنیای امروز می‌باشد. با توجه به کاربرد روزافزون رایانه و گسترش زیرساخت‌های ارتباطی از جمله شبکه‌های سیار و اینترنت، حفظ محرمانگی و تایید صحت تصاویر روز به روز اهمیت بیشتری می‌یابد.

در این مقاله یک روش برای حفظ امنیت داده‌های تصویر ارائه شده است. این روش با استفاده از فشرده‌سازی فرکتالی تصویر ابتدا تصویر را فشرده می‌کند. پارامترهای حاصل از این فشرده‌سازی در یک ماتریس ذخیره می‌شوند. با استفاده از نگاشت هنون این پارامترها رمزگذاری می‌شوند. نتیجه به‌صورت یک تصویر رمزگذاری شده نمایش داده می‌شود. نتایج آزمایش‌ها، کارایی روش پیشنهادی را در بالا بردن امنیت داده‌های تصویری نشان می‌دهند. شیوه ارزیابی، مقایسه تصویر اصلی با تصویر رمزگشایی شده می‌باشد. داده‌های مورد استفاده برای آزمایش تصاویر استاندارد پایگاه داده آموزشی مرجع[۱۵]، یعنی لنا، قایق، و باربارا می‌باشد. یک معیار ارزیابی مورد استفاده PSNR می‌باشد که میزان اختلاف بین کیفیت تصویر اصلی و تصویر رمزگشایی شده را ارائه می‌دهد. هر قدر این معیار عدد بزرگتری باشد به معنی اختلاف کمتر بین تصویر اصلی و تصویر رمزگشایی شده می‌باشد و این به منزله

1-Fractal
2-Self-similar
3-Redundancy



شکل۱- نمودار یک سیستم رمزگذاری

کارایی روش رمزگذاری هست. مقدار PSNR محاسبه شده برای الگوریتم پیشنهادی برای تصویر لنا برابر با ۳٤/۲٤۷ می‌باشد که در مقایسه با تصویر لنا در مرجع[۱۵] که برابر عدد۳۳/۱۵٦ می‌باشد،۱/۰۹۱ رشد داشته است.

در ادامه تعریف کلی از مسئله رمزگذاری و رمزگذاری فشرده شده فرکتالی ارائه خواهد شد. بعد از آن به کارهای مرتبط اخیر پرداخته می‌شود و روش پیشنهای و ارزیابی آن بیان شده و در پایان نتیجه‌گیری خواهد شد.

۲- تعریف مسئله

شانون[۲] اولین کسی بود که سیستم ارتباطات پوشیده را از دیدگاه نظریه اطلاعات بررسی کرد. او ارتباطات پوشیده را در سه گروه دسته‌بندی کرد: سیستم‌های پوشیده، سیستم‌های محرمانه، سیستم‌های رمزگذاری. هدف سیستم‌های رمزگذاری اطلاعات، اختفاء محتویات پیام است و نه به‌طور کلی وجود پیام، در حقیقت شخص سوم از وجود پیام سری آگاه است ولی با توجه به رمزگذاری شدن آن قادر به شناسایی پیام نمی‌باشد. در شکل۱ نمودار یک سیستم رمزگذاری ساده نشان داده شده است.

در بررسی PSNR مربوط به تصویر لنا در مرجع[۱۵] با توجه به پایین بودن مقدار عددی، مشخص است که کیفیت تصویر رمزگشایی شده نسبت به تصویر اصلی پایین‌تر است. لذا مسئله اصلی در این است که با توجه به کیفیت پایین تصویر رمزگشایی شده، روشی برای رمزگذاری ارائه شود تا علاوه بر افزایش امنیت رمزگذاری، کیفیت تصویر رمزگشایی شده نیز نسبت به تصویر مرجع[۱۵] بهبود یابد.

در این مقاله یک روش رمزگذاری تصویر فشرده شده فرکتالی برای افزایش امنیت رمزگذاری تصویر ارائه شده است. این روش از سه مرحله فشرده‌سازی، رمزگذاری و رمزگشایی تشکیل شده است. در مرحله فشرده‌سازی، از روش فشرده‌سازی فرکتالی استاندارد استفاده شده است. در مرحله رمزگذاری از نگاشت هنون برای رمزگذاری نمودن انواع پارامترهایی که از مرحله فشرده‌سازی به‌دست آمده است، استفاده می‌کنیم. در نهایت پارامترهای رمز شده را به‌صورت عکس رمز شده نمایش می‌دهیم. در این مرحله با استفاده از نگاشت آرنولد کت نظم پیکسل‌ها را به هم می‌زنیم و عکس رمز شده نهایی به‌دست می‌آید. در مرحله رمزگشایی بعد از به‌دست آوردن پارامترهای تصویر رمز، معکوس نگاشت آرنولد کت[٤] و معکوس نگاشت هنون[٥] را بر روی تصویر اعمال می‌کنیم و پارامترهای رمزگشایی شده و در نهایت از روی این پارامترها تصویر فشرده رمزگشایی شده به‌دست می‌آید.

