Computational Intelligence in Electrical Engineering
Vol. 14, No. 2, 2023
Research Paper

Generating biometric random cryptographic key based on unique fingerprint features

Bahram Rashidi[1], Ali Goudarzi[2]
[1] Assistant Professor, Dept. of Electrical Engineering, Ayatollah Boroujerdi University, Boroujerd, Iran
[2] Dept. of Electrical Engineering, Ayatollah Boroujerdi University, Boroujerd, Iran

Abstract:
This paper uses the unique biometric features of fingerprints to generate random cryptographic keys. The main aspects of the security of the generated key include the privacy of the fingerprint and the randomness and complexity of the key generation algorithm. In the proposed method, first, the unique fingerprint features, which include Minutiae points, are extracted from the fingerprint image. Then, to increase the statistical properties and complexity of the algorithm, the Euclidean distance and the angle of all the points of Minutiae relative to each other are calculated and stored. In the next step, after normalizing to 8-bit numbers, these data are moved by permutation operations and combined. In the following, the proposed method is used to increase the level of security and the ability to be random from the non-linear operations of 8-bit S-boxes S0 and S1 used in the CLEFIA block cipher. Statistical analyzes performed on the generated keys show the acceptable random nature of the keys. Therefore, the proposed structure for generating a random key can be used in encrypting digital signals with large volumes of data such as image and sound.

Keywords: Fingerprint, Random Encryption Key, Block cipher, Substitution box, Permutation.

https://doi.org/10.22108/isee.2022.131725.1528

مقاله پژوهشی

تولید کلید رمزنگاری تصادفی بیومتریک براساس ویژگی‌های منحصربه‌فرد اثر انگشت

بهرام رشیدی*[۱]، علی گودرزی[۲]

۱- استادیار، دانشکده فنی و مهندسی-گروه مهندسی برق- دانشگاه آیت الله بروجردی (ره)- بروجرد-ایران
b.rashidi@abru.ac.ir

۲- دانشجو کارشناسی، دانشکده فنی و مهندسی- دانشگاه آیت الله بروجردی (ره)- بروجرد-ایران
aligoodarzi550@gmail.com

چکیده: در این مقاله از ویژگی‌های منحصربه‌فرد بیومتریک اثر انگشت برای تولید کلیدهای رمزنگاری تصادفی استفاده شده است. جنبه‌های اصلی حاکم بر امنیت کلید تولیدشده شامل حریم خصوصی اثر انگشت و ویژگی تصادفی و پیچیدگی الگوریتم تولید کلید هستند. در روش پیشنهادی، ابتدا ویژگی‌های منحصربه‌فرد اثر انگشت شامل نقاط مینوشیا از تصویر اثر انگشت استخراج می‌شوند، سپس برای افزایش ویژگی‌های آماری و پیچیدگی الگوریتم، فاصله اقلیدوسی و زاویه تمام نقاط مینوشیا نسبت به یکدیگر، حساب و ذخیره می‌شوند. در مرحله بعد، این داده‌ها بعد از نرمالیزه‌شدن به اعداد ۸-بیتی با عملیات جایگشت، جابجا و در هم دیگر ترکیب می‌شوند. در ادامه، روش پیشنهادی برای افزایش سطح امنیت و قابلیت تصادفی‌بودن از عمل‌های غیر خطی S-boxهای ۸-بیتی S_0 و S_1 به کار برده شده در رمز قالبی CLEFIA استفاده شده است. آنالیزهای آماری صورت‌گرفته روی کلیدهای تولیدشده، نشان‌دهندهٔ پذیرفتنی‌بودن ویژگی تصادفی کلیدها است؛ بنابراین، ساختار پیشنهادی برای تولید کلید تصادفی می‌تواند در رمزنگاری سیگنال‌های دیجیتال با حجم زیادی از داده مانند تصویر و صدا استفاده شود.

واژه‌های کلیدی: اثر انگشت، کلید رمزنگاری تصادفی، سیستم رمزنگاری قالبی، جعبه جابجایی، جایگشت.

۱- مقدمه

سیستم‌های رمزنگاری یکی از مباحثی است که امروزه در برقراری امنیت سیستم‌های ارتباطی در هنگام انتقال یا ذخیره‌سازی اطلاعات نقش اساسی دارند. از فاکتورهای مهم و اساسی در سیستم رمزنگاری، تولید کلیدهای رمزنگاری است. محرمانه‌بودن این کلیدها و دسترسی‌نداشتن فرد غیر مجاز به کلید تصادفی از اصول مهم یک سیستم رمزنگاری است که باید مد نظر قرار بگیرد؛ اما تولید و ذخیره امن کلید برای سیستم کلید متقارن و کلید خصوصی برای سیستم کلید نامتقارن یک چالش مهم است. امنیت الگوریتم رمزنگاری براساس عملکرد آماری کلیدهای تصادفی است. تولید یک کلید تصادفی با کیفیت بالا کار دشواری است که سطح امنیت تأمین‌شده از الگوریتم رمزنگاری را افزایش می‌دهد. برای بهبود امنیت یک سیستم رمزنگاری، کلیدهای به‌کاررفته باید تصادفی و دارای طول مناسب باشند. بسیاری از تکنیک‌های رمزگذاری مانند رمزهای قالبی سبک [۱]-[۲] برای محافظت از داده‌ها در سیگنال‌های دیجیتال و کاهش هزینه‌های پیاده‌سازی ارائه شده‌اند. همچنین، موضوعات تحقیقاتی مانند رمزگذاری تصویر [۳]-[۷] و رمزگذاری صوت [۸]-[۱۱] به زمینه‌های مهم و ضروری تبدیل شده‌اند. تولید کلیدهای تصادفی در این سیستم‌ها یک عمل مهم است.

سه دسته اصلی برای تولید کلید تصادفی وجود دارد؛ شامل ۱- تولید کلید مبتنی بر تئوری آشوب: در این روش از معادلات ریاضی مانند نقشه Cat و نقشه Baker برای

---

[۱] تاریخ ارسال مقاله: ۱۴۰۰/۰۹/۱۲
تاریخ پذیرش مقاله: ۱۴۰۱/۰۱/۲۰
نام نویسندهٔ مسئول: بهرام رشیدی
نشانی نویسندهٔ مسئول: : ایران- بروجرد- دانشگاه آیت الله بروجردی (ره)- دانشکده فنی و مهندسی-گروه مهندسی برق

ایجاد آشفتگی[1] استفاده می‌شود. سیستم‌های آشوب ویژگی‌های مشابهی از حساسیت به شرایط اولیه و پارامترهای کنترل و رفتار شبه‌تصادفی را فراهم می‌کند که نیازهای آشفتگی و پخش[2] در رمزنگاری را برآورده می‌کند.

۲- تولید کلید رمزنگاری مبتنی بر بیومتریک: روشی است که از اطلاعات بیومتریک برای تولید کلیدهای رمزنگاری برای محافظت از امنیت داده‌ها استفاده می‌کند. سیستم‌های رمزنگاری بیومتریک یک زمینه تحقیقاتی در حوضه رمزنگاری است که در آن از بیومتریک یک فرد برای ایمن‌سازی تولید این کلیدهای رمزنگاری استفاده می‌شود.

۳- تولید کلید براساس مولدهای اعداد تصادفی: در این روش از مولد اعداد شبه‌تصادفی و شیفت رجیستر بازخوردی خطی (LFSR) برای تولید کلیدهای تصادفی استفاده می‌شود.

