مقاله پژوهشی

مجله ماشین‌بینایی و پردازش‌تصویر
سال نهم، شماره چهارم، زمستان ۱۴۰۱

طراحی روشی برای تولید کلید رمزنگاری تصادفی بیومتریک بر اساس اثر انگشت

بهرام رشیدی

چکیده

در این مقاله ما از ویژگی سیگنال های بیومتریک اثر انگشت برای تولید کلیدهای رمزنگاری تصادفی استفاده می کنیم. مهم ترین ویژگی این روش استفاده از ویژگی های منحصر به فرد اثرانگشت در تولید کلید تصادفی می باشد. حریم خصوصی کلید بیومتریک تولید شده به صورت تصادفی و پیچیدگی الگوریتمتولید کلید، جنبه های اصلی حاکم بر امنیت کلید است. در روش پشنهادی ابتدا ویژگی های منحصر به فرد اثر انگشت که شامل نقاط مینوشیا می باشد از تصویر اثرانگشت استخراج می شوند. سپس برای افزایش ویژگی های آماری و پیچیدگی، فاصله اقلیدوسی تمام نقاط مینوشیا نسبت به یکدیگر حساب شده و در یک ماتریس ذخیره می شوند. در مرحله بعد داده های این ماتریس بعد از نرمالیزه شدن به اعداد ۸-بیتی توسط عملیات جایگشت جابجا می شوند. سپس برای افزایش سطح امنیت و قابلیت تصادفی بودن از عمل غیر خطی S-box ۸-بیتی استفاده شده در رمز قالبی AES استفاده شده است. بدین صورت که داده های ۸-بیتی هر یک جداگانه به S-box اعمال می شوند و نتیجه ذخیره می شود. در نهایت داده های بدست آمده از بایت کم ارزش تا بایت پر ارزش در دسته های ۱۲۸-بیتی یا ۱۹۲-بیتی یا ۲۵۶-بیتی می توانند به عنوان کلید در سیستم های رمزنگاری مورد استفاده قرار گیرند. آنالیزهای آماری که روی کلیدهای تولید شده صورت گرفته نشان دهنده ویژگی تصادفی بودن قابل قبول کلیدها می باشد. بنابراین ساختار پیشنهادی برای تولید کلید تصادفی می تواند در رمزنگاری سیگنال های دیجیتال با حجم زیادی از داده مانند تصویر و صدا استفاده شود.

کلیدواژه‌ها

اثر انگشت، کلید رمزنگاری تصادفی، سیستم رمزنگاری قالبی، مولد تولید کلید.

۱ مقدمه

امروزه سیستم های رمزنگاری نقش مهمی در ایمن سازی اطلاعات در هنگام انتقال یا ذخیره سازی دارند. کلیدهای رمزنگاری هسته اصلی این سیستم ها هستند. محرمانه بودن این کلیدها باید بسیار مد نظر قرار بگیرد. اما تولید و ذخیره امن کلید متقارن برای سیستم کلید متقارن و کلید خصوصی برای سیستم کلید نامتقارن یک چالش مهم است. امنیت الگوریتم رمزنگاری بر اساس عملکرد آماری کلید های تصادفی آن است. تولید یک کلید تصادفی با کیفیت بالا کاری دشواری است که سطح امنیت ارائه شده توسط الگوریتم رمزنگاری را افزایش می دهد. برای بهبود امنیت یک سیستم رمزنگاری، کلیدهای مورد استفاده در رمزنگاری باید تصادفی باشد و به اندازه کافی به لحاظ تعداد بیت طولانی باشند که قابل شکستن نباشد. بسیاری از تکنیک های رمزگذاری مانند رمزهای قالبی سبک [۱]-[۲] برای محافظت از داده ها در سیگنال های دیجیتال و کاهش هزینه های مصرف سخت افزار ارائه شده است. همچنین، نحوه انجام رمزگذاری تصویر [۳]-[۷]

این مقاله در آبان‌ماه ۱۴۰۰ دریافت، در دی‌ماه بازنگری و در بهمن‌ماه پذیرفته شد.

[۱] دانشگاه آیت الله العظمی بروجردی (ره)، دانشکده فنی و مهندسی، گروه مهندسی برق
رایانامه: b.rashidi@abru.ac.ir

DOR: dorl.net/dor/20.1001.1.23831197.1401.9.4.1.8

و رمزگذاری صوت [۸]-[۱۱] به موضوعات لازم و ضروری تبدیل شده اند. تولید کلیدهای تصادفی در این سیستم ها یک عمل مهم است.

سه دسته اصلی برای تولید کلید تصادفی وجود دارد که شامل ۱- تولید کلید مبتنی بر تئوری آشوب: در این روش از معادلات ریاضی مانند نقشه Cat و نقشه Baker برای ایجاد آشفتگی[1] استفاده می شود. سیستم های آشوب ویژگی های مشابهی از حساسیت به شرایط اولیه و پارامترهای کنترل و رفتار شبه-تصادفی را فراهم می کند، که نیازهای آشفتگی و پخش[2] در رمزنگاری را برآورده می کند. ۲- تولید کلید رمزنگاری مبتنی بر بیومتریک: روشی است که از اطلاعات بیومتریک برای تولید کلیدهای رمزنگاری برای محافظت از امنیت داده ها استفاده می کند. سیستم های رمزنگاری بیومتریک (زیستی) یک زمینهتحقیقاتی در حوضه رمزنگاری است که در آن از بیومتریکیکفرد برای ایمن سازی تولید این کلیدهای رمزنگاری استفاده می شود.۳- تولید کلید بر اساس مولدهای اعداد تصادفی: در این روش از مولد اعداد شبه-تصادفی و شیفت رجیستر بازخوردی خطی (LFSR) برای تولید کلیدهای تصادفی استفاده می شود.

تکنیک های زیادی برای تولید کلید رمزنگاری [۶] و [۱۲]-[38] پیشنهاد شده اند. به عنوان مثال، در [۶] یک سیستم آشوب ۴ بعدی با استفاده از سیگنال زمان گسسته سیستم بی نظم برای تولید کلید ارائه شده است. در [۱۲] نویسندگان کلیدهای بیومتریک را از بردارهای ویژگی بیومتریک عنبیه تولید می کنند. در [۱۳] مکانیسم بازسازی کلید فازی برای استخراج یک الگوی محافظت شده استفاده شده است. سپس، خطای تصحیح کد (ECC) برای تولید کلیدهای تصادفی استفاده می شود. در [۱۴] ساختاری برای استخراج داده های الکتروانسفالوگرافی انسان (EEG) به عنوان بیومتریک برای تولید کلید پیشنهاد شده است. این ساختار پتانسیل بالایی را فراهم می کند زیرا جعل و تقلب در EEG غیرممکن است. در [۱۵] نویسندگان با انجام آزمایشی با استفاده از نمونه های سیگنال صوت برای تولید کلید الگوهای بیومتریک تصادفی را استفاده می کنند. در [۱۶] سیستم تولید کلید از داده های بیومتریک عنبیه استفاده می کند. در [۱۷] ساختار تولید کلید با عبور سیگنال صوتی در چندین مرحله بر اساس تئوری گراف تحقق می یابد. در [۱۸] روشی برای تولید یک کلید رمزنگاری برای رمزگذاری داده ها با استفاده از خصوصیات چهره انسان ارائه شده است. نویسندگان از این کلید برای رمزگذاری پیام های صوتی و پنهان کردن آنها در داخل تصاویر رنگی استفاده کرده اند. در [۱۹] تولید یک کلید ساده مخفی با استفاده از ترکیبی از روش پیش پردازش با کمی سازی چند سطح برای امنیت لایه فیزیکی ارائه شده است. در [۲۰] روشی برای تولید کلیدهای تصادفی ۲۵۶ بیت بر اساس صدای انسان پیشنهاد شده است. در [۲۱] کلیدهای امن رمزنگاری شده براساس توابع درهم تولید می شوند. چندین رویکرد تولید کلید رمزنگاری از ویژگی های بیومتریک اثر انگشت را می توان در کارهای[۲۳]-[۳۲]یافت. در [۲۴] رویکردی را برای تولید کلید رمزنگاری از الگوی اثرانگشت قابل لغو[3]برای هر دو طرف ارتباط پیشنهاد شده است. در [۲۵] از ویژگی‌های آماری مبتنی بر اثر انگشت برای تولید کلمه کد[4]یک کاربر استفادهمی شود. برای تولیدیک کلمه کد، از کدینگ-Reed Solomon (RS) استفاده میشود. سپس از این کلمه کد برای تولیدیک کلید استفاده می شود. در [۳۱] یک رویکرد تولید کلیدبر اساس اثر انگشت با استفاده از فواصل نسبی بین جزئیات اثر انگشت کاربر برای ایجاد یک کلیدبیومتریک منحصر به فرد استفاده شده است. علاوه بر این، از یک تکنیک تصحیح خطای دو لایه برای افزایش قابلیت اطمینان سیستم در طول انتقال داده استفاده میشود. در [۳۲] یک روش برای تولید کلید رمزنگاری بر اساس ویژگی‌های اثر انگشت و الگوریتم آستانه[5] پیشنهاد می کند.

