مقاله پژوهشی

مجله انفورماتیک سلامت و زیست پزشکی
مرکز تحقیقات انفورماتیک پزشکی
دوره اول شماره اول. ص ٤٤-٣٢، ١٣٩٣

آنالیز کیفیت رمزنگاری تصویرهای پزشکی مبتنی بر الگوریتم راین‌دال با کلید رمزنگاری یکسان و آشوب‌گونه

محمدرضا نعیم‌آبادی[1]، علیرضا مهری‌دهنوی[2،3]*، حسین ربانی[2،3]

● **دریافت مقاله:** ۹۳/۶/۱۸ ● **پذیرش مقاله:** ۹۳/۷/۲۶

مقدمه: با توجه به گسترش استفاده از فن‌آوری‌های ارتباطی بی‌سیم در انتقال داده‌های حیاتی، حفظ حریم خصوصی و امنیت داده‌ها از اهمیت زیادی برخوردار می‌باشد. در حال حاضر با الگوریتم‌های متعددی رمزگذاری داده‌ها انجام می‌شود. اغلب این الگوریتم‌ها مبتنی بر رمزنگاری بلوکی می‌باشند که از یک کلید ثابت از پیش تعیین شده استفاده می‌کنند که حداقل ۱۲۸ بیت طول دارد.

روش: در این پژوهش، رمزنگاری با الگوریتم راین‌دال (Rijndael) با کلیدهای ثابت و متغیر صورت گرفته است. در رمزنگاری با کلید متغیر که در این مقاله طراحی شده است از یک بلوک مبتنی بر سیستم آشوب‌گونه (Mackey Glass) در واحد موتور تولیدکننده کلید به عنوان جایگزین الگوریتم گسترش کلید در قلب راین‌دال استفاده شده است و توسط یک بلوک کنترلی، رفتار آن بررسی و اصلاح می‌شود.

نتایج: روش‌های رمزنگاری عنوان شده، توسط ۶ معیار رمزنگاری، بررسی و ارزیابی شد. ارزیابی‌ها نشان داده است استفاده از کلیدهای متغیر آشوب‌گونه با ۲/۴۷ درصد افزایش بار محاسباتی، توانایی الگورتیم راین‌دال را در پنهان کردن الگو و توزیع هیستوگرام در تصویرهای پزشکی به شدت افزایش می‌دهد. استفاده از کلیدهای متغیر آشوب‌گونه به طور ذاتی تاثیری بر میزان حساسیت به کلید الگوریتم راین‌دال نداشته است.

نتیجه‌گیری: استفاده از سیستم آشوب‌گونه در واحد گسترش کلید برای تصویرهای پزشکی که در الگوریتم بهبودیافته راین‌دال عرضه شده است، امنیت داده حیاتی و حفظ حریم شخصی را به خوبی فراهم می‌کند.

کلید واژه‌ها: آنالیز کیفیت رمزنگاری، آنالیز قدرت و بهره‌وری رمزنگاری، رمزنگاری تصویرهای پزشکی، رمزنگاری مبتنی بر سیستم‌های آشوب‌گونه.

● **ارجاع:** نعیم‌آبادی محمدرضا، مهری‌دهنوی علیرضا، ربانی حسین. آنالیز کیفیت رمزنگاری تصویرهای پزشکی مبتنی بر الگوریتم راین‌دال با کلید رمزنگاری یکسان و آشوب‌گونه. مجله انفورماتیک سلامت و زیست پزشکی ۱۳۹۳؛ ۱(۱): ۴۴-۳۲.

۱. کارشناس ارشد مهندسی پزشکی، گروه مهندسی پزشکی، دانشگاه علوم پزشکی اصفهان، اصفهان، ایران

۲. دانشیار ، گروه مهندسی پزشکی، دانشگاه علوم پزشکی اصفهان، اصفهان، ایران

۳. مرکز تحقیقات پردازش تصاویر و سیگنال های پزشکی، دانشگاه علوم پزشکی اصفهان، اصفهان، ایران

* **نویسنده مسؤول:** اصفهان، هزارجریب، دانشگاه علوم پزشکی اصفهان، دانشکده فناوری های نوین، گروه مهندسی پزشکی.

● **شماره تماس:** ۰۳۱-۹۵۰۱۶۴۹۸

●**Email:** mehri@med.mui.ac.ir

مقدمه

با گسترش فن‌آوری‌های مخابراتی و ارتباطی، به‌ویژه ارتباطات بی‌سیم، رمزنگاری و مخفی‌سازی اطلاعات، یکی از ضرورت‌های ارتباطی شده است.

در حال حاضر رمزنگاری اطلاعات تنها مختص اطلاعات نظامی و امنیتی نمی‌باشد، بلکه در بسیاری از حوزه‌های دیگر به کار می‌رود. امروزه رمزنگاری داده‌ها و پرونده‌های پزشکی، ویدیوکنفرانس‌های از راه دور، اطلاعات هویتی افراد و یا اطلاعات یک سازمان به‌طور گسترده‌ای صورت می‌گیرد. همچنین حفظ حریم خصوصی افراد به سادگی با رمزنگاری امکان‌پذیر می‌باشد.

بر اساس آمارها، در ایالات متحده، سازمان‌ها به طور متوسط بودجه تخصیص داده شده به حوزه امنیت خود را از ۴۰ درصد بودجه خدمات فن‌آوری اطلاعات در سال ۲۰۰۶ به ۵۵ درصد افزایش داده‌اند [۱،۲].

با ورود فن‌آوری‌های نوین در علم پزشکی و به خدمت گرفتن مهندسی در پزشکی، ارتقاء قابل توجهی در سطح خدمات ارائه شده در چند دهه اخیر صورت گرفته است. همچنین در در دهه اخیر، فن‌آوری‌های مخابراتی و ارتباطی در پزشکی به منظور انتقال اطلاعات پزشکی و پیدایش پزشکی از راه دور و مراقبت الکترونیک، به کار گرفته شده است [۳].

پرونده‌های پزشکی بیماران دربردارنده اطلاعات بسیار حساسی می‌باشد که نباید افراد غیرمجاز به آنها دسترسی داشته باشند. قابل دسترس نبودن پرونده‌های پزشکی بیماران علاوه بر حفظ حریم شخصی، مانع تهدید و تهاجم به داده‌های بیمار می‌شود [۴،۵].

تهاجم به داده‌های حیاتی یک بیمار به دو گروه تهاجم از داخل و تهاجم از خارج تقسیم می‌شود. تهاجم از خارج با شنود و یا تغییر در پرونده‌های پزشکی به وسیله حمله‌های تحت شبکه‌های کامپیوتری مانند استراق سمع (Eavesdropping)، تزریق بسته (Packet Injection) و یا حمله شخص در وسط (Men in middle Attack)، صورت می‌گیرد [۶]. تهاجم از داخل می‌تواند توسط کلینیسین، بیمار و یا هر فردی که در محل ارائه خدمات مراقبتی حضور دارد، انجام شود. تهاجم از داخل به منظور مخفی کردن خطاهای پزشکی (malpractice) و یا کلاه‌برداری از بیمه‌های درمانی صورت می‌گیرد [۷].

معمول‌ترین راه برای امنیت و حفظ حریم خصوصی، رمزگذاری پرونده‌های پزشکی می‌باشد. گر چه تا کنون روشی اختصاصی برای رمزگذاری داده‌های حیاتی پیشنهاد نشده است [۸،۹]، ولی روش‌های متعددی برای رمزگذاری داده‌ها، مستقل از اطلاعاتی که در بردارند، ارائه شده است. (Data Encryption Standard) DES، Blowfish، IDEA (International Data Encryption Algorithm)، RC5، RC6، Triple DES، راین‌دال (Rijndael)، Serpent، Twofish از جمله رایج‌ترین روش‌های رمزگذاری با کلید متقارن (Symmertic Key) می‌باشند [۱۰،۱۱] که سه مورد اخیر یعنی Rijndael، Serpent و Twofish موفق‌ترین آنها محسوب می‌شوند. در تمامی این روش‌ها از یک کلید باینری که عموماً ۱۲۸ تا ۲۵۶ بیتی است، استفاده می‌شود [۱۲].