تکنیک‌های زیادی برای تولید کلید رمزنگاری [٦] و [۱۲]-[21] پیشنهاد شده‌اند؛ برای مثال، در [٦] یک سیستم آشوب ٤ بعدی براساس استفاده از سیگنال زمان گسسته برای تولید کلید ارائه شده است. در [۱۲] نویسندگان کلیدهای بیومتریک را از بردارهای ویژگی بیومتریک عنبیه تولید می‌کنند. در [۱۳] مکانیسم بازسازی کلید فازی برای استخراج یک الگوی محافظت‌شده استفاده شده است. سپس خطای تصحیح کد (ECC) برای تولید کلیدهای تصادفی استفاده می‌شود. در [14] نویسندگان براساس آزمایش‌های انجام‌شده از نمونه‌های سیگنال صوت برای تولید کلید بیومتریک تصادفی استفاده می‌کنند. در [15] سیستم تولید کلید از داده‌های بیومتریک عنبیه استفاده می‌کند. در [16] ساختار تولید کلید با عبور سیگنال صوتی در چندین مرحله براساس تئوری گراف تحقق می‌یابد. در [17] روشی برای تولید یک کلید رمزنگاری برای رمزگذاری داده‌ها با استفاده از خصوصیات چهره انسان ارائه شده است. نویسندگان از این کلید برای رمزگذاری پیام‌های صوتی و پنهان‌کردن آنها در داخل تصاویر رنگی استفاده کرده‌اند. در [18] تولید یک کلید ساده مخفی با استفاده از ترکیبی از روش پیش‌پردازش با کمی‌سازی چند سطح برای امنیت لایه فیزیکی ارائه شده است. در [19] روشی برای تولید کلیدهای تصادفی ۲٥٦ بیت براساس صدای انسان پیشنهاد شده است. در [20] کلیدهای امنی براساس توابع درهم تولید می‌شوند. در مقالات [۲۲]-[۲٦] ساختارهایی برای استخراج داده‌های الکتروانسفالوگرافی انسان (EEG) به‌عنوان ویژگی بیومتریک برای تولید کلید رمزنگاری پیشنهاد شده است. این ساختارها پتانسیل بالایی را فراهم می‌کنند؛ زیرا جعل و تقلب در EEG غیرممکن است. ویژگی‌های بیومتریک به‌طور کلی به ویژگی‌های فیزیولوژیکی (اثر انگشت، عنبیه، DNA) و ویژگی‌های رفتاری (راه رفتن، امضاء) تقسیم می‌شوند. سیگنال‌های EEG به دلیل وابستگی زیاد به رفتارها و احساسات، تلفیقی از ویژگی‌های فیزیولوژیکی و رفتاری شناخته می‌شوند. در کارهای [۲۲]، [۲۳]، [۲٤] و [۲٥] به‌ترتیب به مطالعه تأثیر بیماری صرع، احساسات، اختلالات مغزی و مصرف الکل بر تولید کلید رمزنگاری مبتنی بر EEG پرداخته‌اند. در این کارها از تکنیک تخمین طیف پارامتریک برای استخراج ویژگی‌های استفاده می‌شود و از یک تکنیک کوانتیزاسیون تصحیح خطا برای حف نویز استفاده می‌کنند. برای اینکه کلید تولیدشده از سیگنال EEG به‌کاررفتنی باشد، باید ویژگی‌های تکرارپذیر از سیگنال EEG استخراج شود تا کلید تکراری به‌طور دقیق تولید شود؛ بنابراین، لازم است به‌طور مکرر کلیدهای تصادفی کافی برای یک فرد تولید شود. سیگنال EEG و رابط‌های مغز و کامپیوتر با مسائل امنیتی مواجه‌اند [25]؛ برای مثال، ممکن است به دستگاهها حمله شود و اطلاعات خصوصی درگیر در سیگنال‌های EEG شخصی به بیرون درز کند.

چندین رویکرد تولید کلید رمزنگاری از ویژگی‌های بیومتریک اثر انگشت در کارهای [27]-[36] یافت می‌شود. در [28] رویکردی برای تولید کلید رمزنگاری از الگوی اثرانگشت قابل لغو[3] برای هر دو طرف ارتباط پیشنهاد شده است. در [29] ویژگی‌های آماری مبتنی بر بیومتریک اثر انگشت را برای تولید کلمه کد[4] یک کاربر استخراج می‌کنند. برای تولید یک کلمه کد، از کدینگ Reed-Solomon (RS) استفاده می‌شود. سپس از این کلمه کد برای تولید یک کلید استفاده می‌شود. در [35] یک روش تولید کلید براساس اثر انگشت با استفاده از فواصل نسبی بین جزئیات اثر انگشت کاربر برای ایجاد یک کلید بیومتریک منحصربه‌فرد 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 [36] یک روش برای تولید کلید رمزنگاری براساس ویژگی‌های اثر انگشت و الگوریتم آستانه[۵] پیشنهاد می‌شود.

سیستم‌های رمزنگاری مانند رمزگذاری سیگنال تصویر و رمزگذاری سیگنال صوت برای انتقال اطلاعات به یک واحد تولید کننده کلید تصادفی نیاز دارند [37] و [38]. با استفاده از تولید کلید تصادفی، امنیت الگوریتم‌های رمزنگاری بهبود می‌یابد. این مقاله یک الگوریتم تولید کلید تصادفی براساس ویژگی‌های منحصربه‌فرد اثر انگشت پیشنهاد می‌کند. حریم خصوصی کلید بیومتریک تولیدشده به‌صورت تصادفی و پیچیدگی الگوریتم تولید کلید، جنبه‌های اصلی حاکم بر امنیت کلید است. با توجه به اینکه پارامترهای بیومتریک برای هر فرد با فرد دیگر متفاوت است و هیچگاه این پارامترها از بین نمی‌روند، یک روش مناسب برای افزایش امنیت سیستم است. این ساختار می‌تواند کلیدهایی با طول‌های مختلف ایجاد کند. طول کلیدهای تولیدشده برابر با ۱۲۸، ۱۹۲ و ۲۵۶ بیت است. آنالیزهای آماری صورت‌گرفته روی کلیدهای تولیدشده نشان‌دهندهٔ ویژگی تصادفی‌بودن پذیرفتنی کلیدها است. مهم‌ترین ویژگی‌های روش پیشنهادی در زیر آورده شده‌اند:

- در الگوریتم پیشنهادی، برای تولید کلید تصادفی براساس ویژگی‌های منحصربه‌فرد اثر انگشت از بلوک‌های سازنده‌ای ازقبیل واحد محاسبه فاصله اقلیدوسی و زاویه بین نقاط مینوشیا استفاده شده است.
- برای افزایش ویژگی‌های آماری و پیچیدگی الگوریتم، فاصله اقلیدوسی و زاویه تمام نقاط مینوشیا نسبت به یکدیگر، حساب و در دو ماتریس ذخیره می‌شود. داده‌های این ماتریس‌ها بعد از نرمالیزه‌شدن به اعداد ۸-بیتی با عملیات جایگشت جداگانه جابجا می‌شوند. سپس نتیجه جایگشت‌یافتهٔ این دو ماتریس با یک عمل جایگشت دیگر در هم دیگر ترکیب می‌شوند و یک ماتریس واحد ایجاد می‌کنند.
- برای افزایش سطح امنیت و قابلیت تصادفی‌بودن از عمل‌های غیر خطی S-boxهای ۸-بیتی S_0 و S_1 به‌کاررفته در رمز قالبی CLEFIA [39] استفاده شده است؛ بدین صورت که داده‌های ۸-بیتی هر یک جداگانه به S-box اعمال می‌شوند (داده‌هایی با موقعیت زوج و فرد به‌ترتیب به S-boxهای ۸-بیتی S_0 و S_1، اعمال می‌شوند) و نتیجه ذخیره می‌شود.

در ادامهٔ مقاله در بخش دوم به‌طور خلاصه روند استخراج ویژگی‌های اثر انگشت توضیح داده شده است. روش تولید کلید تصادفی پیشنهادی در بخش سوم ارائه شده است. در بخش چهارم نتایج و بحث دربارهٔ روش پیشنهادی نشان داده شده است. سرانجام، مقاله در بخش پنجم جمع‌بندی می‌شود.

۲- استخراج ویژگی‌های اثر انگشت

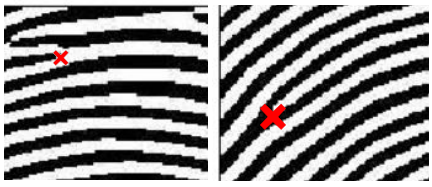
اثر انگشت یکی از پرکاربردترین روش‌های شناسایی بیومتریک است که بیش از یک قرن استفاده شده است. اثر انگشت هر انسان منحصربه‌فرد است و در طول زندگی فرد بدون تغییر باقی می‌ماند. اثر انگشت از الگوی برآمدگی‌های روی انگشت شکل می‌گیرد. برای هر اثر انگشت ویژگی‌های منحصربه‌فردی وجود دارد که در ادامه به مواردی از آنها اشاره می‌شود: ۱- هر اثر انگشت منحصربه‌فرد است؛ یعنی هیچ دو انگشتی دارای ویژگی‌های 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 ازنظر ساختاری در طول زندگی فرد بدون تغییر باقی می‌ماند. ٤- یکی از دقیق‌ترین اشکال بیومتریک موجود است. ۵- به دست آوردن اثر انگشت راحت است و ازاین‌رو، گزینه خوبی برای سیستم‌های امنیتی است.

روی هر اثر انگشت دو بخش رگه و شیار وجود دارد. شکل ۱ رگه‌ها و شیارهای موجود روی تصویر اثر انگشت را نشان می‌دهد. پیکسل‌های سفید نشان‌دهندهٔ برجستگی‌ها هستند و پیکسل‌های سیاه مربوط به شیارها هستند. به رگه‌هایی که به‌صورت موازی در اثر انگشت وجود دارند که در مواردی خاتمه می‌یابند و گاهی اوقات دو شاخه می‌شوند، مینوشیا گفته می‌شود. شکل ۲ نمونه‌ای از نقاط مهم مینوشیا را در یک اثر انگشت نشان می‌دهد. اگر رگه‌ای

به رگهٔ دیگر متصل نباشد و در امتداد همدیگر باشد، امتداد این رگه‌ها به‌عنوان مینوشیا انتهایی در نظر گرفته می‌شود. اگر هر رگه به دو رگه دیگر تبدیل شود، قسمتی که دو شاخه می‌شود را مینوشیا دو شاخه‌ای در نظر می‌گیرند.

از بین انواع مینوشیا دو نوع مینوشیای انتهایی و مینوشیای دوشاخه‌ای بیشتر کاربرد دارد. در مرحله استخراج ویژگی‌های اثر انگشت مختصات این نقاط به دست می‌آید. در این مقاله از روش ارائه‌شده در کار [40] برای بهبود تصویر و استخراج مینوشیاها استفاده می‌شود. در این کار از عملیات موروفولوژیک روی تصویر اثر انگشت استفاده می‌کند که به نازک‌شدن رگه‌های موجود در اثر انگشت منجر می‌شود. قبل از استخراج مینوشیاها نیاز است بر حسب نیاز بهبودها و پیش‌پردازش‌هایی روی تصویر اثر انگشت صورت پذیرد. در ادامه به‌طور خلاصه این پیش‌پردازش‌ها توضیح داده شده‌اند.