سیستم های رمزنگاری مانند رمزگذاری سیگنال تصویر و رمزگذاری سیگنال صوت برای انجام نقل و انتقال اطلاعات به یک واحد تولید کننده کلید تصادفی نیاز دارند[۲۳] و [۲۴]. با استفاده از تولید کلید تصادفی می توان امنیت الگوریتم های رمزنگاری را بهبود بخشید. این مقاله الگوریتم تولید کلید تصادفی را بر اساس ویژگی های منحصر به فرد اثر انگشت پیشنهاد می کند. حریم خصوصی کلید بیومتریک تولید شده به صورت تصادفی و پیچیدگی الگوریتمتولید کلید، جنبه های اصلی حاکم بر امنیت کلید است.در این الگوریتم، ما ساختار جدید پیشنهادی را برای تولید کلید تصادفی بر اساس ویژگی های منحصر به فرد اثر انگشت و بلوک های سازنده ای از قبیل واحد محاسبه فاصله اقلیدوسی نقاط مینوشیا و نرمالیزاسیون، واحد جایگشت و واحد اعمال بلوک S-box مورد استفاده در رمز AES [39] به داده ها ارائه می دهیم. این ساختار می تواند کلید هایی با طول‌های مختلف ایجاد کند. طول کلیدهای تولید شده برابر با ۱۲۸، ۱۹۶ و ۲۵۶ بیت است. برای افزایش ویژگی های آماری و پیچیدگی فاصله اقلیدوسی تمام نقاط مینوشیا نسبت به یکدیگر حساب شده و در یک ماتریس ذخیره می شود. داده های این ماتریس بعد از نرمالیزه شدن به اعداد ۸-بیتی توسط عملیات جایگشت جابجا می شوند. سپس برای افزایش سطح امنیت و قابلیت تصادفی بودن از عمل غیر خطی S-box ۸-بیتی استفاده شده در رمز قالبی AES استفاده شده است. بدین صورت که داده های ۸-بیتی هر یک جداگانه به S-box اعمال می شوند و نتیجه ذخیره می شود. آنالیزهای آماری که روی کلیدهای تولید شده صورت گرفته نشان دهنده ویژگی تصادفی بودن قابل قبول کلیدها می باشد.

[1] confusion
[2] diffusion

[3] Cancelable fingerprint template
[4] Codeword
[5] Threshold

در ادامه مقاله در بخش دوم به طور خلاصه روند استخراج ویژگی های اثر انگشت توضیح داده شده است.روش تولید کلید تصادفی پیشنهادی در بخش سوم ارائه شده است. بخش چهارم نتایج و بحث در مورد روش پیشنهادی را نشان می دهد. سرانجام، مقاله در بخش پنجم جمع بندی می شود.

۲ استخراج ویژگی های اثر انگشت

هر اثر انگشت یکی از پرکاربردترین شکل شناسایی بیومتریک است که بیش از یک قرن است که مورد استفاده قرار می گیرد. اثر انگشت هر انسان منحصر به فرد است و در طول زندگی فرد بدون تغییر باقی می ماند. اثر انگشت از الگوی برآمدگی هایروی انگشت شکل می گیرد.برای هر اثر انگشت یک فرد ویژگی های منحصر به فردی مانند: ۱- هر اثر انگشت برای افراد منحصر به فرد است، یعنی هیچ دو انگشتی دارای ویژگی های برآمدگی یکسان نیستند. ۲- بسیار قابل اعتماد هستند زیرا هیچ دو نفر اثر انگشت مشابهی ندارند. حتی دوقلوهای همسان که DNA مشابهی دارند، اثر انگشت متفاوتی دارند. ۳- اثر انگشت از نظر ساختاری در طول زندگی فرد بدون تغییر باقی می ماند. ۴-یکی از دقیق ترین اشکال بیومتریک موجود است. ۵- به دست آوردن اثر انگشت راحت است و از این رو گزینه خوبی برای سیستم های امنیتی است.

به رگه هایی که به صورت موازي در اثر انگشت وجود دارند، کهدر مواردی خاتمه می یابند و گاهی اوقات دو شاخه می شوند مینوشیا گفته می شود. شکل ۱ نمونه ای از نقاط مهم مینوشیا یک اثر انگشترا نشان می دهد. در این مثال، پیکسل های سفید با برجستگی ها و پیکسل های سیاه مربوط به دره ها هستند.از بین انواعمینوشیا دو نوع مینوشیای انتهایی و مینوشیای دوشاخه ای بیشتر کاربرد دارد. در مرحله استخراج ویژگی های اثر انگشت مختصات این نقاط بدست می آید. در این مقاله ما از روش ارائه شده در کار [40] برای بهبود تصویر و استخراج نقاط مینوشیا استفاده می شود. قبل از استخراج نقاط مینوشیا نیاز می باشد که بر حسب نیاز بهبودها و پیش پردازش هایی بر روی تصویر اثر انگشت صورت پذیرد. در ادامه به طور خلاصه این پیش پردازش ها توضیح داده شده اند.

شکل ۱: نقاط مهم مینوشیا در یک اثر انگشت.

۲.۱.مرحله پیش پردازش

مرحله پیش پردازش برای بهبود تصویر و برجسته کردن ویژگی بیومتریک اثر انگشت انجام می شود. به عبارت دیگر بهبود تصویر اثرانگشت برای حذف نویز ناشی از حسگر و تغییرات ناشی از فشار انگشت روی سنسور صورت می پذیرد.ویژگی‌های بیومتریک اثر انگشت باید تقویت شوند تا بتوان از آنها برای تجزیه و تحلیل بیشتر استفاده کرد. این فرآیند با حذف پیکسل های اضافی از تصویر و رسیدن به روشنایی و کنتراست بهتر انجام می شود.چند مرحله مهم پیش پردازش روی تصویر اثر انگشت مانند افزایش کنتراست، باینریزه کردن[1] و نازک سازی[2] انجام می شود. افزایش کنتراست کیفیت اثر انگشت را با کاهش اثرات نامطلوب تاری، منافذ و برجستگی های اولیه بهبود می بخشد. این امر به بهبود تشخیص نقاط مینوشیا کمک می کند. در بین روش هایی که تا کنون براي افزایش کیفیت اثر انگشت ارائه شده است سه روش وجود دارد که اساس کار در روش هاي دیگر می باشند. این سه روش عبارتند از: یکنواخت سازی هیستوگرام (این روش ساده ترین روش افزایش کیفیت اثر انگشت می باشد که استفاده می شد اما برای تصاویري با کیفیت کم کارآیی خود را از دست می دهد)، تبدیل فوریه سریع و فیلتر گابور.

در کار [40] براي افزایش کیفیت تصویر از روش تبدیل فوریه استفاده می شود.شکل ۲ (a) و (b) به ترتیب تصویر یک اثر انگشت (این تصویر از پایگاه داده[41] استفاده شده است.) و تصویر بهبود داده شده توسط روش تبدیل فوریه را نشان می دهد. همانطور که در تصویر دیده می شود اعمال تبدیل فوریه باعث شده است تا نقاط شکسته در رگه ها به هم متصل شوند و اتصالات اشتباه بین رگه ها از بین رود.

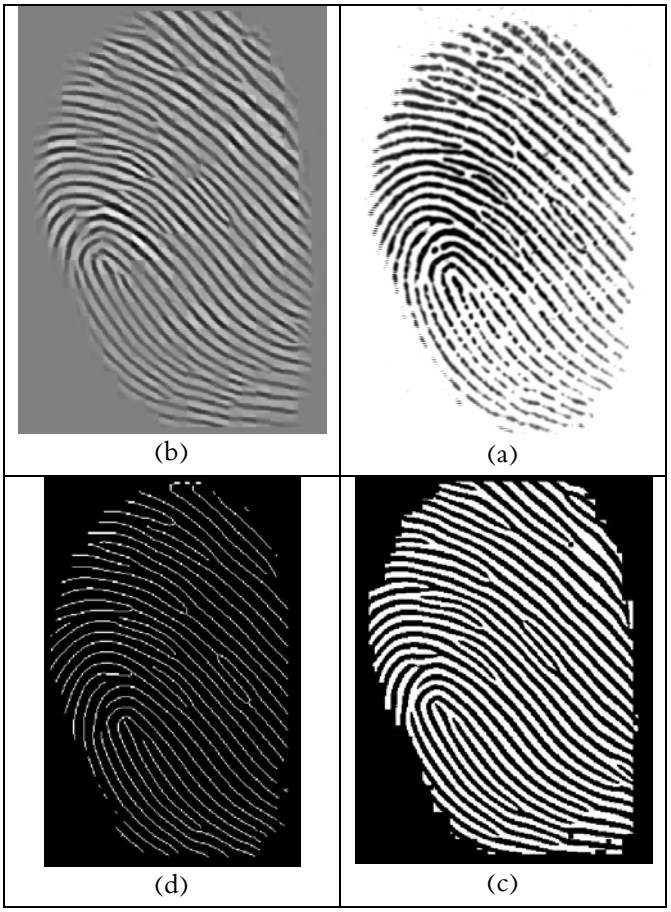
[1] Binarization
[2] Thinning

- **باینریزه کردن تصویر**

هدف از این مرحله به دست آوردن یک تصویر باینری است. می توان یک مقدار آستانه را انتخاب کرد و تمام پیکسل های بالای آن مقدار را سفید و زیر آن مقدار را سیاه کرد. این فرآیند یکی از ساده‌ترین فرآیندها برای باینریزه کردن است.این عمل تصویر اثر انگشت خاکستری را به یک تصویر باینری حاوی برجستگی ها و فرورفتگی ها (دره ها) تبدیل می کند. شکل ۲ (c) تصویر باینریزه شده اثر انگشت را نشان می دهد.

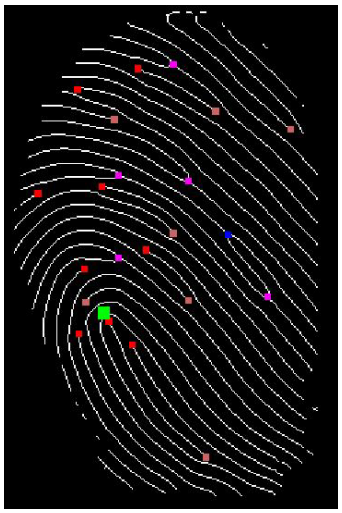
- **نازک سازی**

در فرایند نازک سازی (اسکلت سازی) تمام خطوط موجود در تصویر باینریزه شده به ضخامت یک پیکسل متراکم می شوند. نازک شدن عرض خطوط برآمدگی باینری شده را به ۱ پیکسل کاهش می دهد. فرآیندهایباینریزه کردن و نازک سازی برای مکان یابی نقاط مینوشیا مورد نیاز هستند. شکل ۲ (d) تصویر نازک سازی شده اثر انگشت را نشان می دهد.



شکل۲: (a): تصویر اصلی، (b): تصویر بعد از تبدیل فوریه سریع، (c): تصویر بعد از باینری سازی و (d): تصویر بعد از نازک سازی.