۳- کارهای مرتبط

رمزگذاری چند رسانه‌ای به معنی استفاده از الگوریتم‌های رمزگذاری برای حفظ امنیت اطلاعات چند رسانه‌ای است. محتوای اطلاعات چند رسانه‌ای با استفاده از الگوریتم رمزگذاری و یک کلید، رمزگذاری می‌شود. به‌طورمشابه اطلاعات رمزگذاری شده با استفاده از الگوریتم رمزگشایی و کلید، رمزگشایی می‌شود. فناوری رمزگذاری چند رسانه‌ای اولین بار در سال ۱۹۸۰ به‌وجود آمد و در نیمه دوم سال ۱۹۹۰ به یکی از مهم ترین موضوعات تحقیقاتی تبدیل شد. توسعه این روش را می‌توان به سه بخش، رمزگذاری اطلاعات خام، رمزگذاری

4-Arnold Cat Map
5-Henon Map

اطلاعات فشـرده شـده و رمزگذاری جزئی تقسـیم کرد. روش‌های زیر تکنیک‌های اسـتفاده شـده اخیر در زمینه رمزگذاری می‌باشند.

۳-۱- رمزگذاری مبتنی بر توابع آشوب

آشـوب پدیده‌ای اسـت که در سیسـتم‌های غیرخطی تعریـف پذیـر رخ می‌دهـد، حساسـیت زیاد نسـبت به شـرایط اولیه دارد و رفتار شـبه‌تصادفی از خود نشـان می‌دهد. نخسـتین بار شـانون ایده اسـتفاده از آشوب را در رمزگـذاری مطرح کـرد[۳]. در سـال ۱۹۹۷، با هدف طراحـی یک روش رمزگذاری بلوکی متقارن، طرحی برای تطبیق یک نگاشـت آشـوبگون دو بعدی معکوس‌پذیر بر روی یک حلقه یا یک مربع، پیشـنهاد داده شـده است[٤]. در مقاله [٥] در سـال ۱۹۹۸ یک روش رمزگذاری تصویر مبتنی بر جریان‌های کلموگورف آشـوبگون طراحی شد . در سـال ۲۰۰۰ روشـی را تحت عنوان الگوریتم مبتنی بر کلید آشـوب (CKBA) ارائه دادند[٦]. این الگوریتم، در ابتدا براسـاس یک نگاشت آشوب، یک سری زمانی تولید کرده و سـپس آن سـری زمانی را برای ایجاد یـک کلید دنباله دودویی به‌کار می‌برد. در سـال ۲۰۰۲ طرحی براسـاس یک سیسـتم آشـوب دیجیتال چندگانه ارائه کردند[۷]. در مقاله[۸]پیشـنهاد کردند که پیکسل‌های تصویر با استفاده از نگاشت‌های آشـوبی به‌صورت یک‌سویه نگاشت شوند تا یک شبکه نگاشت آشـوبی(CML) تشکیل دهند. تصویر رمزگذاری شده از طریق تکرار CML همراه با پارامترهای محرمانه سـامانه و تعداد دور به‌دسـت می‌آید. یک روش رمزگذاری تصویر با اسـتفاده از دو نگاشـت لجستیک و یک کلید خارجی در مقاله[۹] ارائه شـده است. یک سامانه رمزگذاری تصویر مبتنی بر آشوب سریع با معماری رمز جریانی پیشـنهاد کردند[۱۰]. در مقاله[۱۱] پیشنهاد شد که یک طرح رمزگذاری تصویر بایستی شامل دو مرحله تکرار شونده باشد: انتشار و اغتشاش. از یک نگاشت آشوبی دو بعدی برای جایگشـت مکان پیکسل‌ها و از سامانه آشوبی گسسـته چن، برای پنهان کردن مقادیر پیکسل‌ها استفاده کردند[۱۲]. در مقاله[۱۳] از یک نگاشت استاندارد دو بعدی در فاز جانشـانی و از یک نگاشت لجستیک در فاز انتشار استفاده کردند.

علاوه بر مـوارد فوق، کارهای دیگـری هم در زمینه رمزگذاری به روش نگاشـت‌های آشوب انجام شده است که همگی آن‌ها سطح امنیتی مطلوبی را در اختیار می‌گذارند و این از ذات سیستم‌های آشوب سرچشمه می‌گیرد.

۳-۲- فشرده‌سازی فرکتالی و رمزگذاری تصویر

در سـال ۲۰۱۱، مقالـه[١٤] روش رمزگذاری تصویر فشـرده شـده فرکتالی را ارائه داد. او در این روش بعد از فشرده‌سازی تصویر و استخراج پارامترهای آن از بین پنج پارامتر فقط رمزگذاری دو پارامتر روشنایی و کنتراست را با استفاده از مدل زنجیره‌ای لیان پیشنهاد داد.