شکل (۱): خطوط سیاه‌رنگ «رگه» و خطوط سفید رنگ «شیار».



(b) (a)

شکل (۲): تصویر (a) مینوشیا انتهایی و تصویر (b) مینوشیا دو شاخه‌ای.

۲-۱- مرحله پیش‌پردازش

در این بخش، مراحل پیش‌پردازش لازم برای استخراج نقاط مینوشیا و نحوه استخراج آنها براساس کار [40] معرفی می‌شود. مراحل پیش‌پردازش صورت‌گرفته در این کار شامل ۱- بهبود تصویر (شامل متعادل‌سازی هیستوگرام و تبدیل فوریه است)؛ ۲- باینری‌کردن تصویر و ۳- نازک‌سازی. مرحله پیش‌پردازش برای بهبود تصویر و برجسته‌کردن ویژگی بیومتریک اثر انگشت انجام می‌شود. به عبارت دیگر، بهبود تصویر اثر انگشت برای حذف نویز ناشی از حسگر و تغییرات ناشی از فشار انگشت روی سنسور صورت می‌پذیرد. ویژگی‌های بیومتریک اثر انگشت باید تقویت شوند تا بتوان از آنها برای تجزیه‌وتحلیل بیشتر استفاده کرد. این فرآیند با حذف پیکسل‌های اضافی از تصویر و رسیدن به روشنایی و کنتراست بهتر انجام می‌شود. چند مرحله مهم پیش‌پردازش روی تصویر اثر انگشت مانند افزایش کنتراست، باینریزه‌کردن[6] و نازک‌سازی[7] انجام می‌شود. افزایش کنتراست، کیفیت اثر انگشت را با کاهش اثرات نامطلوب تاری، منافذ و برجستگی‌های اولیه بهبود می‌بخشد. این امر به بهبود تشخیص نقاط مینوشیا کمک می‌کند. در بین روش‌هایی که تا کنون برای افزایش کیفیت اثر انگشت ارائه شده است، سه روش وجود دارد که اساس کار در روش‌های دیگرند. این سه روش عبارت‌اند از: یکنواخت‌سازی هیستوگرام (این روش ساده‌ترین روش افزایش کیفیت اثر انگشت است؛ اما برای تصاویری با کیفیت کم کارآیی خود را از دست می‌دهد)، تبدیل فوریه سریع و فیلتر گابور.

در کار [40] برای افزایش کیفیت تصویر از روش تبدیل فوریه و متعادل‌سازی هیستوگرام استفاده می‌شود. شکل ۳ (a) و (b) به‌ترتیب تصویر یک اثر انگشت (این تصویر از پایگاه داده [41] استفاده شده است.) و تصویر بهبود داده شده با روش تبدیل فوریه را نشان می‌دهد. همان‌طور که در تصویر دیده می‌شود اعمال تبدیل فوریه باعث شده است تا نقاط شکسته در رگه‌ها به هم متصل شوند و اتصالات اشتباه بین رگه‌ها از بین بروند.

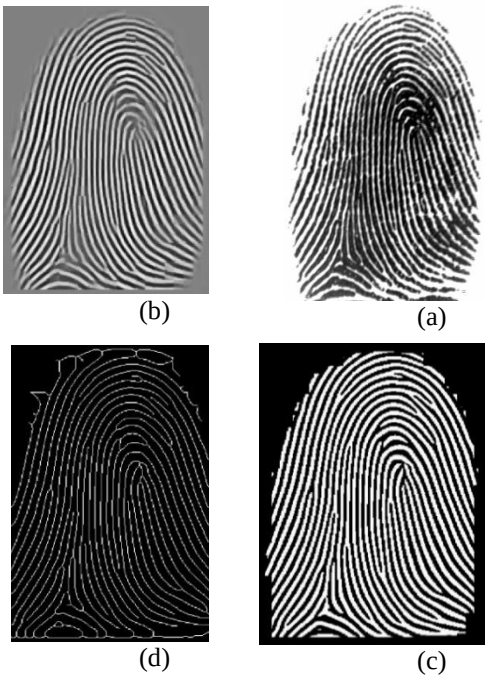
- باینریزه‌کردن تصویر

هدف از این مرحله، به دست آوردن یک تصویر باینری است. می‌توان یک مقدار آستانه را انتخاب کرد و تمام پیکسل‌های بالای آن مقدار را سفید و زیر آن مقدار را سیاه کرد. این فرآیند یکی از ساده‌ترین فرآیندها برای باینریزه‌کردن است. این عمل تصویر اثر انگشت خاکستری

را به یک تصویر باینری حاوی برجستگی‌ها و فرورفتگی‌ها تبدیل می‌کند. شکل ۳ (c) تصویر باینریزه‌شدهٔ اثر انگشت را نشان می‌دهد.

- نازک‌سازی

در فرایند نازک‌سازی تمام خطوط موجود در تصویر باینریزه‌شده به ضخامت یک پیکسل متراکم می‌شوند. نازک‌شدن عرض خطوط برآمدگی باینری‌شده را به ۱ پیکسل کاهش می‌دهد. فرآیندهای باینریزه‌کردن و نازک‌سازی برای مکان‌یابی نقاط مینوشیا مورد نیاز هستند. نازک‌سازی تصویر اثر انگشت روی تصویر باینری اثر انگشت انجام می‌گیرد. برای اینکه تشخیص و حذف پیکسل‌های اضافه راحت‌تر انجام شود، این الگوریتم باید در حالت تکرار، طبق سه شرط (۱- نقاط پایانی حذف نشوند؛ ۲- اتصالات از بین نروند و ۳- باعث سایش بیش از حد نشود) انجام گیرد. شکل ۳ (d) تصویر نازک‌سازی‌شدهٔ اثر انگشت را نشان می‌دهد.



شکل (۳): (a): تصویر اصلی، (b): تصویر بعد از تبدیل فوریه و متعادل سازی هیستوگرام، (c): تصویر بعد از باینری‌سازی و (d): تصویر بعد از نازک‌سازی.

یکی از روش‌های موجود برای پیداکردن مینوشیاهای مورد نیاز روش شماره عبور[۸] است که در مقالات مختلفی ازجمله کار [40] از آن استفاده شده است. در ادامه، دربارهٔ روش پیداکردن نقاط مینوشیا با روش شماره عبور توضیح مختصری داده شده است. این روش در مقایسه با روش‌های دیگر دارای کارایی محاسباتی و سادگی است. با اسکن‌کردن مناطق محلی هر پیکسل در تصویر نازک‌سازی‌شده با استفاده از پنجره ۳ در ۳ نقاط مینوشیا استخراج می‌شوند. مقدار CN به‌صورت زیر محاسبه می‌شود:

$$CN = \frac{\sum_{i=1}^{8} |p_i + p_{i+1}|}{2}$$

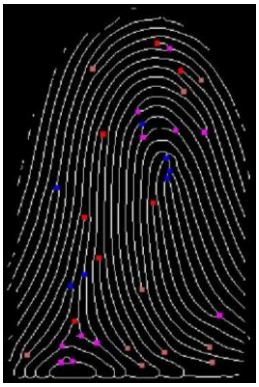
که در آن p_i برابر مقدار پیکسل است و $p_1=p_9$ است. CN به‌عنوان نصف مجموع تفاوت‌های بین جفت پیکسل‌های همسایه در هشت پیکسل همسایه تعریف می‌شود. با استفاده از ویژگی‌های CN در جدول ۱، پیکسل p به‌عنوان مینوشیا انتهایی، دو شاخه‌ای یا نبود مینوشیا است.

جدول (۱): ویژگی‌های CN.

ویژگی	CN
نقطه تکی	۰
مینوشا انتهایی	۱
رگه ادامه‌دار	۲
مینوشا دوشاخه‌ای	۳
مینوشا نیست	٤

این امکان وجود دارد که به دلیل عواملی مانند تصاویر نویزی و مصنوعات تصویری مینوشیاهای غیر قابل قبول وارد تصویر شوند؛ ازاین‌رو، پس از استخراج نقاط، لازم است یک مرحله پس‌پردازش را به‌منظور تأیید نقاط مینوشیا به کار برد. در این مرحله، تمام نقاط مینوشیا نادرست مانند (نقاط مینوشیای جانبی، نقاط شناسایی‌شده در مناطق با کیفیت پایین، جزایر، دریاچه‌ها و غیره) حذف می‌شوند.