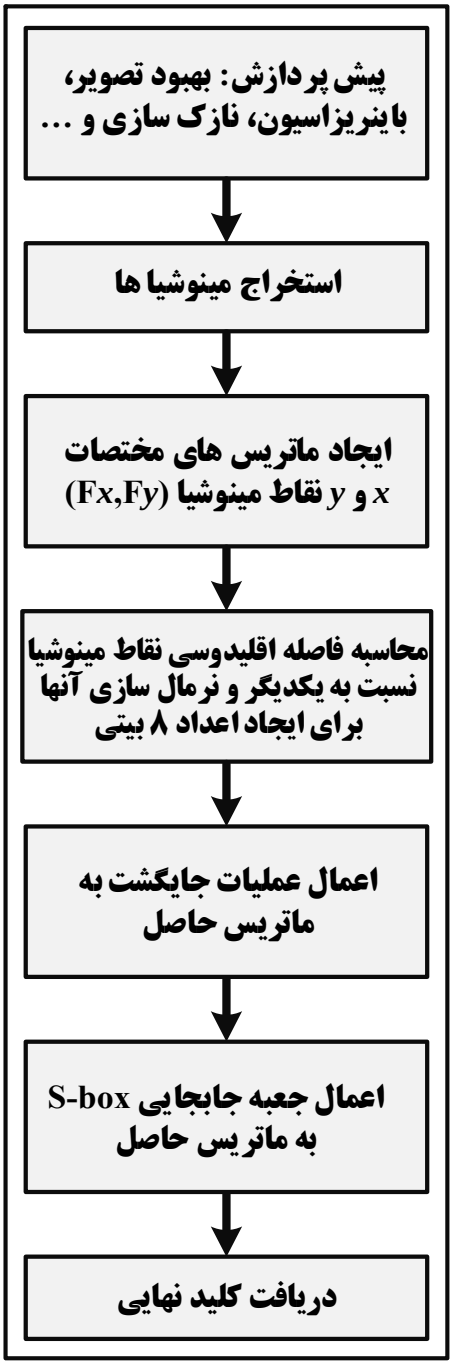
نقاط مینوشیا در شکل ۳ برای تصویر اثر انگشت ارائه شده در شکل ۲ (a)نشان داده شده اند. بیشترین نقاط مینوشیا، انتهایی و دوشاخه ای هستند. همانطورکه دیده می شوداین نقاط انتهایی و دو شاخه ای در شکل شناسایی شده اند. تصویر باینری نازک شده برای شناسایی الگوی پیکسلی محلی که در آن برآمدگی(نقاط با مقدار ۱) به پایان می رسد یا شکاف میابد، تجزیه و تحلیلو شناسایی می شود. در مرحله بعد، تمام نقاط میونشیا نادرست مانند (مینوشیا های جانبی، نقاط شناسایی شده در مناطق با کیفیت پایین، جزایر، دریاچه ها و غیره) حذف می شوند.



شکل۳: تصویر نقاط مینوشیا تشخیص داده شده از تصویر اثر انگشت شکل ۲ (a).

۳. روش پیشنهادی تولید کلید رمزنگاری بیومتریک از اثر انگشت

در این مقاله، تلاش شده است تا یک کلید رمزنگاری مستقیماً از ویژگی‌های منحصر به فرد استخراج شده اثر انگشت فرد تولید شود. در این رویکرد، اثر انگشت به عنوان یک پارامتر بیومتریک برای تولید کلید رمزنگاری استفاده می‌شود. در این روش ما از مختصات نقاط مینوشیا ها برای تولید کلید استفاده می کنیم. نمای کلی از مراحل روش پیشنهادی به صورت شماتیک در شکل ٤ نشان داده شده است. بعد از استخراج نقاط مینوشیا مختصات این نقاط بدست می آید. مولفه x و y نقاط مختصات بترتیب در ماتریس های F_x, F_y ذخیره می شوند. در مرحله بعد به محاسبه فاصله اقلیدوسی نقاط مینوشیا نسبت به یکدیگر و نرمال سازی مقدار فاصله برای ایجاد اعداد ۸ بیتی پرداخته می شوند و نتایج در یک ماتریس ذخیره می شود. بعد از این مرحله به ماتریس حاصل عمل جایگشت اعمال می شود. در مرحله بعد برای افزایش تصادفی شدن اعداد هر مقدار ۸-بیتی در ماتریس بعد از جایگشت به جعبه جابجای S-box ۸-بیتی استفاده شده در رمز قالبی AES [39] اعمال می شوند. در مرحله بعد بایت های کلیدها را می توان از مقادیر ماتریس بدست آمده در مرحله قبل بدست آورد. در روش پیشنهادی با انجام مراحل محاسبه فاصله اقلیدوسی بین نقاط مینوشیا، عمل جایگشت و عملS-box میزان تصادفی بودن کلید را افزایش می یابد.



شکل ۴:نمای کلی از مراحل روش پیشنهادی تولید کلید بر اساس اثر انگشت.

الگوریتم ۱ روش پیشنهادی تولید کلید تصادفی را بر اساس مختصات نقاط مینوشیا $f(x_i,y_i)$ $1 \le i \le D$ که در آن D تعداد نقاط مینوشیا است، نشان می دهد.

الگوریتم ۱: تولید کلید تصادفی بر اساس مختصات نقاط مینوشیا $f(x_i,y_i)$ $1 \le i \le D$ که در آن D تعداد نقاط مینوشیا است.

Input: Input x-coordinate F_x and y-coordinate F_y matrices of the Minutiae.
Output: 128-bit Random Key K_j, $0 \le j \le m/16$.

1. f=2; $m = (D*(D-1))/2$; n=1;
2. **For** i **from** 1 **to** $m-1$ **do** // **Step 1.**
3. **For** j **from** f **to** m **do**
4. $D_p(n) = \sqrt{(F_x(i)-F_x(j))^2+(F_y(i)-F_y(j))^2}$
5. $n = n+1$;
6. **End For**;
7. $f = f+1$;
8. **End For**;
9. **For** i **from** 1 **to** m **do** // **Step 2.**
10. $D_{p1}(i) = D_p(i) \bmod 2^8$;
11. **End For**;
12. $D_{p2}(i) = Permutation(D_{p1}(i))$; // **Step 3.**
13. **For** i **from** 1 **to** m **do** // **Step 4.**
14. $D_{p3}(i) = S-box(D_{p2}(i))$;
15. **End For**;
16. **For** i **from** 1 **to** m **do** // **Step 5.**
17. $Key(i) = D_{p3}(i)$;
18. **End For**;
19. **For** j **from** 1 **to** $m/16$ **do** // **For 128-bit keys.**
20.
21. $i = i+16$;
22. **End For**;

۳.۱. ماتریس های مختصات نقاط مینوشیا و محاسبه فاصله اقلیدوسی

هر مینوشیا استخراج شده از یک تصویر اثر انگشت به صورت مختصات x و y نشان داده می شود. بعد از استخراج نقاط مینوشیا محتصات x و y این نقاط را برای محاسبات بعدی مورد استفاده قرار می شود. فرض کنید مجموعه نقاط مینوشیا با F نمایش داده شود و $f(x_i,y_i)$ مختصات یک نقطه مینوشیا f باشد. در اینجا مجموعه نقاط مینوشیا را با عبارت زیر نمایش می شود:

$$F = \{f1(x_1,y_1), f2(x_2,y_2), f3(x_3,y_3), \ldots, fm(x_m,y_m)\}$$

در ادامه نقاط مینوشیا استخراج شده را در دو بردار متفاوت F_x, F_y ذخیره می شود. بردار F_x شامل تمام مقادیر مختصات x و بردار F_y حاوی همه مقادیر مختصات y است.

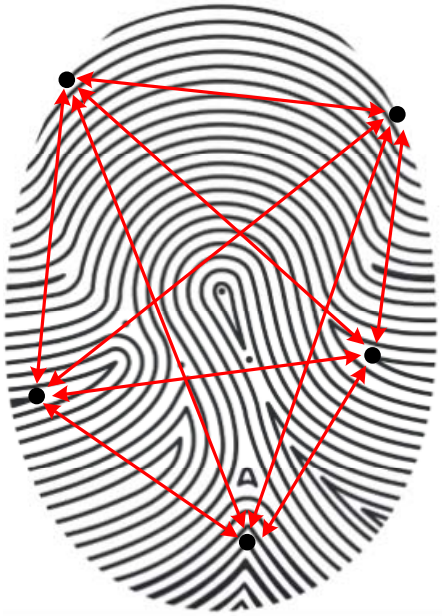
$$F_x = [x_1, x_2, x_3, \ldots, x_m]$$

$$F_y = [y_1, y_2, y_3, \ldots, y_m]$$

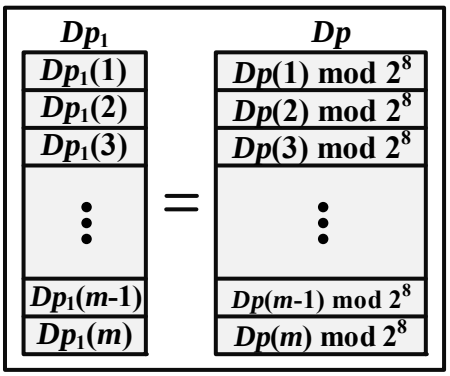
حال فاصله اقلیدوسی بین تک تک نقاط مینوشیا حساب و در یک ماتریس ذخیره می شود. فاصله اقلیدوسی دو نقطه فرضی بر اساس بردارهای F_x, F_y در زیر نشان داده شده است:

$$L_p(n) = \sqrt{(F_x(i) - F_x(j))^2 + (F_y(i) - F_y(j))^2}$$

همان طور که می دانیم تعداد فاصله های اقلیدوسی بین D نقطه مینوشیا نسبت به هم برابر $\binom{D}{2} = \frac{D(D-1)}{2}$ می باشد. شکل ۵ فاصله اقلیدوسی بین چند نقطه میونشیای فرضی در یک تصویر سمبولیک اثر انگشت را نشان می دهد. در بسیاری از تصاویر اثر انگشت تعداد نقاط مینوشیا محدود می باشد و این امر ممکن است میزان تصادفی بودن و نتایج تحلیل های آماری داده های کلید را دچار ضعف کند. استفاده از فاصله اقلیدوسی بین تمام نقاط نسبت به یکدیگر علاوه بر حفظ ویژگی منحصر به فرد بودن پارامترهای اثر انگشت باعث افزایش تعداد داده های استخراجی از اثر انگشت برای تولید کلید می شود. این امر میزان تصادفی بود و نتایج آماری داده های ماتریس کلید و الگوی بیتی آن را بهبود می دهد. به عنوان مثال اگر یک اثر انگشت ۸۰ نقطه مینوشیا داشته باشد تعداد داده های مربوط به فاصله اقلیدوسی تمام نقاط نسبت به یکدیگر برابر ۳۱۶۰ می باشد که این عدد نسبت به تعداد داده خام مختصات نقاط مینوشیا بسیار بزرگتر می باشد. برای نمایش هر داده در ماتریس فاصله اقلیدوسی Dp در قالب یک عدد ۸-بیتی باقیمانده هر داده نسبت به عدد 2^8 بدست آورده شود. این کار در شکل ۶ نشان داده شده است. مقادیر ۸-بیتی ماتریس Dp در ماتریس جدید Dp_1 ذخیره می شوند.