سیستم‌های رمزنگار به دو دسته رمزنگار رشته‌ای (Stream Cipher) و رمزنگار بلوکی (Block Cipher) تقسیم می‌شوند. رمزنگارهای رشته‌ای سعی می‌کنند با ترکیب داده های ورودی با یک رشته اعداد شبه تصادفی، رمزگذاری داده‌ها را انجام دهند. الگوریتم رمزنگاری RC4 نمونه‌ای از رمزنگاری رشته‌ای می‌باشد. در رمزنگاری بلوکی، رمزنگاری داده‌های دارای طول مشخص که بلوک نامیده می‌شوند بر اساس مجموعه‌ای از تبدیل‌های غیر خطی صورت می‌گیرد و داده‌ها در حین رمزگذاری به صورت بلوک به بلوک رمز می‌شوند. الگوریتم‌های رمزنگاری AES (Advanced Encryption Standard) و DES، متداول‌ترین رمزنگارهای بلوکی هستند.

در رمزنگاری رشته‌ای هر چه رشته رمزکننده، تصادفی‌تر باشد سیستم رمزنگار قدرتمندتر می باشد و در رمزنگاری بلوکی هر چه عملیات رمزنگاری، غیرخطی و پیچیده‌تر باشد، الگوریتم رمزنگار قدرتمندتر می‌باشد. بنابراین رمزنگارهای رشته‌ای سریع‌تر و رمزنگارهای بلوکی قدرتمندتر هستند [۱۳،۱۴].

در این پژوهش از رمزنگاری بلوکی به روش راین‌دال با کلیدهای رمزگذاری ثابت (که در حال حاضر از این شیوه استفاده می‌شود) و رمزگذاری متغیر آشوب‌گونه، استفاده و ارزیابی شده است.

روش

در این پژوهش برای رمزنگاری تصویرهای شبکیه چشم از سه الگوریتم رمزنگاری Rijndael، Serpent و Twofish استفاده شده است. تمامی الگوریتم‌های مطرح شده، در دسته

رمزنگارهای بلوکی متقارن قرار می‌گیرند که در ادامه هر یک مختصراً معرفی شده‌اند.

رمزگذاری به روش راین‌دال

الگوریتم رمزنگاری راین‌دال توسط دو رمزنگار بلژیکی به نام‌های Joan Daemen و Vincent Rijmen با هدف شرکت در رقابت برای انتخاب استاندارد الگوریتم پیشرفته، معرفی شد که پس از سه مرحله رقابت و تکامل، این الگوریتم انتخاب شد. طراحان الگوریتم رمزنگاری راین‌دال در آن زمان که در تعریف ساختار الگوریتم زمانی اغلب توجه‌ها به ساختار فیستل معطوف بود، با سنت‌شکنی و بنا کردن ساختار الگوریتم بر اساس شبکه جانشینی–جایگشت، خطر بزرگی کردند. این الگوریتم با توجه به شرایط تعیین شده از سوی NIST از بلوک‌های ورودی ۱۲۸ بیتی و کلیدهای ۱۲۸، ۱۹۲ و ۲۵۶ بیتی بهره می‌گیرد. همچنین تعداد دورها متناسب با طول کلیدها تغییر می‌کند و به ترتیب برای طول‌های ذکر شده ۱۰، ۱۲ و ۱۴ دور برای راین‌دال تعریف شده است. اساس کار این الگوریتم مبتنی بر عملیات مدولار و در میدان گالو GF(28) می‌باشد و پایه محاسبات در راین‌دال بر اساس محاسباتی بایتی (۸ بیتی) تعریف شده است.

الگوریتم رمزنگاری راین‌دال از سه بخش مجزا شامل دور ابتدایی، دورهای اصلی و دور نهایی تشکیل شده است. در دور ابتدایی تنها کلید دور با بلوک ورودی، XOR می‌شود و به نوعی، عمل سفیدسازی ورودی در این دور صورت می‌گیرد و به همین جهت این دور در شمارش تعداد دورها محسوب نمی‌شود. در شکل ۱ این سه بخش به صورت بلوک دیاگرامی نشان داده شده است [۱۵–۱۷].

سیستم آشوب‌گونه Mackey Glass

سیستم آشوب‌گونه‌ای که در این پژوهش برای تولید کلید متغیر استفاده شده است، سیستم آشوب‌گونه Mackey Glass می‌باشد. این سیستم آشوب‌گونه شامل یک سری آشوب‌گونه می‌باشد. لازم به ذکر است که این سیستم‌های آشوب‌گونه دارای خواص زیر می‌باشند:

–غیر خطی

–حساسیت شدید به شرایط اولیه

–عدم تکرار مسیر حرکت (trajectory) در طول زمان

–به حالت آشوب رفتن توسط تعداد بیشماری انشعاب

–رفتار بعدیت کسری (Fractal dimension) [۱۸،۱۹].

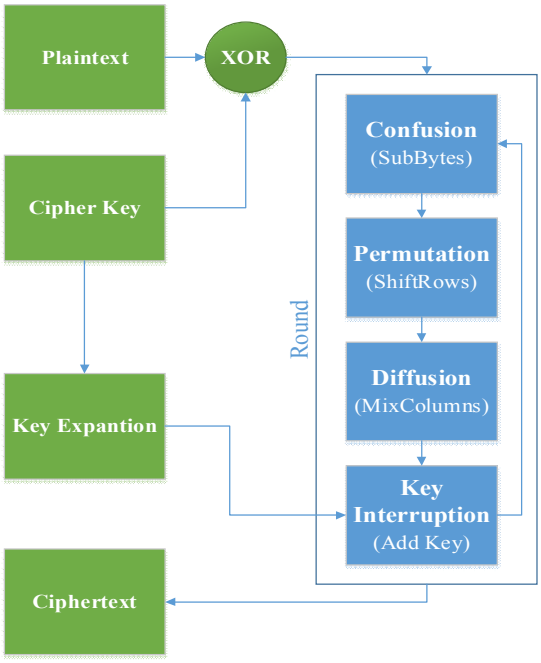
سری Mackey Glass توسط رابطه ۱ تعریف می‌شود.

$$\frac{dx}{dt} = \frac{(ax(t-\tau))}{(1+x^n(t-\tau))} - bx(t)$$

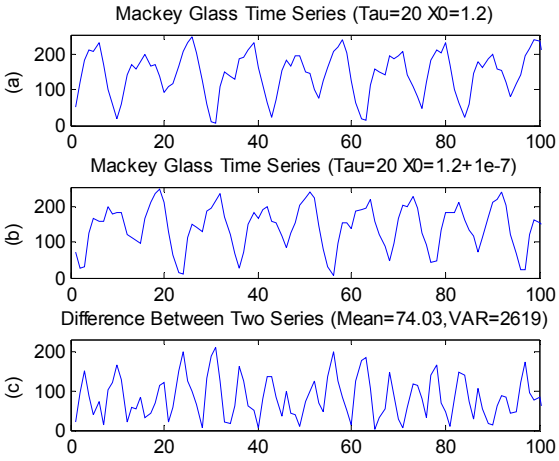
رابطه (۱)

در رابطه ۱، a، b و n مقادیر ثابت هستند و τ تأخیر می‌باشد رفتار آشوبناک این معادله به ازای $\tau > 17$ ایجاد می‌شود. این معادله دارای شرایط اولیه می‌باشد و همان طور که عنوان شد حساسیت شدیدی نسبت به شرایط اولیه دارد [۲۰].

در این مقاله برای a، b، τ و n به ترتیب مقادیر ثابت ۰/۲، ۰/۱، ۲۰ و ۱۰ و تنها شرط اولیه در این روش، متغیر در نظر گرفته شده است. در شکل ۲، دو سری زمانی با اختلاف بسیار اندک در شرایط اولیه (۱۲ میلیون برابر کوچک‌تر از شرایط اولیه) به همراه اختلاف آنها نشان داده شده است. همان طور که مشاهده می‌شود اختلاف بسیار اندک در شرایط اولیه، تفاوت قابل توجهی در نتیجه نهایی ایجاد می‌کند.