در سال ۲۰۱۲، روش رمزگذاری مبتنی بر آشوب برای رمزگذاری تصویر ارائه شـده اسـت[۱۵]. در این مقاله از روش فشرده‌سازی فرکتالی برای کم کردن حجم تصویر و اسـتفاده از مدل آشوب رنی برای تولید رمز و کلید رمز استفاده شده است.

۴- روش پیشنهادی

گام‌های طرح پیشـنهادی رمزگذاری و رمزگشایی به ترتیب زیر می‌باشد:

۱- فشرده‌سازی فرکتالی تصویر اصلی
۲- رمزگذاری پارامترهای حاصل از مرحله اول
۳- بر هم زدن نظم پیکسل‌ها
٤- تصویر فشرده رمزگذاری شده نهایی
٥- رمزگشایی تصویر

در ایـن روش پیشـنهادی ابتـدا تصویر اصلـی را با اسـتفاده از روش اسـتاندارد به ترتیب زیر فشرده‌سازی فرکتالی می‌کنیم:

الگوریتـم کار به این صورت اسـت که فرض کنید یک تصویر ۲۵٦×۲۵٦ داریم، ایـن تصویر را به مربعات ۲×۲ بدون همپوشـانی تقسـیم می‌کنیم و آن‌ها را Ri می‌نامیم،

بنابراین ۱۶۳۸٤ قطعه خواهیم داشت. حال برای یافتن بخشی از تصویر که شبیه به Ri باشد، تمام ماتریس‌های ٤×٤ با همپوشانی را در کل تصویر جستجو می‌کنیم و آن‌ها را D مخفف Domain می‌نامیم و پس از کوچک‌نمایی آن‌ها به اندازه ۲×۲، برای هر کدام یک کنتراست و شدت روشنایی به‌دست می‌آوریم. سپس یک تبدیل خودالحاقی با توجه به معیار انطباق تعریف شده، برای هر قطعه، از بین بلوک‌های دامنه و دوران‌های آن‌ها که عبارتند از: خود بلوک، دوران ۹۰ درجه، دوران ۱۸۰ درجه، دوران ۲۷۰ درجه، انعکاس حول محورy ها، انعکاس حول محور x ها، انعکاس حول محورy=x، انعکاس حول محورy=-x، به‌دست می‌آوریم. بدین ترتیب مناسب ترین بلوک دامنه جستجو می‌شود. برای هر قطعه، شماره بلوک دامنه مناسب و اطلاعات لازم برای به‌دست آوردن آن بلوک از روی آن بلوک دامنه ذخیره می‌شود. به این ترتیب فشرده‌سازی انجام می‌گیرد زیرا به جای ذخیره هر قطعه پارامترهای آن ذخیره می‌گردد. اگر با توجه به ضرایب به‌دست آمده خطای D و Ri کمتر از آستانه قابل قبول باشد، شماره سطر و ستون پیکسل اول D به همراه ضرایب شدت روشنایی، کنتراست و تبدیل خودالحاقی برای قطعهٔ مورد نظر ذخیره خواهد شد. در غیر این‌صورت جستجو در دامنه‌های باقیمانده ادامه می‌یابد.

مزیت این روش قابلیت بازسازی تصویر در هر اندازه‌ای بدون از دست دادن وضوح می‌باشد. بازسازی نسبتا ساده این روش نیز از مزایای دیگر آن است.

روابط محاسبه شدت روشنایی، کنتراست و خطا:

$$S = \frac{n^2(\sum_{i=1}^{n} a_i b_i) - (\sum_{i=1}^{n} a_i)(\sum_{i=1}^{n} b_i)}{n^2 \sum_{i=1}^{n} a_i^2 - (\sum_{i=1}^{n} a_i)^2} \qquad (۱)$$

$$O = \frac{\sum_{i=1}^{n} b_i - s \sum_{i=1}^{n} a_i}{n^2}$$

$$R = \frac{\sum_{i=1}^{n} b_i^2 + S(S\sum_{i=1}^{n} a_i - 2(\sum_{i=1}^{n} a_i b_i) + 2O\sum_{i=1}^{n} a_i) + O(On^2 - 2\sum_{i=1}^{n} b_i)}{n^2}$$

و اگر $n^2 \sum_{i=1}^{n} a_{i=1}^2 - (\sum_{i=1}^{n} a_i)^2 = 0$ آنگاه $S=0$ و $O = \sum_{i=1}^{n} \frac{b_i}{n^2}$ است. در روابط بالا a_i پیکسل‌های دامنه، b_i پیکسل‌های برد،n تعداد پیکسل‌های سطر یا ستون، O شدت روشنایی و S کنتراست هستند[۱٦].