شکل 5:فاصله اقلیدوسی بین چند نقطه میونشیای فرضی در یک تصویر سمبولیک.



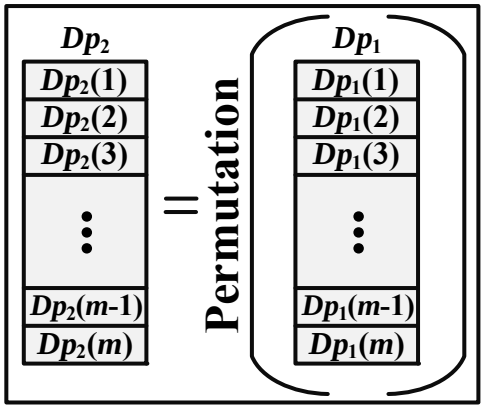
شکل ۶:روند ۸-بیتی کردن اعداد بدست آمده برای ماتریس فاصله اقلیدوسی.

۳.۲. اعمال جایگشت ها

در این مرحله، یک جایگشت برای مقادیر تولید شده (ماتریس Dp_1) در مرحله قبل اعمال می شود. بنابراین، عمل جایگشت با تکرار Pr برای تولید ماتریس Dp_2 ارائه داده شده است. عمل جایگشت برای ماتریس Dp_2 نمونه i از ماتریس Dp_1 را به موقعیت $Pr(i)$ ماتریس Dp_2 به شرح زیر انتقال می دهد:

$$Pr(i) = \begin{cases} (i+5) \times \frac{m}{9} \bmod m - 1 & if\ i \in \{1,2,\ldots,m-1\} \\ m & if\ i = m. \end{cases}$$

مقدار mبرابر با تعداد داده های ماتریس Dp_1 است. شکل ۷ مرحله اعمال جایگشت در روش تولید کلید تصادفی پیشنهادی را نشان می دهد. همانطور که از شکل مشخص است، مقادیر ماتریس Dp_1بر اساس جایگشت $Pr(i)$ به ترتیب برای تولید ماتریس Dp_2 استفاده می شوند.

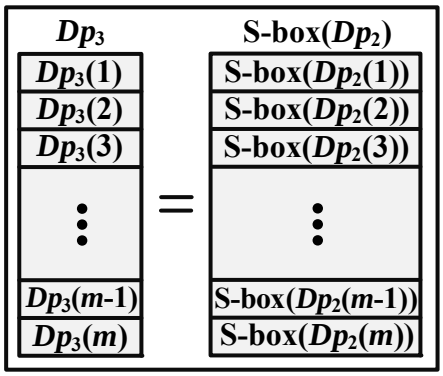


شکل ۷:مرحله جایگشتروش تولید کلید تصادفی پیشنهادی.

۳.۳. اعمال جعبه هاي جابجايي S-box

در این مرحله مقادیر ۸-بیتی ماتریس $Dp_2(i)$، $1 \leq i \leq m$ به ترتیب به S-box ۸-بیتی مورد استفاده در رمز قالبی استاندارد AES اعمال می شوند و ماتریس جدید $Dp_3(i)$، $1 \leq i \leq m$ را ایجاد می کند. هدف از این کار افزایش میزان پیچیدگی داده های

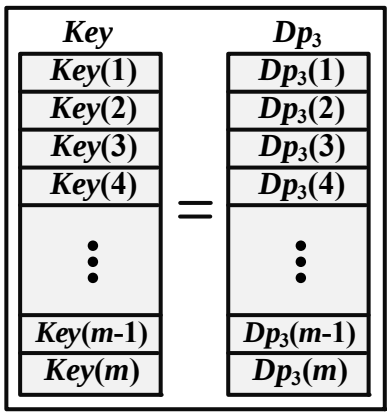
کلید می باشد. این S-box یکی از بهترین S-boxهای ۸-بیتی موجود می باشد که دارای مشخصه های امنیتی بسیار قابل قبولی می باشد. به همین دلیل در این کار از S-box ۸-بیتی رمز کلید متقارن AES استفاده شده است. ساختار این S-box بر اساس واحد معکوس کردن میدانی در میدان متناهی $GF(2^8)$ می باشد که دارای خصوصیات غیرخطی خوبی است. شکل ۸ مرحله اعمال جعبه جابجایی S-box به ماتریس Dp_2 را نشان می دهد. در این حالت ۸ بیت وارد S-box شده و ۸ بیت بر اساس جدول آن [39] تولید و خارج می شود.



شکل ۸:مرحله اعمال S-box-۸-بیتی AES به ماتریس Dp_2.

۳.۴. انتخاب مقادیر کلید

در این مرحله، مقادیر ماتریس Dp_3 برای ایجاد کلید استفاده می شوند. بر حسب اینکه کلید چند بیتی باشد می توان مقادیر مختلفی را انتخاب کرد. به عنوان مثال، برای طول کلید های ۱۲۸-بیتی، ۱۹۲-بیتی و ۲۵۶-بیتی به ترتیب ۱۶، ۲۴ و ۳۲ بایت از ماتریس Dp_2 نیاز می باشد. مقادیر ۸-بیتی برای تولید خروجی های نهایی کلید $Key\ (i)$، $1 \le i \le m$ از ماتریس Dp_2در شکل ۹ نشان داده شده است.جدول ۱ انتخاب بایت های کلید $Key(i)$ برای تولید کلیدهای ۱۲۸-بیتی، ۱۹۲-بیتی و ۲۵۶-بیتی را نشان می دهد.



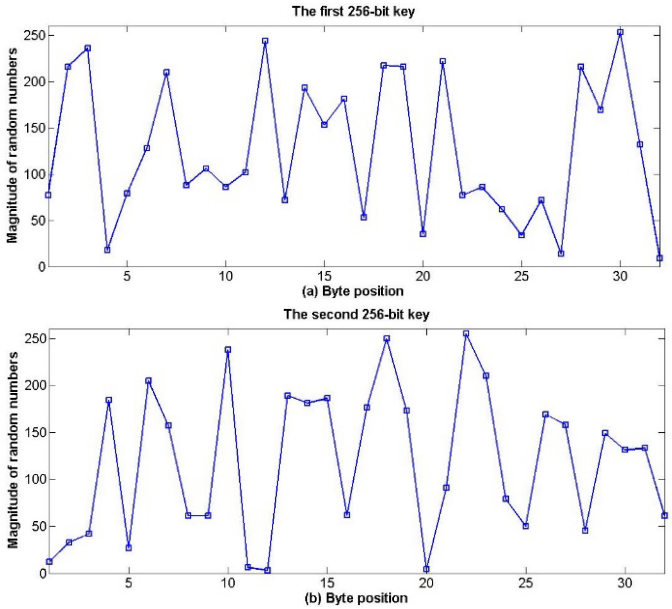
شکل ۹:مرحله اعمال S-box-۸-بیتی AES به ماتریس Dp_2.

جدول ۱: انتخاب بایت های کلید $Key\ (i)$ برای تولید کلیدهای ۱۲۸-بیتی، ۱۹۲-بیتی و ۲۵۶-بیتی.

Keys	128-bit
K_1	$[(Key(16)\|\|Key(15)\|\|...\|\|Key(1)]$
K_2	$[(Key(32)\|\|Key(31)\|\|...\|\|Key(17)]$
K_3	$[(Key(48)\|\|Key(47)\|\|...\|\|Key(33)]$
…	…
K_K	$[Key(m-1)\|\|Key(m-2)\|\|...\|\|Key(m-16)]$
Keys	**192-bit**
K_1	$[(Key(24)\|\|Key(23)\|\|...\|\|Key(1)]$
K_2	$[(Key(48)\|\|Key(47)\|\|...\|\|Key(25)]$
K_3	$[(Key(72)\|\|Key(71)\|\|...\|\|Key(49)]$
…	…
K_K	$[Key(m-1)\|\|Key(m-2)\|\|...\|\|Key(m-24)]$
Keys	**256-bit**
K_1	$[(Key(32)\|\|Key(31)\|\|...\|\|Key(1)]$
K_2	$[(Key(64)\|\|Key(63)\|\|...\|\|Key(33)]$
K_3	$[(Key(96)\|\|Key(95)\|\|...\|\|Key(65)]$
…	…
K_K	$[Key(m-1)\|\|Key(m-2)\|\|...\|\|Key(m-32)]$

۴. بحث و نتایج

این بخش، تجزیه و تحلیل های مختلفی برای روش تولید کلید تصادفی پیشنهادی با استفاده از اثر انگشت ارائه می شود. در اینجا، از ابزار شبیه سازی Matlab R2013b برای این کار استفاده شده است.پایگاه داده ای که تصاویر اثر انگشت از آن استفاده شده است پایگاه داده شناخته شده FVC2002 DB1_B [41] می باشد.در این پایگاه داده ۸۰ اثر انگشت از ۱۰ نفر (۸ نمونه برای هر فرد)قرار داده شده است.اندازه هر اثر انگشت ۳۸۸×۳۷٤ است که با ۵۰۰ نقطه در اینچ (dpi) گرفته شده اند.شکل های ۱۰ (a) و (b) به عنوان مثالبه ترتیب، کلیدهای تصادفی اول و دوم ۲۵۶-بیتی بر اساس تصویر اثرانگشت 108_1.tifرا نشان می دهد. همان طورکه دیده می شود شکل مقادیر کلید مانند یک سیگنال تصادفی است.