شکل ۱: الگوریتم رمزنگاری Rijndael



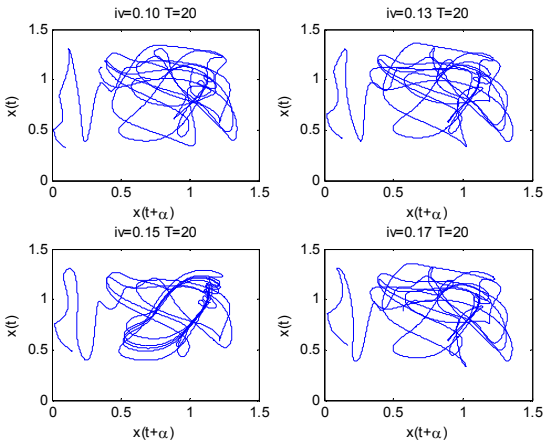
شکل ۲:

a) سری Macky Glass با شرط اولیه X0=1.2

b) سری Macky Glass با شرط اولیه X0=1.2+10-7

c) اختلاف میان دو سری Macky Glass

شکل ۳ نیز نمودار فضای فاز مسیر چند نمونه سری را با اختلاف اندک در شرایط اولیه نشان می‌دهد. همان طور که دیده می‌شود با تغییر اندک، مسیرها به طور کلی عوض می‌شوند.

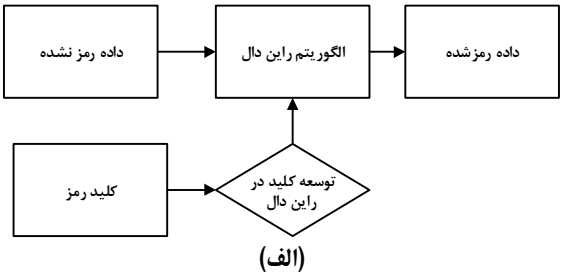


شکل ۳: سطح مقطع پوانکاره چهار مجموعه تولید شده توسط Mackey Glass به ازای تغییر اندک در شرایط اولیه

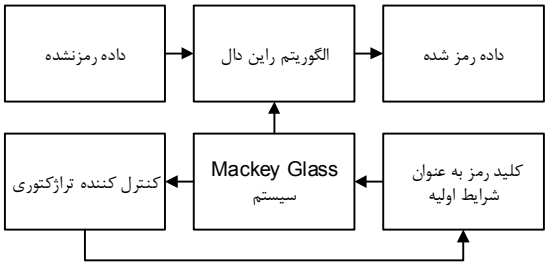
پیاده‌سازی رمزنگاری راین‌دال با کلیدهای متفاوت

در این پژوهش، رمزنگاری به روش راین‌دال توسط دو دسته کلید ثابت و کلید آشوبی صورت گرفت. در شکل ۴، بلوک دیاگرام روش‌های استفاده شده، نشان داده شده است. در الگوریتم رمزنگاری مبتنی بر سیستم آشوبی، کلید رمز، شرایط اولیه را برای سیستم تعریف می‌کند و یک کنترلر تراژکتوری بررسی می‌کند که کلید آشوبی تولید شده بعد فرکتال خود را حفظ کند و در صورت خروج از این معیار، شرط اولیه توسط آخرین عدد تولیدی، بازنشانی می‌شود.

اگر سیگنال رمزگذاری شده توسط کلید ثابت، دارای خاصیت تناوبی با دوره تناوب بزرگتر از بلوک رمزگذاری باشد، سیگنال رمز شده در بازه‌هایی رفتار تناوبی از خود نشان خواهد داد. این رفتار هنگامی که داده‌ها در فریم با سرآیند (Header) و پی‌آیند (Trailer) معین قرار می‌گیرند، تشدید می‌شود. فرد اخلال‌گر می‌تواند حتی بدون در اختیار داشتن اطلاعاتی در مورد سیگنال اصلی، داده‌های رمز شده نامعتبر را ایجاد کند [۲۱].



(الف)



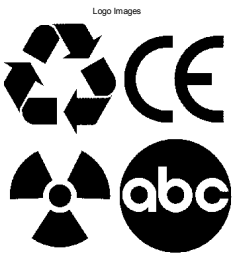
(ب)

شکل ٤:

الف) بلوک دیاگرام رمزنگاری با کلید ثابت

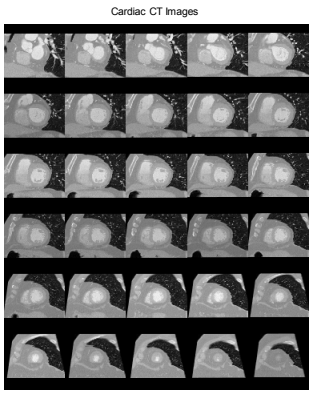
ب) بلوک دیاگرام رمزنگاری با کلید متغیر آشوب‌گونه داده استفاده شده

برای ارزیابی الگوریتم از پنج دسته داده استفاده شد. دسته اول داده‌ها شامل چهار تصویر لوگو می‌باشد که در شکل ۵ نشان داده شده است. از این تصویرها بیشتر برای تشخیص و ارزیابی توانایی الگو در پنهان کردن الگوی تصویر اصلی پس از رمزگذاری و پراکنده کردن هیستوگرام، استفاده شده است. تمامی تصویرهای استفاده شده، دارای دو رنگ (تنها دو سطح رنگی سیاه و سفید) و جزئیات اندک با لبه‌های تیز می‌باشند.



شکل ۵: تصویرهای لوگوی استفاده شده برای ارزیابی

دسته دوم داده‌ها ۳۰ تصویر CT اسکن قلبی است که توسط دستگاه CT اسکن زیمنس مدل SOMATOM Sensation 64 Slices در بیمارستان فوق تخصصی میلاد اصفهان تهیه شده است [۲۲،۲۳]. در شکل ۶، تصویرهای CT اسکن قلبی استفاده شده، نشان داده شده است. هر یک از این تصویرها، یک برش که دارای جزئیات زیاد، همراه با لبه‌های تیز می‌باشد را نشان می‌دهد.



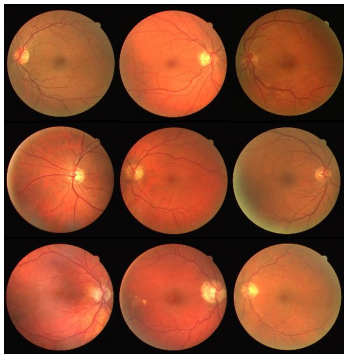
شکل ٦: ۳۰ تصویر Cardiac CT استفاده شده برای ارزیابی

دسته سوم داده‌ها ۴۰ تصویر صورت از مجموعه تصویرهای صورت ORL می‌باشد. این تصویرها همگی در ابعاد ۱۱۲×۹۶ پیکسل و سیاه و سفید با رزلوشن ۸ بیتی [۲۴] و همگی دارای جزئیات متوسط و لبه‌های نرم می‌باشند که فرض شده، بخشی از مشخصات بیمار در پرونده الکترونیک وی باشد.

چهارمین دسته از تصویرها، شامل سه تصویر می‌باشد که توسط دستگاه اولتراسوند GE LOGIQ S6 در بیمارستان الزهرای اصفهان گرفته شده و در شکل ۷ نشان داده شده است [۲۵،۲۶]. این تصویرهای سونوگرافی همگی با فرمت DICOM و بدون فشرده‌سازی، به صورت سیاه و سفید ذخیره شده و بیشترین جزئیات و تیزترین لبه‌ها را در تصویرهای مورد ارزیابی دارند.

شکل ۷: تصویرهای اولتراسوند استفاده شده

آخرین دسته داده‌ها شامل ۹ تصویر شبکیه چشم است که خود بخشی از بانک داده Drive می‌باشند (شکل ۸). علاوه براولویت کلینیکی این تصویرها، طیف رنگی، آنها را از سایر تصویرهای قبلی متمایز نموده است [۲۷].