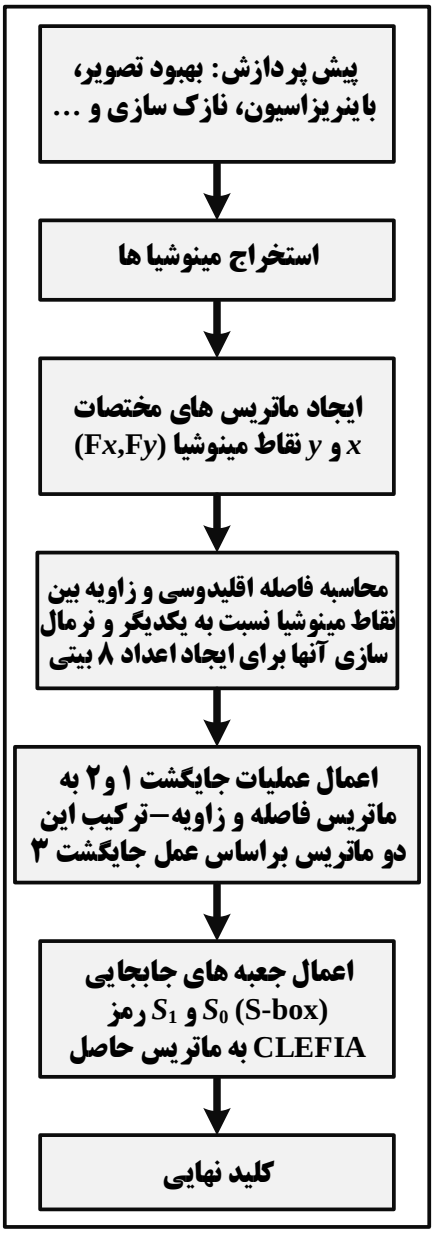
نقاط مینوشیا در شکل ٤ برای تصویر اثر انگشت ارائه‌شده در شکل ۳ (a) نشان داده شده‌اند. بیشترین نقاط مینوشیا، انتهایی و دوشاخه‌ای هستند. همان‌طور که دیده می‌شود این نقاط انتهایی و دو شاخه‌ای در شکل شناسایی شده‌اند.



شکل (٤): تصویر نقاط مینوشیا تشخیص داده شده از تصویر اثر انگشت شکل ۳ (a).

۳- روش پیشنهادی تولید کلید رمزنگاری بیومتریک از اثر انگشت

در این مقاله، هدف تولید کلید رمزنگاری از ویژگی‌های منحصربه‌فرد استخراج‌شده از اثر انگشت است. در این رویکرد، اثر انگشت به‌عنوان یک پارامتر بیومتریک برای تولید کلید رمزنگاری استفاده می‌شود. در این روش از مختصات نقاط مینوشیا برای تولید کلید استفاده می‌شود. نمای کلی از مراحل روش پیشنهادی به‌صورت شماتیک در شکل ۵ نشان داده شده است. بعد از استخراج نقاط مینوشیا مختصات این نقاط به دست می‌آیند. مؤلفه x و y نقاط به‌ترتیب در ماتریس‌های F_x, F_y ذخیره می‌شوند. در مرحله بعد به محاسبه فاصله اقلیدوسی و زاویه بین نقاط مینوشیا نسبت به یکدیگر و نرمال‌سازی مقادیر فاصله و زاویه برای ایجاد اعداد ۸ بیتی پرداخته می‌شود. سپس نتایج در دو ماتریس جداگانه ذخیره می‌شوند. بعد از این مرحله به هر ماتریس عمل جایگشتی اعمال می‌شود. دو ماتریس حاصل با یک جایگشت دیگر در یکدیگر ترکیب می‌شوند و یک ماترس واحد را می‌سازند. در مرحله بعد برای افزایش تصادفی‌شدن اعداد، هر مقدار ۸-بیتی در ماتریس به جعبه‌های جابجای S-box ۸-بیتی S_0 و S_1 استفاده‌شده در رمز قالبی CLEFIA [39] اعمال می‌شود؛ بدین صورت که داده‌های ۸-بیتی هر یک جداگانه به S-box اعمال می‌شوند (داده‌هایی با موقعیت زوج و فرد به‌ترتیب به S-boxهای ۸-بیتی S_0 و S_1، اعمال می‌شوند) و نتیجه ذخیره می‌شود. در مرحله بعد، بایت‌های کلیدها از مقادیر ماتریس به‌دست‌آمده در مرحله قبل به دست می‌آیند. در روش پیشنهادی با انجام مراحل محاسبه، فاصله اقلیدوسی و زاویه بین نقاط مینوشیا، عمل‌های جایگشت و عمل S-box میزان تصادفی‌بودن کلید بسیار افزایش می‌یابد.



شکل (۵): نمای کلی از مراحل روش پیشنهادی تولید کلید براساس اثر انگشت.

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

منظور از بهینه‌سازی مصرف انرژی انتخاب الگوها،

اتخاذ و به‌کارگیری روش‌ها و سیاست‌هایی در مصرف انرژی الکتریکی است. ساختمان‌های مسکونی بخش مهمی از مصرف‌کنندگان انرژی الکتریکی به شمار می‌آیند. ورود تکنولوژی سیستم مدیریت هوشمند به ساختمان‌های مسکونی، تا حدودی مصرف انرژی الکتریکی را بهینه کرده است.

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

Input: Input *x*-coordinate F_x and *y*-coordinate F_y matrices of the Minutiae.
Output: 128-bit Random Key K_j, $0 \le j \le 2m/16$.

1. f=2; $m = (D * (D-1))/2$; n=1;
2. For i from 1 to $D-1$ do // Step 1.
3. For j from f to D do
4. $D_p(n) = \sqrt{(F_x(i) - F_x(j))^2 + (F_y(i) - F_y(j))^2}$
5. $T_p(n) = \left|tan^{-1}\frac{F_y(i)-F_y(j)}{F_x(i)-F_x(j)}\right|$
6. $n = n + 1$;
7. End For;
8. $f = f + 1$;
9. End For;
10. For i from 1 to m do // Step 2.
11. $D_{p1}(i) = D_p(i)\ mod\ 2^8$;
12. $T_{p1}(i) = T_p(i)\ mod\ 2^8$;
13. End For;
14. $D_{p2} = Permutation1(D_{p1})$; // Step 3.
15. $T_{p2} = Permutation2(T_{p1})$;
16. $K = Permutation3(D_{p2}, T_{p2})$;
17. For i from 1 to $2m$ do // Step 4.
18. If (i is odd) then
19. $Key(i) = S_0(K(i))$;
20. Else
21. $Key(i) = S_1(K(i))$;
22. End If;
23. End For;
24. For j from 1 to $2m/16$ do // For 128-bit keys.
25. $Ke_j = Key(i+16)||Key(i+15)||Key(i+14)||\dots||Key(i+2)||Key(i+1)$;
26. $i = i + 16$;
27. End For;

۳-۱- ماتریس‌های مختصات نقاط مینوشیا و محاسبه فاصله اقلیدوسی و زاویه‌ها

هر نقطه مینوشیا به صورت مختصات x و y نشان داده می‌شود. مختصات x و y این نقاط برای محاسبات بعدی مورد استفاده قرار می‌گیرد. 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 با عبارت زیر نمایش داده می شود:

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

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

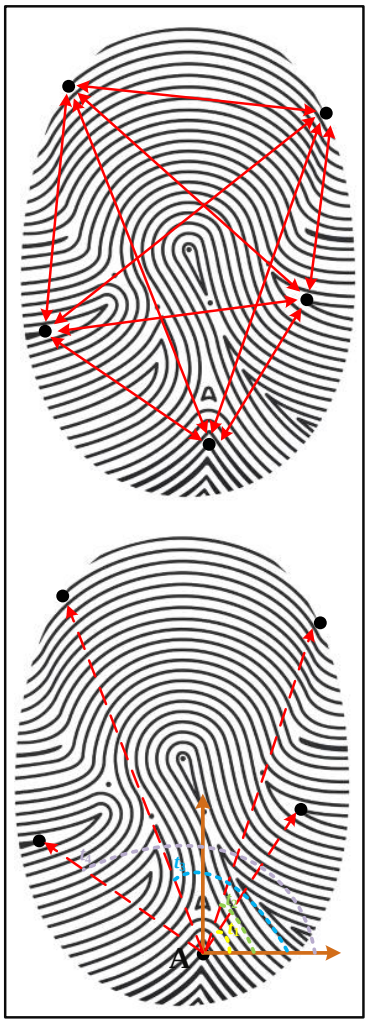
$$F_x = [x_1, x_2, x_3, \dots, x_m]$$
$$F_y = [y_1, y_2, y_3, \dots, y_m]$$

حال فاصله اقلیدوسی و زاویه بین تک‌تک نقاط مینوشیا، حساب و در دو ماتریس ذخیره می‌شوند. فاصله اقلیدوسی و زاویه دو نقطه فرضی براساس بردارهای F_x, F_y در زیر نشان داده شده‌اند:

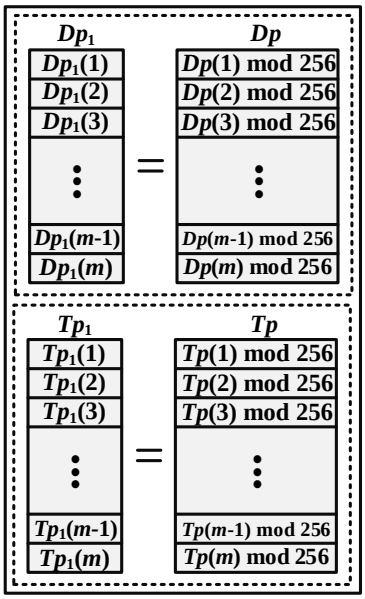
$$D_p(n) = \sqrt{(F_x(i) - F_x(j))^2 + (F_y(i) - F_y(j))^2}$$
$$T_p(n) = \left|tan^{-1}\frac{F_y(i) - F_y(j)}{F_x(i) - F_x(j)}\right|$$