شکل ۱۰:نمودار کلیدهای استخراج شده از روش تولید کلید پیشنهادی اول (a) ودوم (b)، ۲۵۶-بیتی بر اساس تصویر اثرانگشت 108_1.tif.

در کارهای [۶]-[۱۱]، [34]-[36] و [38]از تئوری آشوب برای تولید کلید استفاده کرده اند. در [۸] از معادلات ریاضی مانند نقشه Cat و نقشه Zaslavskyبرای ایجاد آشفتگی و تولید کلید تصادفی استفاده می شود.در [۱۱] از نگاشت های مختلف بر اساس تئوری آشوب برای تولید کلید استفاده کرده است. در[34]از سیستم‌های آشوب مرتبه کسری برای تولید کلیدهای رمزگذاری استفاده شده است.در [۳۵] یک مولد کلیدرمزنگاری با استفاده از تئوری آشوب بر اساس ایجاد آشوب در یک فیلتر دیجیتال برای رمزگذاری و رمزگشایی داده ها ارائه شده است.در[36] یک نگاشت سینوسی بهبود یافته به عنوان یک مولد کلید ارائه شده است. در [۳۸] نوعی سیستم تولید متوالی کلید بر اساس تئوری آشوبها استفاده ازn-ترکیب از نگاشتهای آشوب طراحی شده است که مزایای تئوری آشوب را با رمزنگاری مدرن ترکیب می کند.

همچنین چندین روش تولید کلید رمزنگاری از ویژگی های بیومتریک اثر انگشت را می توان در کارهای[۲۳]-[۳۲]یافت.به عنوان مثال، در [۲۴] رویکردی را برای تولید کلید رمزنگاری از الگوی اثرانگشت قابل لغو برای هر دو طرف ارتباط پیشنهادشده است. در [۲۵] از ویژگی‌های آماری مبتنی بر اثر انگشت برای تولید کلمه کد یک کاربر استفادهمی شود. سپس از این کلمه کد برای تولیدیک کلید استفاده می شود. در [۳۱] یک رویکرد تولید کلیدبر اساس اثر انگشت با استفاده از فواصل نسبی بین جزئیات اثر انگشت کاربر برای ایجاد یک کلید بیومتریک منحصر به فرد استفاده شده است. علاوه بر این، از یک تکنیک تصحیح خطای دو لایه برای افزایش قابلیت اطمینان سیستم در طول انتقال داده استفاده میشود.در ادامه این بخش ضمن انجام تحلیل تصادفی مقایسه با کاری مرتبط پیشین انجام شده است.

زمان محاسبه کلید رمزنگاری برای کار پیشنهادی و چند کار موجود در جدول ۲ آورده شده است. در این جدول برای مقایسه بهتر سخت افزار مورد استفاده نیز بیان شده است. همان طور که مشاهد می شود زمان لازم برای محاسبه کلید در کار پیشنهادی قابل قبول می باشد.

جدول ۲ : مقایسه زمان محاسبه کلید رمزنگاری برای کار پیشنهادی و چند کار موجود.

سخت افزار	زمان (میلی ثانیه)	کار
---	۲۹,۸۰۸۵	[۲۴]
Intel® Core TM i5 processor with 2.3 GHz	۱۰,۱۱	[۲۳]
Intel ®Core TM 2 Duo processor with 2.4 GHz	۶۰,۰۵۲	[42]
ARM processor Broadcom SoC BCM2837B0 of 1.4GHz	14	[34]
Intel® Core TM i5 processor with 2.3 GHz	۱۶,۴۵	کار پیشنهادی

۴.۱.تحلیل تصادفی

برای بررسی تصادفی بودن توالی مقادیر بیت های کلید تجزیه و تحلیل آماری بر اساستست های که در کار [38] ارائه شده و بعضی پارامترهای دیگر انجام می گیرد. در ادامه تست های مورد نظر و پارامترهای مهم در این زمینه مورد بررسی بیشتری قرار گرفته است.در اینجا ما ارزیابي هاي مختلفي براي بررسي پراکندگي داده‌هاي ماتريس کليدهاي توليد شده انجام داده ايم. از جمله اين ارزيابي ها شامل ۱- تست Similarity ۲- تست Monobit۳- تست Poker۴- تست Run۵- بررسي هيستوگرام ماتريس کليد ۶- بررسي همبستگي خودکار مقادير کليد تصادفي ۷- چگالي طيف توان مقادير کليد تصادفي مي باشند. انجام اينارزيابيها به بررسی ميزان پراکندگي داده هاي کليد هاي توليد شده بر اساس اثر انگشت بسيار کمك مي کند. يکي از بلوك هايي که در ايجاد پراکندگي داده هاي کليد تصادفي کمك مي کند استفاده از بلوكS-box است که در اينجا ما از S-box مورد استفاده از رمز استاندارد AES استفاده کرده ايم. اين بلوك داراي مشخصات امنيتي قابل قبولي مي باشد که در مقاله [43] با مقايسه اي که بين S-box هاي مختلف انجام داده است S-box رمز AES داراي مشخصات بسيار خوبي مانند پارامتر غير خطی[1] ۱۱۲، يکنواختی ديفرانسيل[2]۴، معيار دقيق بهمنی[3] ۰,۵۰۵۸، درجه جبری[4]۷، احتمال تقريب ديفرانسيلی[5]۰,۰۱۵۶۲۵ و احتمال تقريب خطی[6]۰,۰۶۲۵ مي باشد. که اين پارامترها در بين S-box هاي مختلف بهترين مي باشند. استفاده از S-box می تواند باعث افزايش ويژگی غير خطی و پراکندگی داده شود که اين بلوک در بسياری از رمزهای قالبی استفاده می شود.

- **تست Similarity**

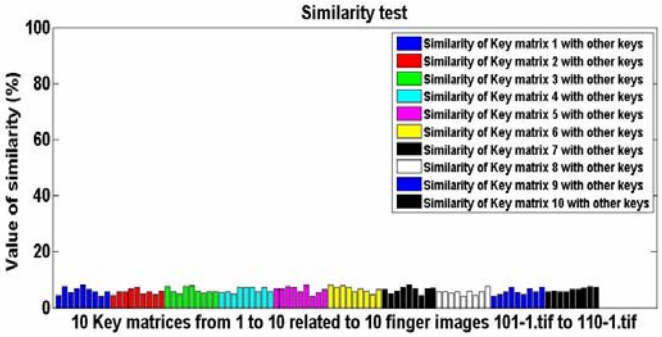
يکی از آنالیزهايي که می شود براي بررسي عدم شباهت کليد هاي توليد شده انجام داد آنالیز بررسی شباهت يا برابری ماتريس کليدهای مختلف می باشد.اين تحليل در خصوص پراکندگی نمونه های تصادفی توليد شده در فضای کليد برای افراد با اثر انگشت های متفاوت انجام شده است. در اين روش برای بررسی پراکندگی داده های کليد، ماتريس کليد های مختلف با هم مقايسه می شوند و ميزان شباهت بين آنها بدست می آيد. در اينجا ۲۰۰۰ بيت اول هر ماتريس کليد مربوط به هر اثر انگشت به صورت ۴ بيت به ۴ بيت با هم مقايسه می شوند. تعداد مقادير ۴ بيتی که برای دو ماتريس کليد با هم برابر هستند شمارش می شوند و اين تعداد بر تعداد کل مقادير ۴ بيتيتقسيم می شود. در اين آنالیز با بررسي ۴ بيت به ۴ بيت مقادير ماتريس کليدهای توليد شده ميزان عدم شباهت آنها نسبت به هم مورد بررسي قرار مي گيرد. بدين

[1]Nonlinearity
[2]Differential uniformity
[3]Strict avalanche criterion
[4]Algebraic degree
[5]Differential approximation probability
[6]Linear approximation probability

صورت ما میزان شباهت دو ماتریس کلید را مورد بررسی قرار می دهیم. همان طور که گفته شد ما از هر ماتریس کلید ۲۰۰۰ بیت اول آنها را با هم مقایسه می کنیم که این ۲۰۰۰ بیت به ۵۰۰ مقدار ۴ بیتی تقسیم می شود. در صد شباهت مقادیر دو ماتریس کلید نسبت به همدیگر به صورت زیر محاسبه می شود:

$$\text{درصد شباهت} = \frac{\text{تعداد مقادیر 4 بیتی برابر هر دو ماتریس}}{\text{تعداد کل مقادیر 4 بیتی}} \times 100$$

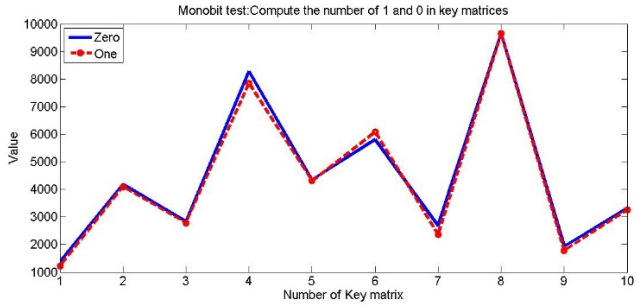
نتیجه مطلوب این است که میزان این پارامتر بسیار کمتر از ۵۰ درصد باشد.این تحلیل بین ۱۰ تصویر اثرانگشت1.tif_101 (تصویر اول)، 1.tif_102 (تصویر دوم)، ... و 1.tif_110 (تصویر دهم) از پایگاه داده اثر انگشت FVC2002 DB1_B انجام می شود به طوری که ابتدا مقادیر ماتریس کلید تصویر اول (به صورت ۴ بیتی) با مقادیر ماتریس کلیدهای دوم تا دهم مقایسه می شود و میزان شباهت آنها به صورت درصد بدست می آید. همین طور برای تصویر دوم میزان شباهت ماتریس کلید آن با ماتریس های کلید تصاویر اول، سوم، چهار تا دهم بدست می آید. این مقادیر به صورت نمودار ستونی در شکل ۱۱ نشان داده شده است. در این شکل به ترتیب از چپ به راست در صد شباهت ماتریس کلید تصویر اول با دیگر تصاویر تا در صد شباهت ماتریس کلید مربوط به تصویر دهم با دیگر تصاویر نشان داده شده است. همان طور که در این شکل دیده می شود در صد شباهت مقادیر ماتریس کلیدهای مختلف نسبت به یکدیگر کمتر از ۱۰% می باشد که درصد قابل قبولی می باشد. این امر میزان پراکندگی و عدم شباهت داده های تولید شده از هر اثر انگشت با اثر انگشت دیگر را نشان می دهد. بنابراین ماتریس های کلید تصادفی تولید شده به اندازه کافی دارای پراکندگی و تفاوت با یکدیگر می باشند.