با توجه به این‌که به جای خود تصویر، پارامترهای حاصل از مرحله فشرده‌سازی، رمزگذاری می‌شود، این کار خود باعث افزایش امنیت داده رمزگذاری شده می‌شود. چون اگر کسی بخواهد تصویر را رمزگشایی کند باید اول تشخیص دهد که چه چیزی و چه پارامترهایی رمزگذاری شده است و این پارامترها از کجا آمده‌اند. برهم زدن نظم پیکسل‌ها در روش پیشنهادی افزایش امنیت را دو چندان می‌کند.

فشرده‌سازی روش پیشنهادی شبیه فشرده‌سازی روش مرجع[۱۵] می‌باشد. بر هم زدن نظم پیکسل‌ها در روش پیشنهادی جهت افزایش امنیت اضافه شده است. در مرجع[۱۵] از مدل آشوب رنی برای تولید رمز و کلید رمز استفاده شده است ولی در روش پیشنهادی از نگاشت هنون استفاده می‌شود. لذا روش‌های رمزگذاری در مرجع[۱۵] و روش پیشنهادی کاملاً متفاوت می‌باشند. افزایش امنیت و کیفیت تصویر رمزگشایی شده از مزایای روش پیشنهادی می‌باشد. اساس روش پیشنهادی بر فشرده‌سازی فرکتالی و رمزگذاری پارامترهای حاصل از آن استوار است. یکی از بخش‌هایی که با کار در آن حوزه می‌توان بهبودهایی را در کارایی روش پیشنهادی ایجاد کرد، تلاش برای کاهش زمان اجرا می‌باشد. البته استفاده از کامپیوترهایی با پردازنده‌های قوی و قدرتمند می‌تواند تا حدودی سرعت الگوریتم را بالا ببرد.

٤-۱- تابع رمزگذاری

نگاشت هنون یک نگاشت دو بعدی معکوس پذیر است که در سال ۱۹۷٦ توسط هنون معرفی شده است. این نگاشت یک نمونه ساده شده نگاشت پوانکاره برای معادلات لورنز می‌باشد. نگاشت هنون به‌عنوان روشی برای تولید دنباله‌های شبه تصادفی معرفی شده است. نگاشت دو بعدی هنون به‌صورت زیر تعریف می‌شود:

$$\begin{cases} x_{n+1} = 1 + y_n - \alpha x_n^2 \\ y_{n+1} = \beta x_n, \end{cases} \qquad (۲)$$

به این صورت که(x_0,y_0) نقطه شـروع و زوج (x,y) یک حالت دو بعدی سـامانه می‌باشـد. هنگامی که α=1/4 و β=0/3 باشد، سامانه در حال آشوب می‌باشد. هنون نشان داد که اگر شـرایط اولیه در ناحیـه S، که در محدوده‌های (۰/۴۲، ۱/۳۳-)، (۰/۱۳۳، ۱/۳۲)، (۰/۱۴-، ۱/۲۴۵) و (۰/۵-، ۱/۰۶-) تعریف شده است، انتخاب شود آنگاه نقاط حاصـل از تکرار نگاشـت، یعنی(x_i,y_i) بـرای i≥۱ نیز در محدوده S قرار می‌گیرد. برای هر مقدار (x_i,y_i) در S دنباله نقاط به این جاذب همگرا می‌شوند و در طول تکرار نگاشت بر روی آن باقی می‌مانند.

٤-۲- برهم زدن نظم پیکسل‌ها

اطلاعات تصویر یا همان پیکسـل‌ها همبستگی بسیار زیادی به یکدیگر دارند. تحلیل‌هـای آماری بر روی تعداد زیادی تصویر نشـان داده‌اند که به‌طور متوسـط ۸ تا ۱۶ پیکسل به‌صورت عمودی، افقی و مورب با یکدیگر مرتبط هستند. به منظور برهم زدن همبستگی پیکسل‌ها در تصویر اصلی، از روش زیر استفاده می‌کنم:

2D Arnold Cat Map: اگر تصویر اولیه را N×N فرض کنیم و رابطه زیر را برای تمامی پیکسل‌های تصویر به‌کار ببریم، مختصات جدید هر پیکسل به دست خواهد آمد:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} modN \qquad (۳)$$

در رابطـه فـوق p و q مقادیر صحیح مثبت هسـتند. (x, و y,) مختصات جدید پیکسل (xو y) می‌باشد. همان‌طور که انتظار داریم در این روش به دلیل این‌که فقط مکان نقاط تغییر می‌یابند و مقادیر سـطوح خاکستری ثابت می‌ماند، هیستوگرام تصویر اصلی و تصویر رمزگذاری شده کاملا مشابه یکدیگرهستند.