شکل ۸: تصویرهای شبکیه چشم

نتایج

تاکنون روش‌های مختلفی برای ارزیابی کیفیت و کارایی الگوریتم‌های رمزنگاری معرفی شده است [۳۱-۲۸]. در این مقاله رمزنگاری‌های معرفی شده، توسط معیارهای کیفیت رمزنگاری (Encryption Quality)، همبستگی متقابل (Cross Correlation)، توزیع هیستوگرام (Histogram Spreading) ، پنهان کردن الگو (Pattern Hiding) ، حساسیت به کلید (Key Sensitivity) و سرعت (Throughput) و مدت زمان صرف شده، ارزیابی شده است.

کیفیت رمزگذاری و یا فاکتور حداکثر انحراف (Maximum Deviation Factor) کیفیت رمزگذاری، متوسط اختلاف هیستوگرام داده اصلی و داده رمز شده را نشان می دهد. کیفیت رمزنگاری بر اساس رابطه ۲ محاسبه شده است [۳۲].

$$EQ = \frac{\sum_{L=0}^{256} \left| Hist(P) - Hist(C) \right|}{256}$$

رابطه (۲)

در رابطه ۲، $Hist(P)$ و $Hist(C)$ به ترتیب هیستوگرام‌های داده‌های اصلی و رمز شده می‌باشند. این پارامتر میزان تغییر ایجاد شده در هیستوگرام داده رمز شده نسبت به داده‌های اصلی را اندازه‌گیری می‌کند و هر چه این مقدار بیشتر باشد، رمزگذاری،

قدرت بیشتری دارد. جدول ۱ کیفیت رمزگذاری داده‌های ارزیابی شده را نشان می‌دهد. همان طور که در این جدول مشاهده می‌شود برای تصویرهایی که دارای جزئیات زیادی می باشند، اختلاف این پارامتر اندک است (برای تصویرهای اولتراسوند و Cardiac CT که دارای جزئیات زیادی هستند، با هم برابر هستند) ولی با کاهش جزئیات، اختلاف دو روش به میزان چشمگیری افزایش می‌یابد.

جدول ۱: مقادیر کیفیت رمزنگاری به ازای کلید ثابت و متغیر

داده‌ها	کلید ثابت	کلید آشوب‌گونه	درصد بهبود
سونوگرافی	۶۱/۸۱	۶۱/۸۱	۰
صورت	۳۰/۵۰	۳۰/۵۲	۰/۰۷
CT قلبی	۸۰/۶۹	۸۰/۶۹	۰
شبکیه	۱۴۳/۵۲	۱۴۳/۵۲	۰
لوگو	۱۰۵/۲۳	۲۵۳/۰۱	۱۴۰/۴۴

فاکتور ضریب همبستگی متقابل

فاکتور ضریب همبستگی متقابل در واقع همبستگی متقابل بین داده‌های رمزنشده و رمزشده می‌باشد. هر چه این مقدار به یک نزدیک‌تر باشد همبستگی سیگنال‌ها بیشتر خواهد بود و هر چه به صفر نزدیک‌تر باشد داده‌ها همبستگی کمتری دارند. همبستگی کمتر نشان‌دهنده بالاتر بودن کیفیت رمزنگاری می‌باشد. همبستگی متقابل بین دو سیگنال توسط رابطه‌های ۳ محاسبه شده است [۳۳].

$$R_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)\times D(y)}}$$

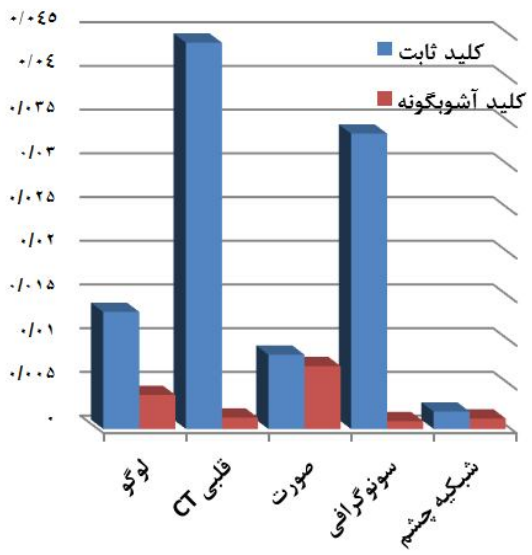
$$\mathrm{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))\times(y_i - E(y))$$

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

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

رابطه‌های (۳)

همبستگی بین داده‌های اصلی و رمزشده برای هر یک از الگوریتم‌های رمزنگاری در نمودار ۱ نشان داده شده است. همان طور که در این شکل مشاهده می‌شود برای تصویرهایی که دارای لبه تیز می‌باشند، رمزنگاری با استفاده از کلید آشوب‌گونه نسبت به رمزنگاری با کلید ثابت به مقدار قابل توجهی همبستگی میان دو تصویر را کاهش داده است ولی این برتری برای تصویرهایی که لبه‌های نرم‌تری دارند (مانند تصویرهای صورت) بسیار کمتر می‌باشد.

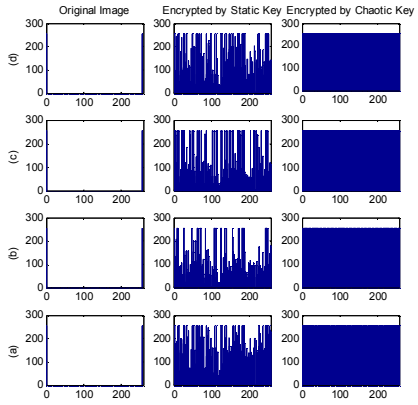


نمودار ۱: هیستوگرام همبستگی متقابل داده‌ها

کیفیت رمزنگاری در الگوریتمی بالاتر می‌باشد که در آن هیستوگرام داده رمزشده نسبت به داده اصلی به کلی تغییر پیدا کند و سیستم رمزنگار بتواند هیستوگرام را بر تمامی اعداد به‌صورت یکسان پخش کند. با مشاهده هیستوگرام تصویر اصلی و هیستوگرام تصویر رمزشده می‌توان کیفیت رمزنگاری را ارزیابی کرد.

همان طور که انتظار می‌رفت با توجه به این نکته که هیستوگرام مجموعه داده اول کاملا مجزا بود، بهره‌گیری از کلید متغیر تنها در این دسته موثر واقع شده است.

در شکل ۹ مشاهده می‌شود که رمزنگاری با کلید ثابت در توزیع هیستوگرام تصویرهای با جزئیات اندک، ناموفق بوده است ولی در روش‌های کلید آشوب‌گونه، هیستوگرام تصویر رمزگذاری شده، به خوبی توزیع شده است.



شکل ۹: هیستوگرام‌های تصویرهای لوگو قبل و بعد از رمزنگاری با کلیدهای متفاوت (ستون‌ها به ترتیب از سمت چپ، تصویر رمزنشده، رمزشده با کلید ثابت و رمزشده با کلید آشوب‌گونه)

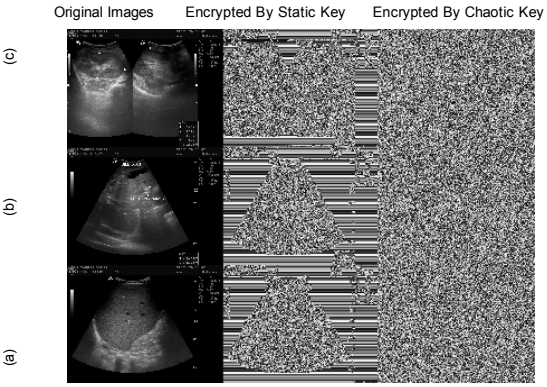
پنهان کردن الگو

الگو عموماً برای تصویرها تعریف می‌شود و پنهان شدن الگوی تصویر پس از رمزنگاری، نشان‌دهنده قدرتمندی الگوریتم رمزنگاری می‌باشد.

پنهان کردن الگو مانند هیستوگرام با مشاهده قابل ارزیابی است. این امر در تصویرها، به ویژه آنهایی که سطوح رنگی کمی را پوشش می‌دهند (الگوی واضح‌تری دارند)، ساده‌تر قابل مشاهده می‌باشد.