شکل ۱۱:نمودار درصد شباهت ۲۰۰۰ بیت اول هر ماتریس کلید نسبت به دیگر ماتریس های کلید برای ۱۰ تصویر اثرانگشت1.tif_101 تا 1.tif_110 از پایگاه داده اثر انگشت FVC2002 DB1_B.

- **تست Monobit**

در این تست تعداد بیت های ۱ و ۰ در کل مقادیر ماتریس کلید محاسبه می شوند. اگر درصد تعداد بیت های ۱ و ۰ به هم نزدیک باشند، یعنی نزدیک ۵۰ درصد برای هرکدام باشد، نشان می دهد که توزیع بیت های ۱ و ۰ در کل ماتریس یکنواخت می باشد. این امر نشان دهنده تصادفی بودن مقادیر کلید می باشد. در اینجا ما تست را برای ماتریس های کلید تولید شده بر اساس ۱۰ تصویر اثر انگشت 1.tif_101 تا 1.tif_110 از پایگاه داده اثر انگشت FVC2002 DB1_B مورد بررسی قرار داده ایم. شکل ۱۲ مقادیر تعداد بیت های ۱ و ۰ در ماتریس کلید تولید شده از این ۱۰ تصویر اثر انگشت را نشان می دهد. محور افقی شماره تصویر می باشد که به ترتیب از ۱ تا ۱۰ می باشند و محور عمودی مقدار مربوط به تعداد بیت های ۱ و ۰ می باشد. نمودار آبی رنگ مربوط به تعداد بیت های ۰ است و نمودار قرمز خط چین شده مربوط به تعداد بیت های ۱ می باشد. همان طور که در این شکل دیده می شود نمودارهای مربوط به تعداد بیت های ۱ و ۰ در ماتریس های کلید تولید شده بر همدیگر منطبق بوده و نشان دهنده نزدیک بودن تعداد بیت های ۱ و ۰ در کلید می باشد. بنابراین،کلید تولید شده توسط روش پیشنهادی دارای ویژگی های تعادل تعداد بیتهای ۰ و ۱ و امنیت مناسبی است.



شکل ۱۲:نمودار مقادیر تعداد بیت های ۱ و ۰ در ماتریس کلید تولید شده از ۱۰ تصویر اثر انگشت1.tif_101 تا1.tif_110 از پایگاه داده .FVC2002 .DB1_B

برای بدست آوردن معیاری برای مقایسه با کارهای دیگر بر اساس کار [۳۸] نسبت تعداد یک های ماتریس کلید تقسیم بر تعداد کل بیت های کلید را به عنوان معیار Monobit در نظر گرفته می شود. در حالت ایده ال مقدار این معیار باید برابر ۰,۵ باشد که نشان دهنده برابر بودن تعداد صفر ها و یک های کلید و توزیع یکنواخت آنها می باشد. مقدار بدست آمده برای معیار Monobit در روش پیشنهادی تولید کلید برای ماتریس های کلید مربوط به تصاویر اثر انگشت 1.tif_101 تا 1.tif_110 از پایگاه داده FVC2002 DB1_B به ترتیب برابر اعداد 0.5292، 0.5059، 0.5056، 0.5131، 0.5022، 0.4886، 0.5309، 0.5007، 0.5196 و 0.5044 می باشند. میانگین این اعداد نیز برابر عدد 0.5100 است. بر اساس این اعداد بدست آمده که همه ی آنها بسیار به عدد 0.5 نزدیک می باشند می توان به این نتیجه رسید که پراکندگی داده های ماتریس های کلید مطلوب می باشد. در جدول ۳ نیز مقدار معیار Monobit برای مقایسه روش پیشنهادی و چند کار مرتبط

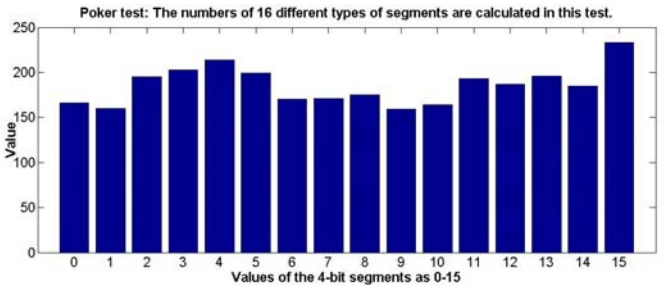
دیگر آورده شده است. همان طور که در این جدول مشاهد می شود نتیجه بدست آمده برای روش پیشنهادی در مقایسه با کارهای پیشین قابل قبول می باشد.

جدول ۳: مقایسه معیار Monobit برای کار پیشنهادی و کارهای مرتبط دیگر.

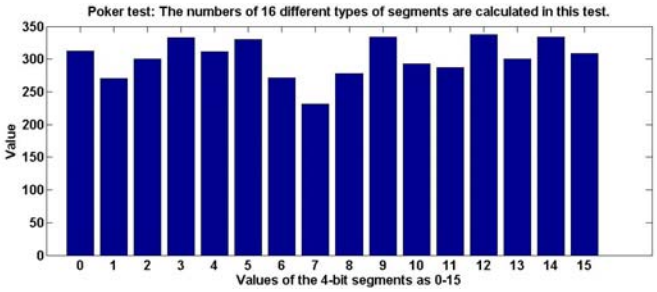
میانگین معیار Monobit	کار
0.5193	[۲۵]
0.4993	[۳۸]
0.1159	[36]
0.2888	[۱۹]
0.3767	[۱۹]
0.7236	[۱۹]
0.8596	[۱۹]
۰,۵۲۰۰	[37]
0.5100	کار پیشنهادی

- **تست Poker**

در این تست تمام مقادیر ۸-بیتی کلید تولید شده به دو قسمت ۴-بیتی تقسیم می شود. مثلا یک عدد ۸-بیتی از دو قسمت ۴-بیت کم ارزش و ۴-بیت پرارزش تشکیل می شود. بعد از اینکار آمار تعداد کل اعداد ۴-بیتی حساب می شود. همان طورکه می دانیم یک عدد ۴-بیتی می تواند بین ۰ تا ۱۵ باشد. لذا ما بعد از محاسبه کردن آمار تعداد اعداد ۴-بیتی در واقع آماری از تعداد اعداد ۰ تا ۱۵ از کل دنباله بدست می آوریم. حال اگر تعداد شمارش شده این اعداد در یک رنج باشد نشان دهنده توزیع یکنواخت داده ها در کل ماتریس تولید کلید می باشد. ما در این تست برای ۱۰ تصویر اثرانگشت 101_1.tif تا 110_1.tif از پایگاه داده اثر انگشت FVC2002 DB1_B این کار را انجام داده ایم و به نتایج قابل قبولی از این تست دست یافته ایم. با توجه به حجم زیاد داده ها در اینجا به عنوان مثال فقط دو نمونه از نتایج مربوط به تصویر اثر انگشت 106_1.tif و 108_1.tif که به ترتیب در شکل ۱۳ (a) و (b) نشان داده اند اورده شده است. محور افقی در این نمودارها نشان دهند اعداد ۰ تا ۱۵ (معادل اعداد ۴-بیتی) و محور عمودی مقدار شمارش هر عدد را نشان می دهد. همان طورکه دیده می شود اندازه ستون ها در سطح های نزدیک به هم هستند. در نتیجه تعداد شمارش شده اعداد ۰ تا ۱۵ در کل ماترس کلید تولید شده با درصد قابل قبولی به یکدیگر نزدیک می باشند.



(a)

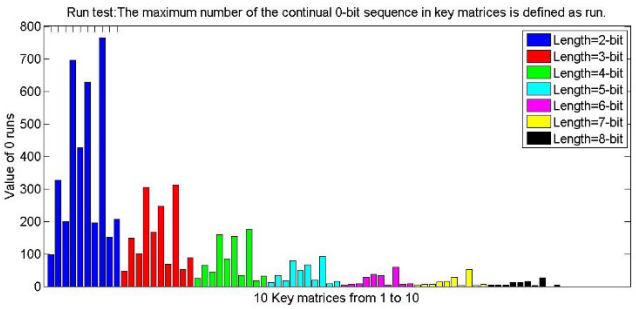


(b)

شکل ۱۳:نمونه نمودار مربوط به تست Poker برای ماتریس کلید تولید شده از تصویر اثرانگشت 101_1.tif (a) و 108_1.tif (b).