٤-۳- نظریهٔ رمزگشایی

در این مرحله ابتدا تصویر رمزگذاری شده را به‌عنوان ورودی دریافت می‌کنیم. سپس معکوس عملیات برهم زدن نظم پیکسل‌ها را بر روی تصویر رمز شده انجام می دهیم. در این مرحله یک تصویر جدید حاصل می‌شـود. معکوس تابـع رمزگذاری را بـر روی پارامترهای تصویر فرکتالی فشرده شده اعمال می‌کنیم. سـپس برای بازیابی تصویر روند زیررا دنبال می‌کنیم.

$$Range = Domain \times S + O \qquad (٤)$$

۵- ارزیابی روش پیشنهادی

در این مقاله، جهت مقایسـه کارایی و میزان مطلوبیت روش پیشـنهادی، امنیـت روش پیشـنهادی را با سـایر روش‌های متداول و کارآمد مورد مقایسه قرار داده‌ایم.

۵-۱- محیط پیاده سازی

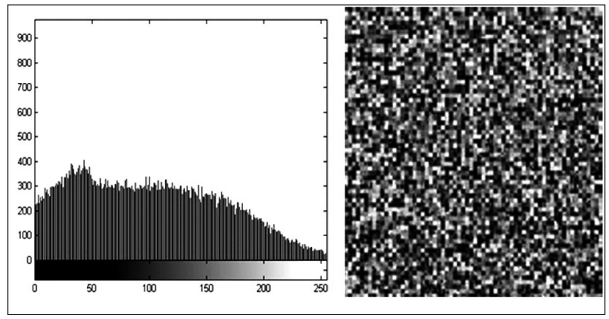
طـرح پیشـنهادی رمزگذاری تصویر فشـرده شـده فرکتالـی در یک برنامـه در محیط برنامه نویسـی متلب Version v,10,0,499(R2010a) در کامپیوتـر شـخصی بـا پردازشـگر IntelCore(TM)i5 و حافظه ٤GB و تحت ویندوز ۳۲ بیتی ۷ اجرا شده است.

تصاویر اسـتاندارد ۲۵٦×۲۵٦ به نام‌های لنا، باربارا و قایق با این طرح رمزگذاری و رمزگشـایی شـده‌اند. برای ارزیابی عملکرد طرح پیشنهادی رمزگذاری تصویر فشرده شده فرکتالی با رمزگذاری تصویر فشرده شده در مرجع [۱۵] مقایسـه شـده است. نتایج مقایسـه در قسمت های بعدی آمده است.

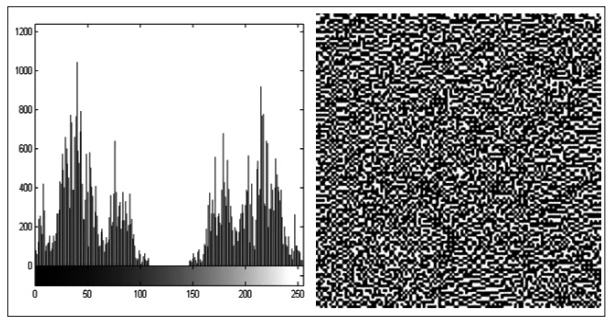
۵-۲- پایـگاه داده (داده‌هـای مـورد اسـتفاده برای آزمایش) [۱۵]

یکی از جنبه‌های مهم هر کار ارزیابی کارایی پایگاه داده به کار رفته در آزمایش‌ها می‌باشد. هدف ما استفاده از یک پایگاه داده تصاویر، شـامل انـواع تصاویر با پیچیدگی و بافت‌های متنوع است. همچنین استاندارد بودن و شناخته شـده بودن آن پایگاه داده نیز اهمیت دارد. چون زمانی که کارهای قبلی نیز از آن پایگاه اسـتفاده کرده باشند، نتایج حاصل قابل اسـتنادتر می‌باشـند. همان‌طور که ذکر شد، برای مقایسـه روش‌های رمزگذاری، ما به تصاویر متنوع از لحاظ بافت و پیچیدگی و دسترس پذیر بودن نیازمندیم.

شکل۳- تصاویر استاندارد پایگاه داده آموزشی (لنا، باربارا، قایق) [۱۵]



شکل ۴: تصویر رمز شده و هیستوگرام آن با کلید های
Key1= (-1.23555656465656565,
0.31565646466546654653)
Key2= (-0.9985474987648123456,
0.295565657913056454541)



شکل ۵: تصویر رمز گشایی شده و هیستوگرام آن با کلید های(غیر صحیح)
Key1= (-1.23555656465656565 ,
0.31565646466546654653)
Key2= (-0.9985474987648123456,
0.295564657913056454541)

در این کار برای مقایسه و ارزیابی روش ارائه شده با سایر روش‌ها به جهت امنیت تصویر رمزگذاری شده، چند تصویر استاندارد را به‌عنوان پایگاه داده آموزشی انتخاب کردیم. زیرا این تصاویر قابل دسترس است و در برخی کارهای قبلی نیز مورد استفاده قرار گرفته است.

برای هماهنگی با کارهای پیشین تمام تصاویر به تصاویر سطح خاکستری با اندازه ۲۵۶×۲۵۶ تبدیل شده‌اند.