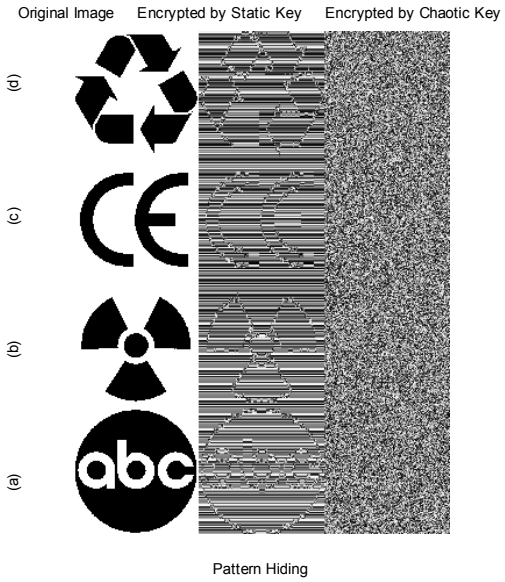
ارزیابی پنهان کردن الگو برای پنج گروه تصویرهای معرفی شده نشان داده است که استفاده از کلید ثابت در رمزنگاری راین‌دال باعث می‌شود که این الگوریتم در پنهان کردن الگوهای بارز، عملکرد ضعیفی داشته باشد. شکل‌های ۱۰ و ۱۱ برجسته‌ترین اختلاف عملکردی را در این مورد نشان می‌دهد.

در شکل ۱۰ تصویرهای رمزنگاری شده با کلید ثابت و کلید آشوب‌گونه برای تصویرهایی که دارای جزئیات زیاد هستند (اولتراسوند)، نشان داده شده است. با کمی دقت می‌توان به ضعف الگوریتم راین‌دال در پنهان کردن اطلاعات در این گروه پی برد.



شکل ۱۰: تصویرهای اولتراسوند قبل و پس از رمزنگاری با کلیدهای متفاوت (ستون‌ها به ترتیب از سمت چپ، تصویر رمزنشده، رمزشده با کلید ثابت و رمزشده با کلید آشوب‌گونه)

در شکل ۱۱ توانایی پنهان کردن الگو در تصویرهای الگوی سیاه و سفید (لوگوها) نشان داده شده است. با توجه به اینکه الگوهای مورد استفاده دارای ناحیه‌هایی به رنگ سیاه و سفید و همچنین دارای لبه‌های تیز در تصویر می‌باشند، تشخیص الگو در آنها ساده‌تر صورت می‌گیرد.



شکل ۱۱: تصویرهای لوگوها قبل و پس از رمزنگاری با کلیدهای متفاوت (ستون‌ها به ترتیب از سمت چپ، تصویر رمزنشده، رمزشده با کلید ثابت و رمزشده با کلید آشوب‌گونه)

همان طور که در شکل ۱۲ مشاهده می‌شود رمزگذاری با استفاده از کلید ثابت در حذف الگوی تصویر، به کلی ناموفق بوده است و الگوی تصویر پس از رمزگذاری شدن، به سادگی قابل تشخیص می‌باشد، در صورتی‌که در رمزنگاری با کلید آشوب‌گونه، الگوی تصویر به طور کامل پنهان می‌شود.

زمان صرف شده و نرخ خروجی

سرعت رمزگذاری و مدت زمان صرف شده برای رمزگذاری یکی از مهم‌ترین شاخص‌های روش‌های رمزنگاری می‌باشد. مدت زمان صرف شده وابسته به محاسبات و عملیاتی است که در حین رمزنگاری صورت می‌گیرد.

آن دسته از روش‌های رمزنگاری دارای قدرت بیشتری هستند که با استفاده از محاسبات کمتر، امنیت بالایی را ارائه دهند. رمزنگاری‌هایی که امنیت آنها ناشی از پیچیدگی و محاسبات بسیار سنگین باشد، رمزنگاری مناسبی نمی‌باشند [۳۲].

باتوجه به اینکه در هر دو روش از یک الگوریتم رمزگذاری استفاده شده، با این تفاوت که در روش دوم از یک سری آشوب‌گونه برای تولید کلید استفاده شده است، عملیات تولید کلید متغیر مقداری به بار محاسباتی رمزنگاری می‌افزاید، بنابراین هنگامی که از کلید متغیر در رمزنگاری استفاده می‌شود انتظار می‌رود محاسبات بیشتر و به دنبال آن مدت زمان بیشتری نسبت به حالتی که رمزنگاری توسط کلید ثابت انجام می‌گیرد، صرف شود. رمزنگاری توسط یک کامپیوتر Desktop با پردازنده

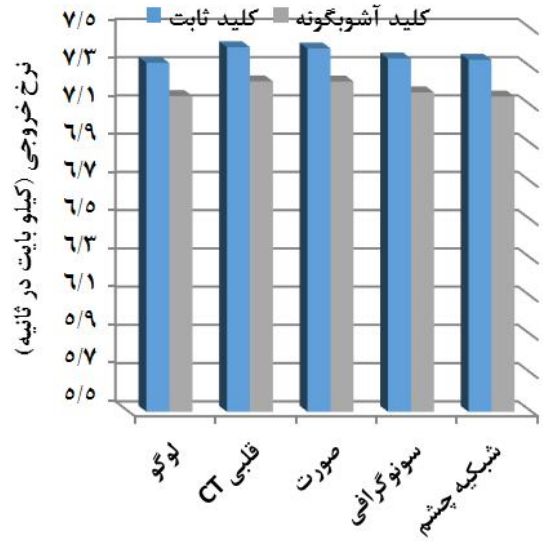
Q6600 Intel و حافظه در دسترس 4GB، در سیستم عامل Windows 7 64bit و تحت نرم‌افزار Matlab2011a 64bit صورت گرفته است.

همان طور که در جدول ۲ مشاهده می‌شود استفاده از کلید متغیر به‌طور متوسط ۲/۴۷ درصد، مدت زمان رمزنگاری را افزایش می‌دهد. سرعت رمزگذاری یا نرخ خروجی با مدت زمان صرف شده رابطه عکس دارد.

جدول ۲: درصد زمان صرف شده افزوده در روش کلید متغیر نسبت به کلید ثابت

داده‌ها	درصد
شبکیه	۲/۶۲
سونوگرافی	۲/۴۶
صورت	۲/۳۹
سی تی اسکن قلبی	۲/۴۶
لوگو	۲/۴۳

در نمودار ۲ سرعت خروجی برحسب کیلوبیت در ثانیه برای روش‌های مختلف رمزنگاری نشان داده شده است. مشاهده می‌شود که نرخ رمزنگاری در حالت‌های رمزنگاری با کلید متغیر اندکی از حالت کلید ثابت کمتر می‌باشد.



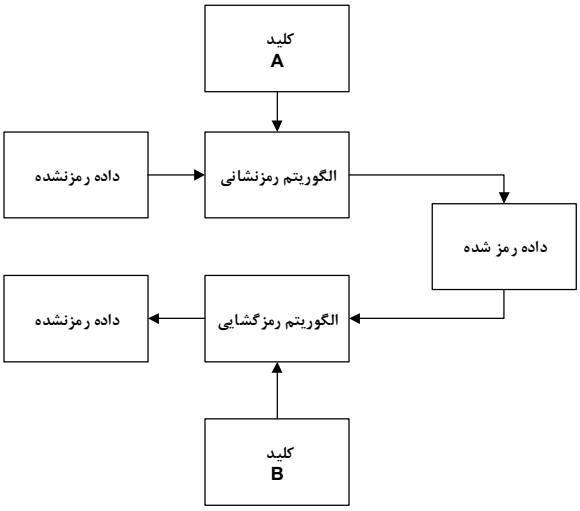
نمودار ۲: هیستوگرام سرعت رمزگذاری برای روش‌های مختلف رمزگذاری

حساسیت به کلید

قدرت کلید در رمزگذاری دارای اهمیت زیاد و متناسب با طول کلید می‌باشد. همان طور که پیش از این عنوان شد الگوریتم راین‌دال از یک کلید ۱۲۸ بیتی برای رمزنگاری بهره می‌گیرد.