- **تست Run**

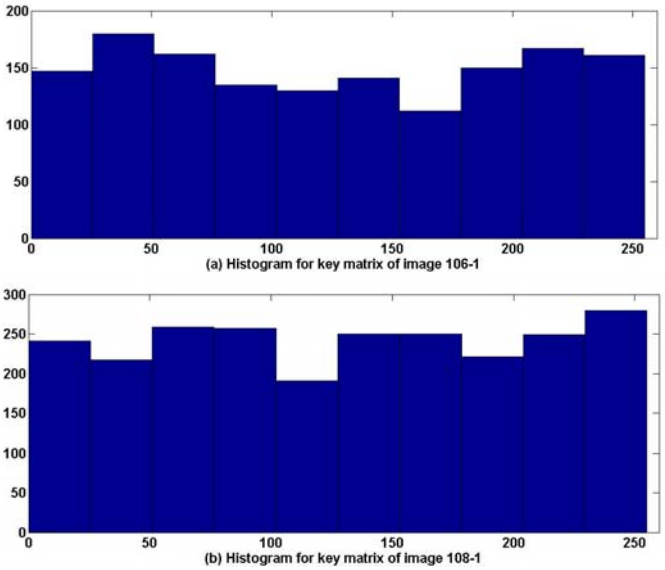
بیشترین تعداد بیت ۱ یا ۰ به هم پیوسته در دنباله اعداد کلید به عنوان run تعریف می شود [38]. اگر این تعداد بیت ۱ یا ۰ به هم پیوسته منجر به اعداد بسیار بزرگ شود نامطلوب می باشد. این امر نشان دهنده توزیع غیر یکنواخت بیت های ۱ یا ۰ در دنباله اعداد می باشد. در اینجا ما تعداد بیت های صفر به هم پیوسته با طول ۲ تا ۸ می پردازیم. نتایج برای تعداد بیت ۱ به هم پیوسته نیز مشابه بیت های ۰ بدست آمده است. شکل ۱۴ تعداد شمارش بیت های ۰ به هم پیوسته با طول ۲ تا ۸ را برای ۱۰ تصویر اثرانگشت 101_1.tif تا 110_1.tif از پایگاه داده اثر انگشت FVC2002 DB1_B نشان می دهد. هر دسته (رنگ) شامل ۱۰ ستون است که ستون ها از سمت چپ به راست به ترتیب مربوط به تصاویر 101_1.tif تا 110_1.tif می باشند. همان طورکه در این تصویر دیده می شود هر چقدر طول بیت های ۰ به هم پیوسته زیاد می شود اندازه ستون ها بسیار کاهش می یابد. با بررسی رفتار کاهشی تعداد بیت های ۰ به هم پیوسته با افزایش طول بیت ها از ۲ تا ۸ به این نتیجه می رسیم که این تعداد برای طول های بیش از ۱۰ بیت ۰ به هم پیوسته تقریبا به صفر می رسد. این امر نشان دهنده توزیع بسیار مناسب بیت های ۰ در ماتریس کلید می باشد. برای کار [۳۸] تعداد بیت های صفر یا یک به هم پیوسته برای تعداد ۲۵ تا به بالا برابر صفر می شود. بنابراین، در کار [۳۸] تعداد صفرها یا یک های به هم پیوسته نسبت به کلید های تولید شده در روش پیشنهادی بسیار بیشتر می باشد.



شکل ۱۴:نمودار تعداد شمارش بیت های ۰ به هم پیوسته با طول ۲ تا ۸ بیت برای ۱۰ تصویر اثرانگشت 1.tif_101 تا 1.tif_110 از پایگاه داده اثر انگشت FVC2002 DB1_B.

۴.۲.هیستوگرام مقادیر کلید تصادفی

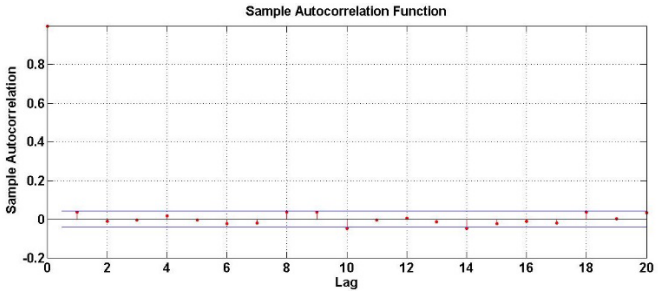
هیستوگرام مقادیرماتریس کلید تصادفی به ترتیب برای دو تصویر اثرانگشت ورودی1.tif_101 و 1.tif_108 در شکل های ۱۵ (a)و(b) نشان داده شده است. توزیع مقادیرکلید تصادفی در هیستوگرام نشان داده شده است. اگر نمودار به اندازه کافی مسطح نباشد، مقدار قابل توجهی از داده ها می تواند با حمله آماری تهدید شوند. در رمزنگاری، پاسخ مسطح و یکنواخت برای هیستوگرام بسیار مطلوب [44] است. تمام بایت های کلید تصادفی در محدوده ۰ تا ۲۵۵ با مقدار شمارش بسیار زیاد (تعداد وقوع اعداد تصادفی) رخ می دهد. مقدار شمارش برای اعداد تصادفی کلیدهای نزدیک به یکدیگر است. این امر نشان می دهد که هر مقداری در محدوده ۰ تا ۲۵۵ می تواند در تولید مقادیر کلید رخ دهد. بنابراین، هیستوگرام مقادیر تصادفی کلید توزیع یکنواختی دارد.



شکل ۱۵ : هیستوگرام مقادیرماتریس کلید تصادفی به ترتیب برایدوتصویر اثرانگشت ورودی(a)1.tif_101 و (b)1.tif_108.

۴.۳.همبستگی خودکار مقادیر کلید تصادفی

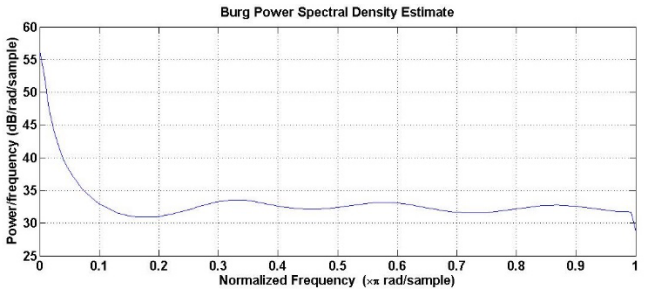
همبستگی خودکار، همبستگی سیگنال با خودش است. به عنوان مثال، همبستگی خودکار مقادیر کلید تصادفی برای تصویر 1.tif_108 در شکل۱۶ نشان داده شده است. مقادیر بسیار کمی دارد، همبستگی کمی بین مقادیر و میزان بالایی از تصادفی بودن را نشان می دهد. از آنجا که بیشترین مقدار در همبستگی خودکار برابر با ۰,۰۴۹۰ است، مقادیر کلید تصادفی هیچ شباهت قابل توجهی با خود ندارند، که این امر یک ضرورت اساسی برای قابلیت تصادفی بودن است.



شکل ۱۶ : همبستگی خودکار مقادیر کلید تصادفی پیشنهادی برای تصویر 1.tif_108.

۴.۴.چگالی طیفی توان مقادیر کلید تصادفی

چگالی طیفی توان مقادیر کلید تصادفی برای تصویر 1.tif_108 در شکل۱۷ نشان داده شده است. چگالی طیفی توان، توان تغییرات را به عنوان تابعی از فرکانس نشان می دهد. همانطور که از این شکل دیده می شود، چگالی طیفی توان مقادیر کلید تصادفی تقریباً مسطح هست مشابه مساوی سیگنال‌های تصادفی. بنابراین، این مسئله تصادفی بودن مقادیر کلید را تأیید می کند.



شکل ۱۷ : چگالی طیفی توان مقادیر کلید تصادفی پیشنهادی برای تصویر 1.tif_108.

۵. نتیجه گیری

در این مقاله از ویژگی های بیومتریک اثر انگشت برای تولید کلیدهای رمزنگاری تصادفی استفاده شده است. تولید کلیدهای تصادفی در رمزنگاریبا حجم زیادی از داده ها مانند رمزگذاری تصویر و صدا امری ضروری است. با استفاده از تولید کلید تصادفی می توان امنیت الگوریتم های رمزنگاری را بهبود بخشید. در روش پشنهادی ابتدا ویژگی های منحصر به فرد اثر انگشت که شامل نقاط مینوشیا می باشد از تصویر اثر انگشت استخراج می شوند. سپس برای افزایش ویژگی های آماری و پیچیدگی، فاصله اقلیدوسی تمام نقاط مینوشیا نسبت به یکدیگر حساب شده و در

یک ماتریس ذخیره می شوند. در مرحله بعد داده های این ماتریس بعد از نرمالیزه شدن به اعداد ۸-بیتی توسط عملیات جایگشت جابجا می شوند. سپس برای افزایش سطح امنیت و قابلیت تصادفی بودن بیشتر از عمل غیر خطی S-box ۸-بیتی استفاده شده در رمز قالبی AES استفاده شده است. بدین صورت که داده های ۸-بیتی هر یک جداکانه به S-box اعمال می شوند و نتیجه ذخیره می شود. استفاده از این ویژگی ها در تولید کلید تصادفی منجر به آشفتگی (confusion) و پخش (diffusion) می شود. آنالیزهای آماری که روی کلیدهای تولید شده صورت گرفته نشان دهنده ویژگی تصادفی بودن قابل قبول کلیدها می باشد

مراجع

[1] Sadhukhan, R., Patranabis, S., Ghoshal, A., Mukhopadhyay, D., Saraswat, V. and Ghosh, S., An Evaluation of Lightweight Block Ciphers for Resource-Constrained Applications: Area, Performance, and Security, Journal of Hardware and Systems Security, Vol. 1, Iss. 3, 2017, pp. 203-218.

[2] Hatzivasilis, G., Fysarakis, K., Papaefstathiou, I. and Manifavas, C., A review of lightweight block ciphers, Journal of Cryptographic Engineering, Vol. 11, Iss. 3, 2018, pp. 141-184.

[3] N.Noura, H., Chehab, A., Raphael, C. E□cient & secure cipher scheme with dynamic key-dependent mode of operation, Signal Processing: Image Communication, 2019, Vol. 78, pp. 448-464.

[4] Ismail Abdelfatah, R. Secure Image Transmission Using Chaotic-Enhanced Elliptic Curve Cryptography, IEEE Access, 2019, Vol. 8, pp. 3875-3890.