تعداد فاصله‌های اقلیدوسی و زاویه بین D نقطه مینوشیا نسبت به هم برابر $\binom{D}{2} = \frac{D(D-1)}{2}$ است. شکل ٦ فاصله اقلیدوسی (شکل بالا) و زاویه (شکل پایین) بین چند نقطه مینوشیای فرضی در یک تصویر سمبولیک اثر انگشت را نشان می‌دهد؛ البته در شکل پایین به دلیل شلوغ‌شدن تصویر زوایای دیگر نقاط نسبت به هم نشان داده نشده است. در بسیاری از تصاویر اثر انگشت تعداد نقاط مینوشیا محدود است و این امر ممکن است میزان تصادفی‌بودن و نتایج تحلیل‌های آماری داده‌های کلید را دچار ضعف کند. استفاده از فاصله اقلیدوسی و زاویه بین تمام نقاط نسبت به یکدیگر علاوه بر حفظ ویژگی منحصربه‌فرد بودن پارامترهای اثر انگشت باعث افزایش تعداد داده‌های استخراجی از اثر انگشت برای تولید کلید می‌شود. این امر میزان تصادفی‌بودن نتایج آماری داده‌های ماتریس کلید و الگوی بیتی آن را بهبود می‌دهد؛ برای مثال، اگر یک اثر انگشت ۸۰ نقطه مینوشیا داشته باشد، تعداد داده‌های مربوط به فاصله اقلیدوسی و زاویه تمام نقاط نسبت به یکدیگر به‌طور

جداگانه برابر ۳۱٦۰ است. روی هم تعداد داده‌های فاصله اقلیدوسی و زاویه برابر ٦۳۲۰ است که این عدد نسبت به تعداد داده خام مختصات نقاط مینوشیا بسیار بزرگ‌تر است. برای نمایش هر داده در ماتریس فاصله اقلیدوسی Dp و ماتریس زاویه Tp در قالب یک عدد ۸-بیتی باقیمانده هر داده نسبت به عدد 2^8 به دست آورده می‌شود. این کار در شکل ۷ نشان داده شده است. مقادیر ۸-بیتی ماتریس فاصله اقلیدوسی Dp در ماتریس جدید Dp_1 و برای ماتریس زاویه Tp در ماتریس جدید Tp_1 ذخیره می‌شوند.



شکل (٦): فاصله اقلیدوسی و زاویه بین چند نقطه مینوشیای فرضی در یک تصویر اثر انگشت سمبولیک.



شکل (۷): روند ۸-بیتی کردن اعداد بدست آمده برای ماتریس‌های فاصله اقلیدوسی و زاویه.

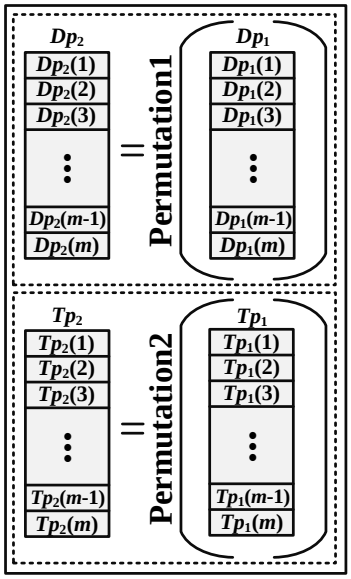
۳-۲- اعمال جایگشت‌ها

در این مرحله، به‌ترتیب جایگشت‌های $Pr1$ و $Pr2$ برای مقادیر نرمال‌شدهٔ فاصله اقلیدوسی (ماتریس Dp_1) و زاویه (ماتریس Tp_1) در مرحله قبل اعمال می‌شود. عملیات جایگشت به شرح زیرند:

$$Pr1(i) = \begin{cases} (i+9) \times \frac{i}{7} \bmod m - 1 & if\ i \in \{1,2,\dots,m-1\} \\ m & if\ i = m. \end{cases}$$

$$Pr2(i) = \begin{cases} (i+7) \times \frac{i}{11} \bmod m - 1 & if\ i \in \{1,2,\dots,m-1\} \\ m & if\ i = m. \end{cases}$$

مقدار m برابر با تعداد داده‌های ماتریس Dp_1 است؛ برای مثال، عمل جایگشت برای ماتریس Dp_2 نمونه i از ماتریس Dp_1 را به موقعیت $Pr1(i)$ ماتریس Dp_2 انتقال می‌دهد. شکل ۸ مرحله اعمال جایگشت‌های $Pr1$ و $Pr2$ را در روش تولید کلید تصادفی پیشنهادی نشان می‌دهد. با توجه به شکل، مقادیر ماتریس‌های Dp_1 و Tp_1 براساس جایگشت‌های $Pr1$ و $Pr2$ به‌ترتیب برای تولید ماتریس‌های Dp_2 و Tp_2 استفاده می‌شوند.

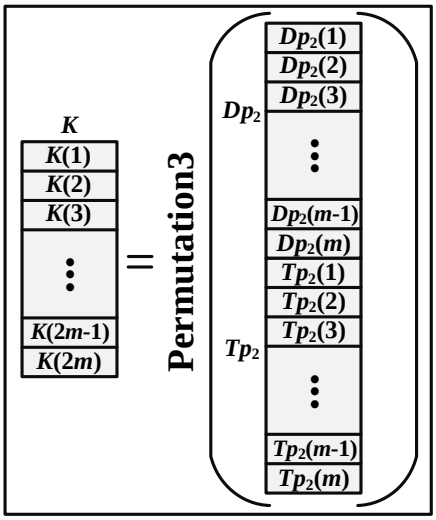


شکل (۸): مرحله اعمال جایگشت‌های Pr1 و Pr2 در روش تولید کلید تصادفی پیشنهادی.

در مرحله بعد، دو ماتریس Dp_2 و Tp_2 با m عضو براساس یک عمل جایگشت دیگر $Pr3$ با همدیگر ترکیب می‌شوند و یک ماترس K با $2m$ عضو را ایجاد می‌کنند. این عمل جایگشت در زیر نشان داده شده است:

$$Pr3(i) = \begin{cases} (i+5) \times \frac{i}{9} \ mod\ 2m-1 & if\ i \in \{1,2,\dots,2m-1\} \\ 2m & if\ i = 2m. \end{cases}$$

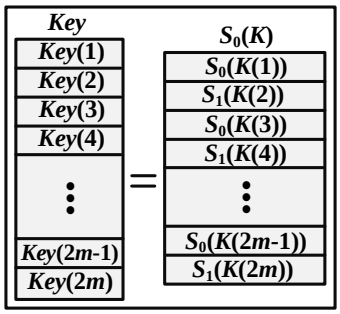
شکل ۹ مرحله اعمال جایگشت $Pr3$ به مقادیر ماتریس‌های Dp_2 و Tp_2 را نشان می‌دهد.



شکل (۹): مرحله اعمال جایگشت Pr3 در روش تولید کلید تصادفی پیشنهادی.

۳-۳- اعمال جعبه‌های جابجایی S-box

در این مرحله مقادیر ۸-بیتی ماتریس $K(i)$، $1 \le i \le 2m$ به‌ترتیب به دو S-box ۸-بیتی S_0 و S_1 استفاده‌شده در رمز قالبی استاندارد CLEFIA اعمال می‌شوند و ماتریس جدید $Key(i)$، $1 \le i \le 2m$ را ایجاد می‌کنند. CLEFIA یک الگوریتم رمز قالبی است که با شرکت Sony توسعه یافته است [39]. اندازه قالب داده در این رمز ۱۲۸ بیت است و اندازه کلید می‌تواند ۱۲۸ بیت، ۱۹۲ بیت یا ۲۵۶ بیت باشد. برای استفاده به‌عنوان رمز قالبی در سیستم‌های مدیریت حقوق دیجیتال[9] در نظر گرفته شده است. این تکنیک رمزنگاری با CRYPTREC اصلاح و در سال ۲۰۱۳ برای استفاده دولت ژاپن به کار گرفته شده است. با توجه به امنیت پذیرفتنی این رمز قالبی و اینکه S-boxهای آن از بهترین S-boxهای ۸-بیتی موجود و دارای مشخصه‌های امنیتی بسیار پذیرفتنی‌اند، در روش تولید کلید پیشنهادی برای افزایش میزان پیچیدگی داده‌های کلید از این S-boxها استفاده شده است. ساختار S-box S_0 براساس استفاده از ٤ S-box ٤-بیتی است. همچنین، ساختار S-box S_1 براساس واحد معکوس‌کردن میدانی در میدان متناهی $GF(2^8)$ است که دارای خصوصیات غیرخطی خوبی است. شکل ۱۰ مرحله اعمال جعبه‌های جابجایی S_0 و S_1 به ماتریس K را نشان می‌دهد. در این حالت ۸ بیت وارد هر S-box و ۸ بیت براساس جدول آنها [۳۵] تولید و خارج می‌شود.