حساسیت به کلید یکی از مهم‌ترین ویژگی‌های الگوریتم‌های رمزنگاری است. در یک رمزنگاری قوی، با تغییر اندک در کلید، رمزگشایی آن غیر ممکن می‌شود. در صورتی که رمزگشایی با کلیدی که اختلاف بسیار اندکی با کلید رمزگذاری داشته باشد صورت گیرد، تفاوت با داده اصلی بسیار زیاد خواهد شد.

به منظور ارزیابی حساسیت به کلید در الگوریتم‌های رمزنگاری، ابتدا یک مجموعه داده توسط کلید A (KEY1) رمزگذاری شده است و سپس توسط کلید B (KEY2) که تنها یک بیت با کلید قبلی تفاوت دارد رمزگشایی می‌شود. از نقطه نظر ایده‌آل تفاوت بین داده اصلی و داده رمزگشایی شده با کلید اشتباه باید حداکثر باشد. شکل ۱۲ بلوک دیاگرام روش استفاده شده برای ارزیابی حساسیت به کلید را نشان می‌دهد.



شکل ۱۲: بلوک دیاگرام ارزیابی حساسیت به کلید

برای اندازه‌گیری اختلاف دو تصویر از معیارهای میانگین مربع خطا (Mean Square Error: MSE)، میانگین خطای مطلق (Mean Absolute Error=MAE) و نسبت پیک سیگنال به نویز (Peak Signal to Noise Ratio=PSNR) استفاده شده است. الگوریتمی قدرتمندتر است که با تغییر اندک در کلید، اختلاف و یا خطای زیادی را ایجاد کند. بنابراین مطلوب است که مقادیر میانگین مربع خطا و میانگین خطای مطلق برای ارزیابی حساسیت کلید، حداکثر و نسبت پیک سیگنال به نویز، حداقل مقدار ممکن باشد.

۷-٤-۱- کلید ثابت

در این بخش در تمامی رمزگذاری‌ها به روش راین‌دال با کلید، از کلیدهای ۱۲۸ بیتی زیر استفاده شده است که تنها در

کم ارزش‌ترین بیت اختلاف دارند. از کلید اول برای رمزگذاری و از کلید دوم برای رمزگشایی استفاده شده است.

KEY_1=2B7E151628AED2A6ABF7158809CF4F3C

KEY_2=2B7E151628AED2A6ABF7158809CF4F3B

٤-٧-٢- کلید متغیر Mackey Glass

همان طور که عنوان شد از سیستم آشوب‌گونه Mackey Glass برای تولید کلید آشوب‌گونه استفاده شده است. در رابطه ١، مقادیر متغیرهای a، b، n و τ مقادیر ثابت و به ترتیب برابر ٠/٢، ٠/١، ١٠ و ٢٠ است و شرط اولیه توسط یک متغیر ٣٢ بیتی اعشاری (float) تعیین می‌شود. شرط اولیه را نیز می‌توان توسط یک متغیر ۶۴ بیتی (double) با دقت بالاتری در نظر گرفت. طول کلید در این روش می‌تواند بین ٣٢ تا ٢٠٨ بیت باشد که در این پژوهش از حداقل طول کلید و همچنین از شرط ٣٢ بیتی یعنی حداقل قدرت سیستم تولید کننده کلید استفاده شده است.

در تمامی ارزیابی‌هایی که با کلید متغیر Mackey Glass صورت گرفته از کلیدهای ٣٢ بیتی زیر به عنوان شرایط اولیه سری Macky-Glass استفاده شده است. اختلاف این دو کلید نیز در کم ارزش‌ترین بیت می‌باشد و از کلید اول برای رمزگذاری و از کلید دوم برای رمزگشایی استفاده شده است [٣۴].

$(3F99999A)_{Hex}=(1.2000000)_{Dec}$ KEY_1=

$(3F99999B)_{Hex}=(1.2000002)_{Dec}$ KEY_2=

٧-٤-٣- نتایج خطای ایجاد شده ناشی از کلید اشتباه

معیار میانگین مربع خطاها توسط رابطه ۴ محاسبه شده است که در آن $P(i,j)$، تصویر اصلی و $P'(i,j)$، تصویر رمزگشایی شده با کلید نادرست می‌باشد. M و N طول ابعاد تصویر را تعیین می‌کند.

$$MSE=\frac{1}{N\times M}\sum_{j=1}^{M}\sum_{i=1}^{N}[P(i,j)-P'(i,j)]^2$$

رابطه (٤)

جدول ٣، میانگین مربع خطا محاسبه شده بین دو داده اصلی و رمزگشایی شده با کلید نادرست را نشان می‌دهد.

جدول ٣: مقایسه حساسیت به کلید در روش های مختلف رمزنگاری بر اساس معیار میانگین مربع خطا

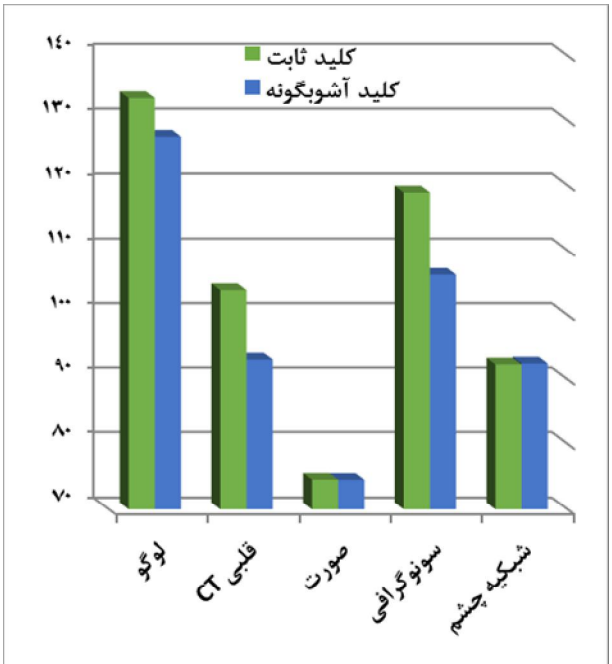
داده‌ها	کلید ثابت	کلید آشوب‌گونه	درصد تغییر
لوگو	٢٣٢٠٠	٢١٧٣٥	-٦/٧
سی‌تی‌اسکن قلبی	١٥٧٤٦	١٢٨٩١	-٢٢/٢
صورت	٨١٧٤	٨١٦١	-٠/١٥
سونوگرافی	١٩٧٣٤	١٦٢٦٤	-٢١/٣
شبکیه	١٢٦٩٨	١٢٧٣٦	٠/٣

میانگین خطای مطلق نیز مشابه میانگین مربع خطا می‌باشد، با این تفاوت که در میانگین مربع خطا، خطای کوچک، کوچک‌نمایی و خطاهای بزرگ، بزرگ‌نمایی می‌شود، در صورتی‌که در معیار میانگین خطای مطلق، خطاها بدون بزرگ-نمایی و یا کوچک‌نمایی نشان داده می‌شود.

میانگین مطلق خطای ناشی از رمزگشایی با کلید نادرست اضافه شده پس از رمزگذاری در داده رمزگشایی، بر اساس رابطه ۵ محاسبه شده است که در نمودار ٣ آمده است.

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

رابطه (٥)



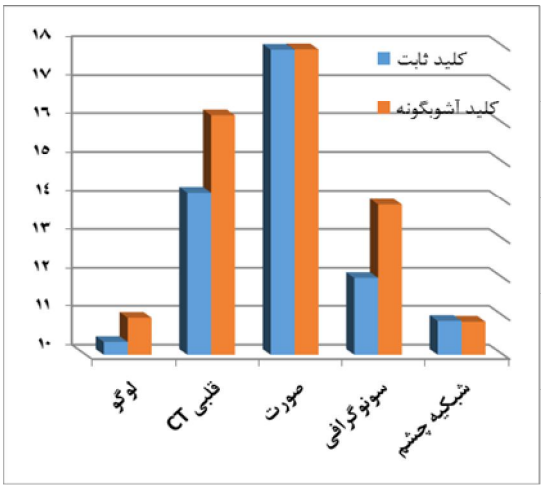
نمودار ٣: میانگین خطای مطلق میان دو تصویر رمز نشده و رمزگشایی شده توسط کلید نادرست توسط الگوریتم‌های رمزنگاری راین‌دال با کلید ثابت و متغیر آشوب‌گونه

نسبت پیک سیگنال به نویز، معیاری است که نسبت حداکثر توان ممکن سیگنال به توان نویز تخریبی را نشان می‌دهد. باتوجه به اینکه توان سیگنال می‌تواند شامل محدوده گسترده‌ای باشد، معمولا در مقیاس لگاریتمی دسیبل محاسبه می‌شود.