۵-۳- حساسیت به کلید

یک رویّه پنهان‌سازی تصویر مناسب باید نسبت به تغییرات کوچک کلید حساس باشد. بدین معنی که تغییر یک بیت در کلید باید سبب ایجاد یک نتیجه بسیار متفاوت شود. نتایج به دست آمده نشان می‌دهد که این روش نسبت به تغییراتی هر چند کوچک در کلید، حساسیت بالایی را نشان می‌دهد. حساسیت بسیار بالا نسبت به کلید، امنیت سامانه رمزگذاری را در برابر حملات تا حدی تضمین می‌کند.

برای آزمودن میزان حساسیت نسبت به کلید طرح رمزگذاری مورد مطالعه، تصویر مورد آزمایش یکبار با استفاده از کلید محرمانه اصلی و یکبار با استفاده از کلید محرمانه کمی تغییر یافته، رمزگذاری می‌شود. اگر مقایسه این دو تصویر رمزی به‌صورت بصری امکان پذیر نباشد، آنگاه طرح رمزگذاری مورد مطالعه نسبت به کلید حساسیت بالایی دارد. از آنجا که مقایسه دو تصویر از طریق مشاهده کاری دشوار است، لذا برای مقایسه بهتر می‌توان درصد پیکسل‌های متمایز دو تصویر رمزی با کلیدهای متفاوت را محاسبه کرد.

هر چه مقدار این محاسبه به ۱۰۰٪ نزدیک تر باشد، آنگاه حساسیت نسبت به کلید بیشتر است. برای تحلیل حساسیت نسبت به کلید، تصویر استاندارد لنا به وسیله سامانه رمزگذاری مورد مطالعه، با استفاده از مجموعه کلیدهای اصلی و مجموعه کلیدهای کمی متفاوت، رمزگذاری شد. شکل‌های ٤ و ٥ نتیجه آزمون حساسیت به کلید را نشان می‌دهد. تشخیص تفاوت بین تصاویر رمزی به‌صورت بصری کاری دشوار است. لذا نمودار پیشینه‌نما تصاویر ترسیم شده است تا قیاس آسان‌تر شود.

جدول۱- مقایسه PSNR تصاویر رمزگشایی شده با کلید صحیح در طرح پیشنهادی و مقایسه با مرجع[۱۵]

نام تصویر	لنا	لنا[۱۵]	قایق	باربارا
اندازه تصویر	۲۵۶×۲۵۶	۲۵۶×۲۵۶	۲۵۶×۲۵۶	۲۵۶×۲۵۶
نوع تصویر	خاکستری	خاکستری	خاکستری	خاکستری
PSNR	۳۴/۲۴۷	۳۳/۱۵۶	۳۲/۵۹۷	۳۱/۷۱۲

PSNR -۵-٤

یک معیار ارزیابی مورد استفاده PSNR می‌باشد که میزان اختلاف بین کیفیت تصویر اصلی f(x,y) و تصویر رمزگشایی شده g(x,y) را ارائه می‌دهد. رابطه زیر این معیار را نشان می‌دهد.

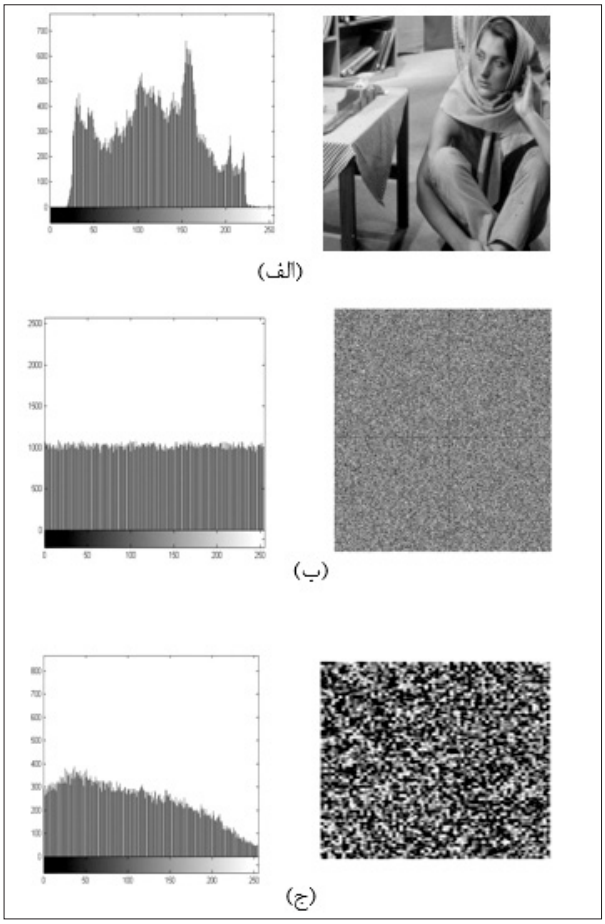
$$PSNR=10log_{10}\frac{255^2}{MSE} \qquad (۵)$$