شکل (۱۰): مرحله اعمال S-boxهای S_0 و S_1 ۸-بیتی CLEFIA به ماتریس K.

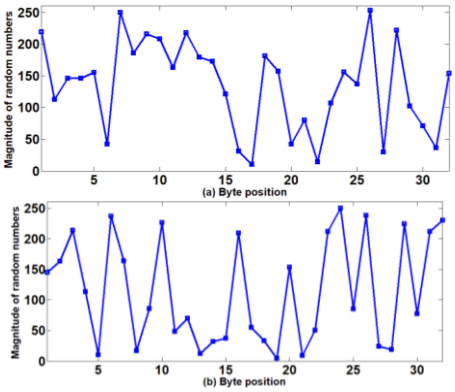
۴-۳- انتخاب مقادیر کلید

در این مرحله، مقادیر ماتریس Key برای ایجاد کلید

استفاده می‌شوند. براساس اینکه کلید چند بیتی باشد، مقادیر مختلفی انتخاب می‌شوند؛ برای مثال، برای طول کلیدهای ۱۲۸-بیتی، ۱۹۲-بیتی و ۲۵٦-بیتی به‌ترتیب ۱٦، ۲٤ و ۳۲ بایت از ماتریس *Key* نیاز است.

٤- بحث و نتایج

در این بخش، تجزیه‌وتحلیل‌های مختلفی برای روش تولید کلید تصادفی پیشنهادی با استفاده از اثر انگشت ارائه می‌شود. در اینجا از ابزار شبیه‌سازی Matlab R2013b برای این کار استفاده شده است. پایگاه داده‌ای که تصاویر اثر انگشت از آن استفاده شده، پایگاه داده شناخته‌شده FVC2002 DB1_B [41] است؛ برای مثال، شکل‌های ۱۱ (a) و (b) به‌ترتیب، کلیدهای تصادفی اول و دوم ۲۵٦-بیتی براساس تصویر اثر انگشت 102_1.tif را نشان می‌دهد. همان‌طور که دیده می‌شود شکل مقادیر کلید مانند یک سیگنال تصادفی است.



شکل (۱۱): نمودار کلیدهای استخراج شده از روش تولید کلید پیشنهادی اول (a) و دوم (b)، ۲۵٦-بیتی براساس تصویر اثر انگشت 102_1.tif.

دو نمونه اول کلید تولیدشده از تصویر اثر انگشت 102_1.tif در زیر نشان داده شده است.

K_1=1101101101110001100100101001001001
0011011001010101111101010111010110001
1101000010100011110110101011001110101
1010111001000111110000101010110101100111
0100101010010100000000111001101011001
1001000100111111101000111101101111001
0110010001110010010010011010

K_2=10010001101000111101011001110001
0001010111011011010010000010001010101
1110001000110000010001100000110000100000
0001001011101000100110111001000010000001
0010011001000010010011001011010100111111
0100101010111101110000110000001001111100
0000010011011101010011100110

در ادامه، این بخش ضمن انجام تحلیل‌های تصادفی مقایسه با کارهای مرتبط پیشین انجام شده است.

زمان محاسبهٔ کلید رمزنگاری برای کار پیشنهادی و چند کار موجود در جدول ۲ آورده شده است. در این جدول برای مقایسه بهتر سخت‌افزار استفاده‌شده نیز بیان شده است. همان‌طور که مشاهده می‌شود زمان لازم برای محاسبه کلید در کار پیشنهادی پذیرفتنی است.

جدول (۲): مقایسهٔ زمان محاسبهٔ کلید رمزنگاری برای کار پیشنهادی و چند کار موجود.

کار	زمان (میلی‌ثانیه)	سخت‌افزار
[28]	۲۹,۸۰۸۵	---
[27]	۱۰,۱۱	Intel® Core TM i5 processor with 2.3 GHz
[42]	٦۰,۰۵۲	Intel ®Core TM 2 Duo processor with 2.4 GHz
[38]	14	ARM processor Broadcom SoC BCM2837B0 of 1.4GHz
کار پیشنهادی	۲۰,۵۷	Intel® Core TM i5 processor with 2.3 GHz

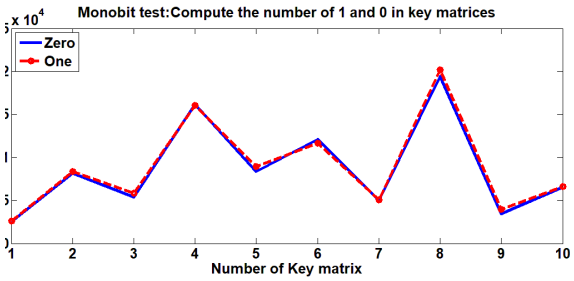
٤-۱- تحلیل تصادفی

برای بررسی تصادفی‌بودن توالی مقادیر بیت‌های کلید تجزیه‌وتحلیل آماری براساس تست‌های ارائه‌شده در کار [43] و بعضی پارامترهای دیگر انجام می‌گیرد. در ادامه تست‌های مدنظر و پارامترهای مهم در این زمینه بررسی بیشتری شده‌اند.

- تست Monobit

در این تست تعداد بیت‌های ۱ و ۰ در کل مقادیر ماتریس کلید محاسبه می‌شوند. اگر درصد تعداد بیت‌های ۱ و ۰ به هم نزدیک باشند، یعنی نزدیک ۵۰ درصد برای هرکدام باشد، نشان می‌دهد توزیع بیت‌های ۱ و ۰ در کل ماترسی یکنواخت است. این امر نشان‌دهندهٔ تصادفی‌بودن

مقادیر کلید است. در اینجا تست برای ماتریس‌های کلید تولیدشده براساس ۱۰ تصویر اثر انگشت 101_1.tif تا 110_1.tif از پایگاه داده اثر انگشت FVC2002 DB1_B بررسی شده است. شکل ۱۲ مقادیر تعداد بیت‌های ۱ و ۰ در ماتریس کلید تولیدشده از این ۱۰ تصویر اثر انگشت را نشان می‌دهد. محور افقی شماره تصویر است که به‌ترتیب از ۱ تا ۱۰ است و محور عمودی مقدار مربوط به تعداد بیت‌های ۱ و ۰ است. نمودار آبی رنگ مربوط به تعداد بیت‌های ۰ است و نمودار قرمز خط‌چین‌شده مربوط به تعداد بیت‌های ۱ است. همان‌طور که در این شکل دیده می‌شود نمودارهای مربوط به تعداد بیت‌های ۱ و ۰ در ماترسی‌های کلید تولیدشده بر همدیگر منطبق بوده و نشان‌دهندهٔ نزدیک‌بودن تعداد بیت‌های ۱ و ۰ در کلید است؛ بنابراین، کلید تولیدشده با روش پیشنهادی دارای ویژگی‌های تعادل تعداد بیت‌های ۰ و ۱ و امنیت مناسبی است.



شکل (۱۲): نمودار مقادیر تعداد بیت‌های ۱ و ۰ در ماتریس کلید تولیدشده از ۱۰ تصویر اثر انگشت 101_1.tif تا 110_1.tif از پایگاه داده DB1_B. FVC2002.

برای به دست آوردن معیاری برای مقایسه با کارهای دیگر معیار Monobit در نظر گرفته می‌شود. این معیار براساس کار [۴۳] به‌صورت نسبت تعداد یک‌های ماتریس کلید تقسیم بر تعداد کل بیت‌های کلید تعریف می‌شود. در حالت ایدئال مقدار این معیار باید برابر ۰٫۵ باشد که نشان‌دهندهٔ برابربودن تعداد صفرها و یک‌های کلید و توزیع یکنواخت آنها است. مقدار به‌دست‌آمده برای معیار Monobit در روش پیشنهادی تولید کلید برای ماتریس‌های کلید مربوط به تصاویر اثر انگشت 101_1.tif تا 110_1.tif از پایگاه داده FVC2002 DB1_B به‌ترتیب برابر اعداد 0.5087، 0.5066، 0.5204، 0.4978، 0.5169، 0.4902، 0.5027، 0.5100، 0.5368 و 0.5025 است. میانگین این اعداد نیز برابر عدد 0. 5093 است. براساس این اعداد به‌دست‌آمده که همهٔ آنها بسیار به عدد 0.5 نزدیک‌اند، می‌توان به این نتیجه رسید که پراکندگی داده‌های ماتریس‌های کلید مطلوب است. در جدول ۳ نیز مقدار معیار Monobit برای مقایسه روش پیشنهادی و چند کار مرتبط دیگر آورده شده است. همان‌طور که در این جدول مشاهده می‌شود نتیجه به‌دست‌آمده برای روش پشنهادی در مقایسه با کارهای پیشین پذیرفتنی است.

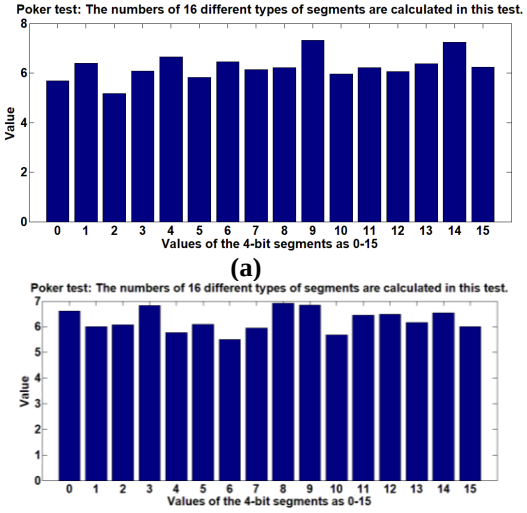
جدول (۳): مقایسه معیار Monobit برای کار پیشنهادی و کارهای مرتبط دیگر.