نسبت پیک سیگنال به نویز عموماً به عنوان معیاری از کیفیت بازسازی تصویرها از کدکننده‌های فشرده‌سازی با اتلاف استفاده می‌شود [۵،۳۵].

بر اساس رابطه ۶، نسبت پیک سیگنال به نویز میان دو تصویر رمزنشده و رمزگشایی شده با کلید نادرست برای روش‌های رمزگذاری راین‌دال، با کلید ثابت و متغیر، محاسبه و در نمودار ۴ نشان داده شده است

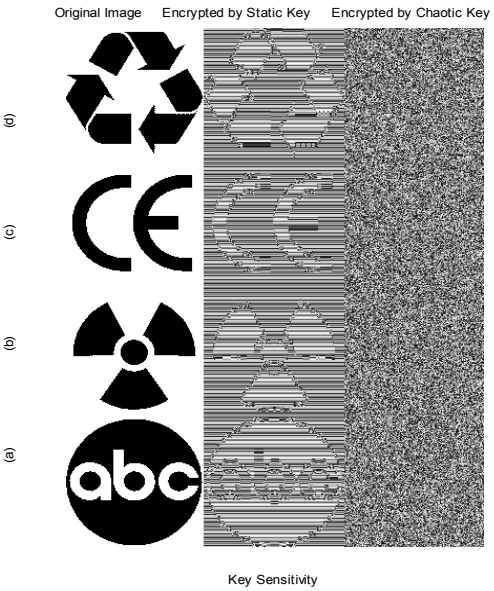
$$PSNR = 10\log\left(\frac{\max(P)}{MSE}\right)$$ **رابطه (٦)**



نمودار ٤: نسبت پیک سیگنال به نویز میان دو تصویر رمز نشده و رمزگشایی شده توسط کلید نادرست توسط الگوریتم‌های رمزنگاری راین‌دال با کلید ثابت و متغیر آشوب‌گونه

نتایج به دست آمده نشان می‌دهد که حساسیت به کلید نیز وابسته به هسته الگوریتم است و مستقل از متغیر یا ثابت بودن کلید می‌باشد. تفاوت خطای به‌دست آمده در هر دو حالت اندک است.

در شکل ۱۳، تصویر الگوهای سیاه و سفید توسط الگوریتم‌های راین‌دال با کلیدهای ثابت و متغیر، رمزگذاری شده است و در مرحله رمزگشایی از کلید دوم (کلید نادرست) استفاده شده است. این شکل نشان می‌دهد اگر در رمزگشایی با استفاده از کلید متغیر آشوب‌گونه از کلید نادرست حتی با اختلاف بسیار اندک استفاده شود، الگوی تصویر به کلی پنهان می‌شود ولی در رمزنگاری راین‌دال با کلید ثابت، الگوی تصویر حفظ می‌شود که این مسئله نقطه ضعفی برای راین‌دال محسوب می‌شود.



شکل ۱۳: نمایش حساسیت به کلید با رمزگشایی با کلید نادرست

به‌طور کلی می‌توان نتیجه‌گیری کرد که اگر داده اصلی دارای الگوی مشخص و واضحی باشد، استفاده از کلیدهای متغیر، حساسیت به کلید را افزایش می‌دهد. در غیر این صورت تاثیر چندانی بر حساسیت به کلید ندارد.

بحث و نتیجه‌گیری

این پژوهش با هدف ارزیابی و بررسی استفاده از کلید متغیر آشوب‌گونه در رمزنگاری تصویرها، با الگوریتم رمزنگاری راین‌دال صورت گرفت.

پنج دسته تصویر که دارای خصوصیات و ویژگی‌های متفاوت بودند، برای ارزیابی انتخاب شدند. بخشی از تصویرها دارای جزئیات زیاد و لبه‌های تیز (تصویرهای اولتراسوند و CT اسکن قلبی) می‌باشند؛ بخشی دیگر جزئیات متوسط و لبه‌های نرم دارند (تصویرهای صورت و شبکیه چشم) و بخشی دارای جزئیات اندک و لبه تیز (لوگوها) می‌باشند.

از شش معیار برای ارزیابی کارایی و کیفیت رمزنگاری استفاده شده است. از معیار کیفیت رمزنگاری و یا فاکتور حداکثر انحراف که معرف میزان انحراف از میانگین هیستوگرام‌های دو تصویر اصلی و رمزشده می‌باشد و فاکتور همبستگی متقابل دو تصویر، به عنوان معیارهایی با اهمیت بیشتر، استفاده شده است. از توزیع هیستوگرام و پنهان کردن الگو عمدتاً برای ارزیابی

تصویرهای با الگوی باز و از نرخ خروجی و حساسیت به کلید نیز به عنوان معیار جانبی، استفاده شده است.

ارزیابی‌ها نشان داده است که استفاده از کلید متغیر آشوب‌گونه، کیفیت رمزنگاری و همبستگی متقابل دو تصویر رمزشده و اصلی را به شدت کاهش می‌دهد.

برای تصویرهایی که دارای جزئیات اندک می‌باشند کیفیت رمزنگاری، توزیع هیستوگرام و پنهان کردن الگو بسیار قوی‌تر صورت می‌گیرد.

نتایج ارزیابی حساسیت به کلید، نشان‌دهنده بی تأثیر بودن به‌کارگیری کلیدهای متغیر آشوب‌گونه می‌باشد و استفاده از کلید آشوب‌گونه هیچ تأثیری در حساسیت به کلید الگوریتم ندارد.

به‌طور کلی می‌توان نتیجه گرفت که استفاده از رمزنگاری با کلید متغیر آشوب‌گونه، پنهان کردن الگو و کیفیت رمزنگاری (به‌ویژه برای تصویرهای دارای جزئیات اندک یا با الگوی تصویر بارز) بالاتری را با حدود ۲ درصد افزایش بار محاسباتی تضمین می‌کند. بنابراین استفاده از کلیدهای آشوب‌گونه در رمزنگاری راین‌دال تصویرها، امنیت اطلاعات را افزایش می‌دهد.