$$MSE=\frac{\sum_{i=0}^{m-1}\sum_{i=0}^{n-1}(f(i,j)-g(i,j))^2}{m*n}$$

که در این رابطه m و n ابعاد تصویر می‌باشند. این رابطه میزان قدرت یک سیگنال به نوفه آن را نشان می‌دهد. در اینجا منظور از نوفه مجموع مربعات خطای بین تصویر اصلی و تصویر رمزگشایی شده می‌باشد. هر قدر این معیار عدد بزرگ‌تری باشد به معنی اختلاف کمتر بین تصویر اصلی و تصویر رمزگشایی شده می‌باشد و این به منزله کارایی روش رمزگذاری است [۱۷]. مقدار PSNR محاسبه شده برای الگوریتم پیشنهادی برابر با ۳٤/۲٤۷ می‌باشد. (جدول ۱)

۵-۵- تحلیل نمودار پیشینه‌نمای تصویر

نمودار پیشینه‌نما، تعداد پیکسل‌ها در هر سطح خاکستری را برای یک تصویر نشان می‌دهد. در این نمودار محور افقی بیانگر سطوح خاکستری که از ۰ تا ۲۵۵ می‌باشد و محور عمودی فراوانی پیکسل‌ها را مشخص می‌نماید. اگر چه با داشتن این نمودار نمی‌توان به تصویر اصلی رسید اما این نمودار حاوی اطلاعات مفیدی از قبیل میزان روشنایی و تیرگی تصویر، میزان کنتراست تصویر و... می‌باشد که مورد استفاده رخنه‌گران و مهاجمان قرار



شکل۶- (الف) تصویر باربارا و نمودار پیشینه‌نما
(ب) تصویر رمزگذاری شده باربارا و نمودار پیشینه‌نما
(ج) تصویر فشرده و رمزگذاری شده باربارا و نمودار پیشینه‌نما

می‌گیرد. برای جلوگیری از نشت اطلاعات و جلوگیری از حملات مهاجمان، مهم است که تضمین شود که تصویر اصلی و تصویر رمزی هیچ گونه تشابه آماری ندارند. الگوریتم رمزگذاری تصویر بایستی به گونه‌ای باشد که هیچ نوع سرنخی برای حمله آماری ندهد. به‌طور کلی می‌توان نشان داد که هر چه نمودار پیشینه‌نما تصویر یکنواخت‌تر باشد امکان وقوع حملات آماری بر روی آن کمتر خواهد بود.

همان‌طور که در شکل ٦ به وضوح قابل مشاهده است نمودار پیشینه‌نما تصویر رمزگذاری شده، یک نمودار پیشینه‌نمای یکنواخت است. این ویژگی باعث می‌شود هیچ گونه مدرکی برای موفقیت حملات آماری در دست رخنه‌گران نباشد و طرح پیشنهادی از این نظر امن می‌باشد.

جدول۲- مقایسه آنتروپی تصاویر فشرده رمزگذاری شده در طرح پیشنهادی

باربارا	قایق	لنا	نام تصویر
۲۵۶×۲۵۶	۲۵۶×۲۵۶	۲۵۶×۲۵۶	اندازه تصویر
خاکستری	خاکستری	خاکستری	نوع تصویر
۷/۹۹۳	۷/۹۸۶	۷/۹۸۹	آنتروپی

۵-۶- آنتروپی اطلاعات

آنتروپی یکی از خصوصیات برجسته برای تصادفی بودن است .آنتروپی اطلاعات یک نظریهٔ ریاضی برای ارتباط داده‌ای و ذخیره‌سازی است که در سال ۱۹۴۹ توسط کلود شانون معرفی شده است. یکی از معروفترین فرمول‌ها برای به دست آوردن آنتروپی به‌صورت زیر است:

$$H(s) = \sum_{i=0}^{2^N-1} P(s_i)\, log_2 \frac{1}{P(s_i)} \qquad (٤)$$

که در آن N برابر با تعداد سطح خاکستری استفاده شده در تصویر (در تصاویر ۸ بیتی برابر با ۲۵٦ خواهد بود) و $P(S_i)$ نشان دهنده احتمال وقوع سطح خاکستری i ام در تصویر خواهند بود. در تصاویری که به‌طور کامل تصادفی ایجاد شده است این مقدار برابر با ۸ خواهد بود که این مقدار به‌عنوان ایده‌آل در نظر گرفته می‌شود. هر چقدر مقدار به دست آمده برای آنتروپی در یک روش به ۸ نزدیک‌تر باشد به این معنی خواهد بود که امکان پیش‌بینی‌پذیری این روش کمتر و در نتیجه امنیت این روش بالاتر خواهد بود. جدول شماره ۲ نتایج آنتروپی را در روش پیشنهادی نشان می‌دهد.