کار	میانگین معیار Monobit
[29]	0.5193
[43]	0.4993
[44]	0.1159
[18]	0.2888
[18]	0.3767
[18]	0.7236
[18]	0.8596
[45]	۰٫۵۲۰۰
کار پیشنهادی	0.5093

- تست Poker

در این تست تمام مقادیر ۸-بیتی کلید تولیدشده به دو قسمت ٤-بیتی تقسیم می‌شوند؛ برای مثال، یک عدد ۸-بیتی از دو قسمت ٤-بیت کم‌ارزش و ٤-بیت پرارزش تشکیل می‌شود. بعد از این کار آمار تعداد کل اعداد ٤-بیتی حساب می‌شود. همان‌طور که می‌دانیم یک عدد ٤-بیتی می‌تواند بین ۰ تا ۱۵ باشد؛ بنابراین، بعد از محاسبه‌کردن آمار تعداد اعداد ٤-بیتی، آماری از تعداد اعداد ۰ تا ۱۵ از کل دنباله به دست آمد. حال اگر تعداد شمارش‌شدهٔ این اعداد در یک رنج باشد، نشان‌دهندهٔ توزیع یکنواخت داده‌ها در کل ماتریس تولید کلید است. در این تست برای ۱۰ تصویر اثر انگشت 101_1.tif تا 110_1.tif از پایگاه داده اثر انگشت

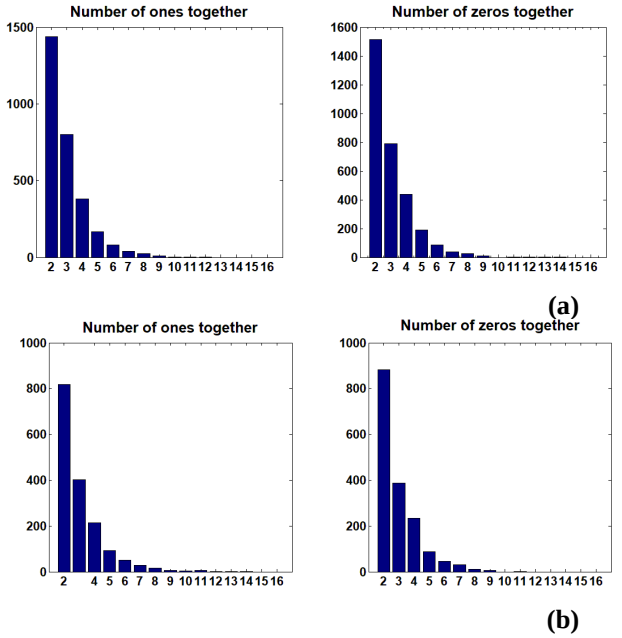
FVC2002 DB1_B این کار انجام شد و نتایجی پذیرفتنی از این تست به دست آمد. با توجه به حجم زیاد داده‌ها در اینجا، برای مثال، فقط دو نمونه از نتایج مربوط به تصویر اثر انگشت 102_1.tif و 104_1.tif آورده شده است که به‌ترتیب در شکل ۱۳ (a) و (b) نشان داده شده‌اند. محور افقی در این نمودارها نشان‌دهندهٔ اعداد ۰ تا ۱۵ (معادل اعداد ٤-بیتی) است و محور عمودی مقدار شمارش هر عدد را نشان می‌دهد. همان‌طور که دیده می‌شود اندازه ستون‌ها در سطح‌های نزدیک به‌هم‌اند؛ درنتیجه، تعداد شمارش‌شدهٔ اعداد ۰ تا ۱۵ در کل ماترس کلید تولیدشده با درصد پذیرفتنی به یکدیگر نزدیک‌اند.



شکل (۱۳): نمونه نمودار مربوط به تست Poker برای ماتریس کلید تولید شده از تصویر اثرانگشت 102_1.tif (a) و 104_1.tif (b).

- تست Run

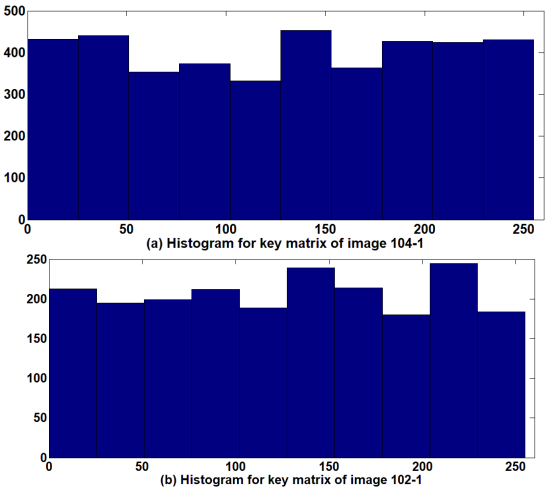
بیشترین تعداد بیت ۱ یا ۰ به‌هم‌پیوسته در دنباله اعداد کلید به‌عنوان run تعریف می‌شود [43]. اگر این تعداد بیت ۱ یا ۰ به‌هم‌پیوسته به اعداد بسیار بزرگ منجر شود، نامطلوب است. این امر نشان‌دهندهٔ توزیع غیر یکنواخت بیت‌های ۱ یا ۰ در دنباله اعداد است. در اینجا تعداد بیت‌های صفر و یک به‌هم‌پیوسته با طول ۲ تا ۱٦ محاسبه شده‌اند. نتایج برای تعداد بیت‌های ۱ به‌هم‌پیوسته مشابه تعداد بیت‌های ۰ به دست آمده‌اند؛ برای مثال، شکل ۱٤ تعداد شمارش بیت‌های ۰ و ۱ به‌هم‌پیوسته با طول ۲ تا ۱٦ را برای دو تصویر اثر انگشت 106_1.tif و 110_1.tif از پایگاه داده اثر انگشت FVC2002 DB1_B نشان می‌دهد. تعداد بیت به‌هم‌پیوسته در زیر هر ستون مشخص شده است. همان‌طور که در این تصاویر دیده می‌شود هر چقدر طول بیت‌های ۰ و ۱ به‌هم‌پیوسته زیاد می‌شود، اندازه ستون‌ها کاهش می‌یابد. با بررسی رفتار کاهشی تعداد بیت‌های ۰ و ۱ به‌هم‌پیوسته با افزایش طول بیت‌ها از ۲ تا ۱٦ این نتیجه به دست می‌آید که این تعداد برای طول‌های بیش از ۱٦ بیت ۰ یا ۱ به‌هم‌پیوسته تقریباً به صفر می‌رسد. این امر نشان‌دهندهٔ توزیع بسیار مناسب بیت‌های ۰ و ۱ در ماتریس کلید است. در کارهای [۲۲]، [۲۳]، [۲٤]، [۲۵] و [۲٦] که براساس سیگنال EEG کلید تولید کرده‌اند، حداکثر تعداد یک به‌هم‌پیوسته به‌ترتیب برابر ۱۰۰، ۱۰۰، ۹۷، ۹۷ و ۹۹ است. این در حالی است که در روش پیشنهادی حداکثر تعداد یک به‌هم‌پیوسته برابر عدد ۱٦ است. برای کار [43] تعداد بیت‌های صفر یا یک به‌هم‌پیوسته برای تعداد ۲۵ تا به بالا برابر صفر می‌شود؛ بنابراین، در کار [43] تعداد صفرها یا یک‌های به‌هم‌پیوسته نسبت به کلیدهای تولیدشده در روش پیشنهادی بیشتر است.



شکل (۱٤): نمودار تعداد شمارش بیت‌های ۰ و ۱ به‌هم‌پیوسته با طول ۲ تا ۱٦ بیت برای دو تصویر اثر انگشت 106_1.tif (a) و تصویر 110_1.tif (b) از پایگاه داده اثر انگشت FVC2002 DB1_B.

٤-٢- هیستوگرام مقادیر کلید تصادفی

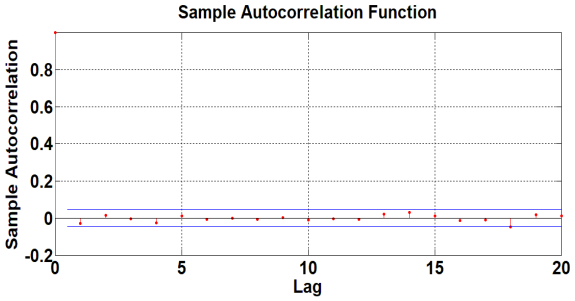
هیستوگرام مقادیر ماتریس کلید تصادفی به‌ترتیب برای دو تصویر اثر انگشت ورودی 104_1.tif و 102_1.tif در شکل‌های ۱۵ (a) و (b) نشان داده شده است. توزیع مقادیر کلید تصادفی در هیستوگرام نشان داده شده است. اگر نمودار به اندازه کافی مسطح نباشد، مقدار چشمگیری از داده‌ها می‌تواند با حمله آماری تهدید شود. در رمزنگاری، پاسخ مسطح و یکنواخت برای هیستوگرام بسیار مطلوب [46] است. تمام بایت‌های کلید تصادفی در محدوده ۰ تا ۲۵۵ با مقدار شمارش بسیار زیاد (تعداد وقوع اعداد تصادفی) رخ می‌دهد. مقدار شمارش برای اعداد تصادفی کلیدهای نزدیک به یکدیگر است. این امر نشان می‌دهد هر مقداری در محدوده ۰ تا ۲۵۵ می‌تواند در تولید مقادیر کلید رخ دهد؛ بنابراین، هیستوگرام مقادیر تصادفی کلید توزیع یکنواختی دارد.