References

1. Richardson R. CSI Survey 2007. The 12th Annual computer crime and security survey. Computer security institute; 2007.
2. Richardson R. CSI computer crime and security survey. Computer Security Institute; 2008. P.1-30.
3. Machkour M, Khamlichi YI, Afdel K. Data security in medical information system. Multimedia computing and systems, 2009. ICMCS '09. International Conference on; 2009 Apr 2-4; Ouarzazate: IEEE; 2009. P. 391- 4.
4. Kovacevic S, Kovac M, Knezovic J. System for secure data exchange in telemedicine. 9th International Conference on Telecommunications; 2007 Jun 13-15; Zagreb: IEEE; 2007. P. 267-74.
5. Bouslimi D, Coatrieux G, Roux C. A joint encryption/watermarking algorithm for verifying the reliability of medical images: application to echographic images. Comput Methods Programs Biomed. 2012; 106(1):47-54.
6. Andersen J, Lo B, Yang GZ. Experimental platform for usability testing of secure medical sensor network protocols. 5th International summer school and symposium on medical devices and biosensors; 2008 June 1-3; Hong Kong: IEEE; 2008. P.179-82.
7. Lin CC, Lin PY, Lu PK, Hsieh GY, Lee WL, Lee RG. A healthcare integration system for disease assessment and safety monitoring of dementia patients. IEEE Trans Inf Technol Biomed. 2008; 12(5):579-86.
8. Dunnebeil S, Kobler F, Koene P, Krcmar H, Leimeister JM. Encrypted NFC emergency tags based on the German telematics infrastructure. 3th International workshop on near field communication. Hagenberg, Austria; 2011.p.50-5.
9. Yu WD, Jothiram V. Security in wireless mobile technology for healthcare systems. E-Health Networking, Application and Services. 9th International Conference on; 2007 Jun 19-22; Taipei: IEEE; 2007.p. 308 -11.
10. Kaufman C, Perlman R, Speciner M. Network security: private communication in a public world. 2th ed. New York: Prentice Hall Press; 2002.
11. Kahate A. Cryptography and network security. 2th ed. Tata McGraw-Hill Education; 2008.
12. Tanenbaum AS. Computer networks. 4th ed. India:Prentice Hall; 2003.
13. Menezes AJ, Van Oorschot PC, Vanstone SA. Handbook of applied cryptography discrete mathematics and its applications). 1th ed. London: Crc Press; 1997.
14. Lian S. A block cipher based on chaotic neural networks. Neurocomputing. 2009; 72(4-6):1296-301.
15. Daemen J, Rijmen V. AES proposal: Rijndael. 1th advanced encryption standard (AES) candidate Conference; 1998 Aug 20-22; Ventura California: 1998.
16. Daemen J, Rijmen V. The design of Rijndael: AES-the advanced encryption standard (Information Security and Cryptography). Berlin- NewYork: Springer; 2002.
17. Daemen J, Rijndean V. Advanced encryption standard (AES) algorithm- Rijndael as the design [M]. Tsinghua University Press; 2003.
18. Wu Q, Cao Y. An equivalent stochastic system model for control of chaotic dynamics. Decision and Control, 1995, Proceedings of the 34th IEEE Conference on; 1995 Dec 13-15; New Orleans, LA: IEEE; 1995.p. 2898 - 903.
19. Wang D, Yu J. Chaos in the fractional order Mackey-Glass system. Communications, Circuits and Systems, 2008. ICCCAS 2008.

International Conference on; 2008 May 25-27; Fujian: IEEE; 2008. P. 641- 5.
20. Kyrtsou C, Terraza M. Is it possible to study chaotic and ARCH behaviour jointly? Application of a noisy Mackey–Glass equation with heteroskedastic errors to the Paris Stock Exchange returns series. Computational Economics. 2003; 21(3):257-76.
21. Naeemabadi M, Chomachar N, Zabihi M, Ordoubadi BS, Khalilzadeh M, Ordoubadi MS. Encryption based on variable chaotic key for wireless medical data transmission. Application of information and communication technologies (AICT), 2011 5th International Conference on; 2011 Oct 12-14; Baku: IEEE; 2011. p.1-5
22. Isfahan: Milad General Hospital [cited]. Available from: www.isfahanmiladhospital.ir.
23. Siemens Global Website. Somatom Sensation, Siemens ag. [cited 2014 Dec 3] Available from:http://www.medical.siemens.com/webapp/wcs/stores/servlet/ProductDisplay?catalogId=1&catTree=12781&langId=1&productId=143945&storeId=10001.
24. Samaria FS, Harter AC. Parameterisation of a stochastic model for human face identification. Applications of Computer Vision, 1994, Proceedings of the 2th IEEE Workshop on; 1994 Dec 5-7; Sarasota, FL: IEEE;1994. p.138- 42.
25. GE Health care Product Features, LOGIQ S6. General Electric Company: [cited 2011 Dec 3] Available from:http://www.gehealthcare.com/euen/ultrasound/products/general-imaging/logiq-s6/index.html.
26. Tehran: Alzahra University Hospital, Isfahan University of Medical Science [cited]. Available from: www.alzahra.mui.ac.ir
27. Staal J, Abramoff MD, Niemeijer M, Viergever MA, Ginneken BV. Ridge-based vessel segmentation in color images of the retina. IEEE transactions on medical imaging. 2004; 23(4):501-9.
28. Ahmed HE-dH, Kalash HM, Farag Allah OS. Encryption efficiency analysis and security evaluation of RC6 block cipher for digital images. African Journal of Information and Communication Technology. 2007; 3(1):1-7.
29. Elkamchouchi H, Makar M. Measuring encryption quality for bitmap images encrypted with Rijndael and kamkar block ciphers. Radio Science Conference, 2005 NRSC 2005 Proceedings of the 22th National; 2005 Mar 15-17; Cairo, Egypt: IEEE; 2005.p. 277-84.
30. Ziedan IE, Fouad MM, Salem DH. Application of data encryption standard to bitmap and JPEG images. Radio Science Conference, 2003 NRSC 2003 Proceedings of the 20th National; 2003 Mar 18-20: IEEE; 2003. P.1-8.
31. Ahmed HE, Kalash HM, Farag Allah OS. Encryption quality analysis of the RC5 block cipher algorithm for digital images. Opt Eng. 2006; 45(10):107003-7.
32. El-Fishawy N, Abu Zaid OM. Quality of encryption measurement of bitmap images with RC6, MRC6, and Rijndael block cipher algorithms. International Journal of Network Security. 2007; 5(3):241–51.
33. Krishnamurthy GN, Ramaswamy V. Encryption quality analysis and security evaluation of CAST-128 algorithm and its modified version using digital images. International Journal of Network Security & its Applications. 2009; 1(1):28-33.
34. Krishnamurthy GN, Ramaswamy V. Performance analysis of blowfish and its modified version using encryption quality, key sensitivity, histogram and correlation coefficient analysis. International Journal of Recent Trends in Engineering. 2009; 1(2):1-4.
35. Huynh-Thu Q, Ghanbari M. Scope of validity of PSNR in image/video quality assessment. Electronics letters. 2008; 44(13):800-1.

Original Article

Journal of Health and Biomedical Informatics
Medical Informatics Research Center
2014; 1(1): 32-44

Statistical Analysis of Encryption Quality for Medical Images Based on Rijndael Encryption Algorithm Using Both Static and Chaotic Cipher Key

Mohammadreza Naeemabadi[1], Alireza Mehri Dehnavi[2,3]*, Hossein Rabbani[2,3]

• **Received:** 9 Sept, 2014 • **Accepted:** 18 Oct, 2014

Introduction: Growing application of medical information systems and various digital communication channels to transfer and share vital and medical information demonstrate the significance of medical data security and privacy policy. Nowadays several block cipher encryption algorithms secure information have done by encrypting them. Most of these algorithms are based on a block cipher that use a predetermined fixed/constant key with at least 128 bits length.
Method: In this study encryption performed by Rijndael encryption algorithm using conventional constant and variable cipher key. Mackey Glass, known as chaotic system, attached in key expansion block of Rijndael and play role in place of its conventional key expansion procedure. Mackey Glass generates series of chaotic cipher key, monitored and modified by controlling block.
Results: Both methods were evaluated by 6 individual criteria. Results have shown that variable chaotic keys are significantly successful to hide medical image pattern and histogram distribution with 2.47 percent increase in computational time where conventional Rijndael failed. Moreover this modification does not lead to considerable changes in sensitivity.
Conclusion: Employing chaotic system in Rijndael key expansion block for medical images improves security of medical information and privacy policy.

Key words: Encryption quality analysis, Encryption robustness and efficiency analysis, Medical images encryption, Chaotic encryption

•**Citation:** Naeemabadi M, Mehri Dehnavi AR, Rabbani H. Statistical Analysis of Encryption Quality for Medical Images based on Rijndael Encryption Algorithm Using both Static and Chaotic Cipher Key. Journal of Health and Biomedical Informatics 2014; 1(1): 32-44

1. M.Sc Student, Medical Engineering Department, Isfahan University of Medical sciences, Isfahan, Iran.
2. Associate Professor, Medical Engineering Department, Isfahan University of Medical sciences, Isfahan, Iran.
3. Medical Image & Signal Processing Research Center, Isfahan University of Medical Sciences, Isfahan, Iran.

***Correspondence**: Medical Engineering Department, New technologies school, Isfahan university of medical sciences, Hezar Jarib st, Isfahan, Iran.
• **Tel**: 03195016498 • **Email:** mehri@med.mui.ac.ir