۶- نتیجه گیری

هدف اصلی در حوزه رمزگذاری بر افزایش امنیت و سرعت استوار است. مسئله‌ای که مطرح است بالابردن امنیت در کمترین زمان ممکن است. در دهه اخیر علم رمزگذاری تصویر در رسانه‌های دیجیتال پیشرفت چشمگیری داشته است و روش‌ها و الگوریتم‌های متنوعی در این زمینه ارائه شده است. در این مقاله یک روش جدید برای بالا بردن امنیت داده‌های تصویری ارائه شده است. روش‌های رمزگذاری سعی دارند داده‌های تصویری را به طریقی امن رمزگذاری کنند که کسی نتواند داده اصلی را از آن استخراج کند.

در این مقاله روشی پیشنهاد شده است که با انجام یکسری عملیات روی داده تصویری، آن را رمزگذاری می‌کند. در مرحله اول چون تصویر را به‌صورت فرکتالی فشرده می‌کنیم حجم تصویر تا حد زیادی کاهش پیدا می‌کند و این یکی از مزایای طرح پیشنهادی محسوب می‌شود. در مرحله دوم با توجه به این‌که به جای خود تصویر، پارامترهای حاصل از مرحله فشرده‌سازی رمزگذاری می‌شود، این کار خود باعث افزایش امنیت داده رمزگذاری شده می‌شود. چون اگر کسی بخواهد تصویر را رمزگشایی کند باید اول تشخیص دهد که چه چیزی و چه پارمترهایی رمزگذاری شده است و این پارامترها از کجا آمده‌اند. استفاده از نگاشت هنون با توجه به حساسیت بالای آن نسبت به محدوه اعداد، امنیت داده تصویری را دوچندان می‌کند. در نهایت برهم زدن نظم پیکسل‌ها نیز بر امنیت داده تصویری مورد نظر می‌افزاید.

مراجع

[1] Ahn, L.V. Hopper, N.J. , Public-key steganography, In Lecture Notes in Computer Science of Advances inCryptology, Springer-Verlag Heidelberg. Vol. 3027, pp: 323–341, 2004.

[2]Shannon, C.E.,Communication theory of secrecy systems. Bell System Technical Journal. Vol.28, pp 656-715, 1949.

[3] Shannon, C. E. , Communication Theory of Secrecy Systems. Bell Syst. Tech. J. vol. 28, pp:656-715, 1949.

[4] Fridrich, J. , Secure image ciphering based on chaos. Final report for AFRL, New York, 1997.

[5] Scharinger, J. , Fast encryption of image data using chaotic Kolmogorov flow. Journal of Electronic Imaging. Vol. 7, pp: 318–325, 1998.

[6] Yen, J.C. and Guo, J.I. , A new chaotic key-based design for image encryption and Decryption. in Proc. IEEE Int. Symposium Circuits and Systems, Geneva, Switzerland. pp: 49–52, 2000.

[7] Li, SJ. Zheng, X. Mou X. and Cai, Y., Chaotic encryption scheme for real-time digital video. Proc SPIE on Electronic Imaging, Real-Time Imaging. Vol. 4666, pp:149–160, 2002.
[8] Pisarchik, A. N.; Zanin, M. , Image Encryption with Chaotically Coupled Chaotic Maps. Physica D., 237(20), 2638-2648, 2008.
[9] Pareek, N. K. Patidar, V. Sud, K. K. , Discrete Chaotic Cryptography Using External Key. Phys. Lett. A. vol. 309, pp: 75-82, 2003.
[10] Kwok, H. S. Tang, W. K. S. , A Fast Image Encryption System Based on Chaotic Maps with Finite Precision Representation. Chaos, Solitons and Fractals. vol.32, pp: 1518-1529, 2007.
[11] Fridrich, J., Symmetric Ciphers Based on Two Dimensional Chaotic Maps. International Journal of Bifurcate Chaos. Vol.8, pp: 1259-1284, 1998.
[12] Guan, Z. Huang, F. Guan, W. , A Chaos-based Image Encryption Algorithm. Phys. Lett. A. vol.346, pp: 153-157, 2005.
[13] Lian, S. G. Sun, J. Wang, Z. , A Block Cipher Based on a Suitable Use of Chaotic Standard Map. Chaos, Solitons and Fractals. Vol.26, pp: 117-129, 2005.
[14] Lian,S., Secure Fractal Image Coding. France Telecom R&D Beijing, 2 Science Institute South Rd., Haidian District, Beijing, 100080, P.R China, 2011.
[15] Hung, Y. C. and Wo, W. K., Chaos-based encryption for fractal image coding Department of Electronic Engineering. City University of Hong Kong, Hong Kong, China, 2012.
[16] Fisher, Y. Jacobs, E. W. Boss, R. D. , Fractal Image Compression Using Iterated Transforms. NOSC Technical Report, San Diego, 1998.
[17] he, x.p. zhang, Q. H. , Image Encryption Based on Chaotic Modulation of wavelet Coefficient. Congress on Image and Singnal Processing, CISP. Vol. 222, pp:622-626, 2008.