[5] Shanthakumari, R. and Malliga, S., Dual layer security of data using LSB inversion image steganography with elliptic curve cryptography encryption algorithm, Multimedia Tools and Applications, 2020, Vol. 79, pp. 3975-3991.

[6] Yang, C.H., Wu, H.C., and Su, S.F., Implementation of Encryption Algorithm and Wireless Image Transmission System on FPGA, IEEE Access, 2019, Vol. 7, pp. 50513-50523.

[7] You, L., Yang, E., and Wang, G., A novel parallel image encryption algorithm based on hybrid chaotic maps with OpenCL implementation, Soft Computing, Vol. 24, 2020, pp. 12413-12427.

[8] Farsana, F.J., Gopakumar, K., A Novel Approach for Speech Encryption: Zaslavsky Map as Pseudo Random Number Generator, Procedia Computer Science, 2016, Vol. 93, pp. 816-823.

[9] Wang, X., Su, Y., An Audio Encryption Algorithm Based on DNA Coding and Chaotic System, IEEE Access, 2020, Vol. 8, pp. 9260-9270.

[10] Sathiyamurthi, P. and Ramakrishnan, S., Speech encryption algorithm using FFT and 3D-Lorenz-logistic chaotic map, Multimedia Tools and Applications, 2020, Vol. 79, pp. 17817-17835.

[11] Sathiyamurthi, P. and Ramakrishnan, S., Speech encryption using chaotic shift keying for secured speech communication, EURASIP Journal on Audio, Speech, and Music Processing, 2017, Vol. 20, pp. 1-11.

[12] Rathgeb, C., and Uhl, A., Context-based biometric key generation for Iris, IET Computer Vision, 2011, Vol. 5, Iss. 6, pp. 389-397.

[13] Kanade, S., Petrovska-Delacretaz, D., and Dorizzi, B., Generating and Sharing Biometrics Based Session Keys for Secure Cryptographic Applications, in Proc. Fourth IEEE International Conference on Biometrics: Theory, Applications and Systems, 2010, Washington, DC, USA, pp. 1-7.

[14] Nguyen, D., Tran, D., Sharma, D., and Ma, W., On The Study of EEG-based Cryptographic Key Generation, in Proc. International Conference on Knowledge Based and Intelligent Information and Engineering Systems, 2017, Marseille, France, pp. 936-945.

[15] Carrara, C., and Adams, C., You are the Key: Generating Cryptographic Keys from Voice Biometrics, in Proc. Eighth Annual International Conference on Privacy, Security and Trust, 2010, Ottawa, ON, Canada, pp. 213-222.

[16] Camara, D.P.B.A., and Rocha, C.D., Providing Higher Entropy Cryptographic Keys by the Use of Biometrics, in Proc. The 7 th International Telecommunications Symposium, 2010, Manaus, Amazon, Brazil, pp. 1-5.

[17] Abduljaleel, I.Q., Abdul-Ghani, S.A., and Naji, H.Z., An Image of Encryption Algorithm Using Graph Theory and Speech Signal Key Generation, Journal of Physics: Conference Series, 2021, Vol. 1804, pp. 1-11.

[18] Majjed, I.A., and Majeed, A.M., Key Generation Based on Facial Biometrics, in Proc. the 1st International Multi-Disciplinary Conference Theme: Sustainable Development and Smart Planning, 2020, University of Bradford, UK, pp. 1-9.

[19] Yuliana, M., Wirawan, and, Suwadi, A Simple Secret Key Generation by Using a Combination of Pre-Processing Method with a Multilevel Quantization, Entropy, 2019, Vol. 21, pp. 1-25.

[20] Bano, A., Random Key Generator Using Human Voice, in Proc. International Multimedia, Signal Processing and Communication Technologies, 2013, Aligarh, India, pp. 41-45.

[21] Srinivas J., Mishra D., Mukhopadhyay S., Kumari S., Provably secure biometric based authentication and key agreement protocol for wireless sensor networks, J Ambient Intell Humaniz Comput, 2018, Vol. 9, No. 4, pp. 875-895.

mode of operation, Perspectives in Science, 2016, Vol. 8, pp. 57-60.

[34] Montero-Canela, R., Zambrano-Serrano, E., Tamariz-Flores, E.I., Munoz-Pacheco, J.M., and Torrealba-Melendez, R., Fractional chaos based-cryptosystem for generating encryption keys in Ad Hoc networks, Ad Hoc Networks, 2020, Vol. 97, pp. 1-21.

[35] Pich, R., Chivapreecha, S., Prabnasak, J., A New Key Generator for Data Encryption Using Chaos in Digital Filter, 8th Control and System Graduate Research Colloquium, in Proc. 8th Control and System Graduate Research Colloquium, 2017, Shah Alam, Malaysia, pp. 87-92.

[36] Ogras, H., Turk, M., A Secure Chaos-based Image Cryptosystem with an Improved Sine Key Generator, American Journal of Signal Processing, 2016, Vol. 6, No. 3, pp. 67-76.

[37] Tuncer, T., Avaroglu, E., Random Number Generation with LFSR Based Stream Cipher Algorithms, 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2017, Opatija, Croatia, pp. 171-175.

[38] Wang, J.J., Chen, J.Y., Yang, X.Y., Research on generating good key sequence based on chaos, Int. J. High Performance Computing and Networking, Vol. 9, Nos. 5/6, 2016, pp. 480-488.

[39] Daemen J, Rijmen VTDR. AES-The Advanced Encryption Standard. In: Information Security and Cryptography. New York: Springer;2002.

[40] Alilou, V.K.: Fingerprint matching: a simple approach. http://www.mathworks.com/matlabcentral/fileexchange/44369-fingerprint-matching--a-simple-approach (2016). Accessed 15 Mar 2016.

[41] The Fingerprint Verification Competition. The Biometric System Laboratory, University of Bologna, Bologna, Italy. Accessed: Jan. 2016. [Online]. Available: http://bias.csr.unibo.it/fvc2002/databases.asp.

[42] Barman, S., Samanta, D., Chattopadhyay, S., Approach to cryptographic key generation from fingerprint biometrics, Int. J. Biometrics, 2015, Vol. 7, No. 3, pp. 226-248.

[43] Rashidi, B., Compact and efficient structure of 8-bit S-box for lightweight cryptography, Integration, the VLSI Journal, 2021, Vol. 76, pp.۱۸۲-۱۷۲ .

[44] Nagakrishnan, R. and Revathi, A., A Robust Speech Encryption System Based on DNA Addition and Chaotic Maps, in Proc. 18 th International Conference on Intelligent Systems Design and Applications, Vellore, India, 2018, pp. 1070-1080.

[22] Pradeep, L.N., and Bhattacharjya, A., Random Key and Key Dependent S-box Generation for AES Cipher to Overcome Known Attacks, in Proc. International Symposium on Security in Computing and Communication, Springer, 2013, Mysore, India, pp. 63-69.

[23] Dwivedi, R., Dey, S., Sharma, M.A., Goel , A., A fingerprint based crypto_biometric system for secure communication, Journal of Ambient Intelligence and Humanized Computing, 2019, Vol. 11, pp. 1495-1509.

[24] Barman, S., Samanta, D., Chattopadhyay, S., Fingerprint-based crypto-biometric system for network security, EURASIP Journal on Information Security, 2015, Vol. 3, pp. 1-17.

[25] Panchal, G., Samanta, D., A Novel Approach to Fingerprint Biometric-Based Cryptographic Key Generation and its Applications to Storage Security, Computers and Electrical Engineering, 2018, Vol. 69, pp. 461-47.

[26] Barzut, S., Milosavljevic, M., Adamovic, S., Saracevic, M., Macek, N., Gnjatovic, M., A Novel Fingerprint Biometric Cryptosystem Based on Convolutional Neural Networks, Mathematics, 2021, Vol. 9, No. 7, pp. 1-12.

[27] Li, S., Zhang, X., Qian, Z., Feng, G., Ren, Y., Key based Artificial Fingerprint Generation for Privacy Protection, IEEE Transactions on Dependable and Secure Computing, 2020, Vol. 17, Iss. 4, pp. 828- 840.

[28] Suresh, K., Pal, R., Balasundaram, S.R., Fingerprint Based Cryptographic Key Generation, International Conference on Intelligent Data Communication Technologies and Internet of Things, 2020, India 38, pp. 704-713.

[29] Jo, J.G., Seo, J.W., Lee, H.W., Biometric Digital Signature Key Generation and Cryptography Communication Based on Fingerprint, FAW: International Workshop on Frontiers in Algorithmics, 2007, Lanzhou, China, pp 38-49.

[30] Wang, P., You, L., Hu, G., Hu, L., Jian, Z., Xing, C., Biometric Key Generation Based on Generated Intervals and Two-layer Error Correcting Technique, Pattern Recognition, 2020, Vol. 111, pp. 1-36.

[31] Sarkar, A., Singh, B.K., Cryptographic Key Generation From Cancelable Fingerprint Templates, Int'l Conf. on Recent Advances in Information Technology, 2018, Dhanbad, India, pp. 1-6.

[32] You, L., Zhang, G., Zhang, F., A Fingerprint and Threshold Scheme-Based Key Generation Method, International Conference on Computer Sciences and Convergence Information Technology, 2010, Seoul, Korea pp. 615- 619.

[33] Penchalaiah, P., and Ramesh Reddy, K., Random multiple key streams for encryption with added CBC

بهرام رشیدی مدرک کارشناسی مهندسی برق خود را در سال ۱۳۸۸ از دانشگاه لرستان دریافت کرد. مدرک کارشناسی ارشد و دکتری خود را به ترتیب در سال های ۱۳۹۰ و ۱۳۹۵ از دانشگاه تبریز و دانشگاه صنعتی اصفهان اخذ کرد است. در حال حاضر استادیار گروه مهندسی برق دانشگاه آیت الله بروجردی (ره) است. علایق تحقیقاتی او شامل پیاده سازی سخت افزار برای محاسبات میدان های محدود، پردازش تصویر، سخت افزار رمزنگاری، اینترنت اشیا(IoT) ، رمزهای بلوکی و مدارهای VLSIبرای سیستم های رمزنگاری منحنی بیضی است.