شکل (۱۵): هیستوگرام مقادیر ماتریس کلید تصادفی به‌ترتیب برای دو تصویر اثر انگشت ورودی 104_1.tif (a) و (b) 102_1.tif.

٤-٣- همبستگی خودکار مقادیر کلید تصادفی

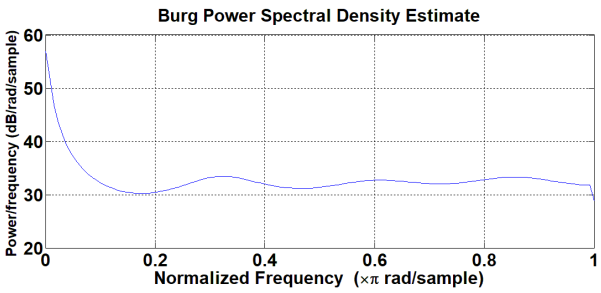
همبستگی خودکار، همبستگی سیگنال با خودش است؛ برای مثال، همبستگی خودکار مقادیر کلید تصادفی برای تصویر 102_1.tif در شکل ۱۶ نشان داده شده است. مقادیر بسیار کمی دارد، همبستگی کمی بین مقادیر و میزان بالایی از تصادفی‌بودن را نشان می‌دهد. با توجه به اینکه بیشترین مقدار در همبستگی خودکار برابر با ۰,۰۴۸۲ است، مقادیر کلید تصادفی هیچ شباهت درخور توجهی با خود ندارند که این امر یک ضرورت اساسی برای قابلیت تصادفی‌بودن است.



شکل (۱۶): همبستگی خودکار مقادیر کلید تصادفی پیشنهادی برای تصویر 102_1.tif.

٤-٤- چگالی طیفی توان مقادیر کلید تصادفی

چگالی طیفی توان مقادیر کلید تصادفی برای تصویر 102_1.tif در شکل ۱۷ نشان داده شده است. چگالی طیفی توان، توان تغییرات را تابعی از فرکانس نشان می‌دهد. همان‌طور که از این شکل دیده می‌شود چگالی طیفی توان مقادیر کلید تصادفی تقریباً مسطح است؛ مشابه مساوی سیگنال‌های تصادفی؛ بنابراین، این مسئله، تصادفی‌بودن مقادیر کلید را تأیید می‌کند.



شکل (۱۷): چگالی طیفی توان مقادیر کلید تصادفی پیشنهادی برای تصویر 102_1.tif.

۵- نتیجه‌گیری

در این مقاله برای تولید کلیدهای رمزنگاری تصادفی از ویژگی‌های بیومتریک اثر انگشت استفاده شده است. با استفاده از تولید کلید تصادفی، امنیت الگوریتم‌های

رمزنگاری بهبود می‌یابد. تولید کلیدهای تصادفی در رمزنگاری با حجم زیادی از داده‌ها مانند رمزگذاری تصویر و صدا امری ضروری است. در روش پیشنهادی، ابتدا ویژگی‌های منحصربه‌فرد اثر انگشت شامل نقاط مینوشیا از تصویر اثر انگشت استخراج می‌شوند، سپس برای افزایش ویژگی‌های آماری و پیچیدگی، فاصله اقلیدوسی و زوایای بین تمام نقاط مینوشیا نسبت به یکدیگر، حساب و در دو ماتریس جداگانه ذخیره می‌شوند. در مرحله بعد، داده‌های این ماتریس‌ها بعد از نرمالیزه‌شدن به اعداد ۸-بیتی با عملیات جایگشت مخصوص به خود جابجا می‌شوند. در ادامه، با یک عمل جایگشت دیگر این دو ماتریس در همدیگر ترکیب می‌شوند و یک ماترس ایجاد می‌کنند. سپس برای افزایش سطح امنیت و قابلیت تصادفی‌بودن بیشتر داده‌های ۸-بیتی این ماتریس به S-boxهای ۸-بیتی S_0 و S_1 استفاده‌شده در رمز قالبی CLEFIA اعمال می‌شوند که واحدهایی غیر خطی‌اند. استفاده از این ویژگی‌ها در تولید کلید تصادفی به آشفتگی و پخش داده‌های کلید منجر می‌شود. آنالیزهای آماری صورت‌گرفته روی کلیدهای تولیدشده نشان‌دهندهٔ ویژگی تصادفی‌بودن پذیرفتنی کلیدها است.

مراجع

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

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

[3] H.N. Noura, A. Chehab, C. Raphael, "Efficient & secure cipher scheme with dynamic key-dependent mode of operation", Signal Processing: Image Communication, Vol. 78, No. 3, pp. 448-464, 2019.

[4] R. Ismail Abdelfatah, "Secure Image Transmission Using Chaotic-Enhanced Elliptic Curve Cryptography", IEEE Access, Vol. 8, No. 2, pp. 3875-3890, 2019.

[5] R. Shanthakumari, and S. Malliga, "Dual layer security of data using LSB inversion image steganography with elliptic curve cryptography encryption algorithm", Multimedia Tools and Applications, Vol. 79, No. 4, pp. 3975-3991, 2020.

[6] C.H. Yang, H.C. Wu, and S.F. Su, "Implementation of Encryption Algorithm and Wireless Image Transmission System on FPGA", IEEE Access, Vol. 7, No. 6, pp. 50513-50523, 2019.

[7] L. You, E. Yang, and G. Wang, "A novel parallel image encryption algorithm based on hybrid chaotic maps with OpenCL implementation", Soft Computing, Vol. 24, No. 4, pp. 12413-12427, 2020.

[8] F.J. Farsana, K. Gopakumar, "A Novel Approach for Speech Encryption: Zaslavsky Map as Pseudo Random Number Generator", Procedia Computer Science, Vol. 93, No. 3, pp. 816-823, 2016.

[9] X. Wang, Y. Su, "An Audio Encryption Algorithm Based on DNA Coding and Chaotic System", IEEE Access, Vol. 8, No. 2, pp. 9260-9270, 2020.

[10] P. Sathiyamurthi, and S. Ramakrishnan, "Speech encryption algorithm using FFT and 3D-Lorenz-logistic chaotic map", Multimedia Tools and Applications, Vol. 79, No. 1, pp. 17817-17835, 2020.

[11] P. Sathiyamurthi, and S. Ramakrishnan, "Speech encryption using chaotic shift keying for secured speech communication", EURASIP Journal on Audio, Speech, and Music Processing, Vol. 20, No. 3, pp. 1-11, 2017.

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

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

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

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

5, 2010.
[16] I.Q. Abduljaleel, S.A. Abdul-Ghani, and H.Z. Naji, "An Image of Encryption Algorithm Using Graph Theory and Speech Signal Key Generation", Journal of Physics: Conference Series, Vol. 1804, No. 4, pp. 1-11, 2021.
[17] I.A. Majjed, and A.M Majeed, "Key Generation Based on Facial Biometrics", in Proc. the 1st International Multi-Disciplinary Conference Theme: Sustainable Development and Smart Planning, University of Bradford, UK, pp. 1-9, 2020.
[18] M. Yuliana, G. Wirawan, and A. Suwadi, "A Simple Secret Key Generation by Using a Combination of Pre-Processing Method with a Multilevel Quantization", Entropy, Vol. 21, No. 1, pp. 1-25, 2019.
[19] A. Bano, "Random Key Generator Using Human Voice", in Proc. International Multimedia, Signal Processing and Communication Technologies, Aligarh, India, pp. 41-45, 2013.
[20] J. Srinivas, D. Mishra, S. Mukhopadhyay, S. Kumari, "Provably secure biometric based authentication and key agreement protocol for wireless sensor networks", J Ambient Intell Humaniz Comput, Vol. 9, No. 4, pp. 875-895, 2018.
[21] L.N. Pradeep, and A. Bhattacharjya, "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, Mysore, India, pp. 63-69, 2013.
[22] D. Nguyen, D. Tran, D. Sharma, and W. Ma, "Investigating The Impact Of Epilepsy On EEG-based Cryptographic Key Generation Systems", in Proc. International Conference on Knowledge Based and Intelligent Information and Engineering Systems, Marseille, France, pp. 177-185, 2017.
[23] D. Nguyen, D. Tran, D. Sharma, and W. Ma, "Emotional Influences on Cryptographic Key Generation Systems using EEG signals", in Proc. 22nd International Conference on Knowledge-Based and Intelligent Information & Engineering Systems, Belgrade, Serbia, pp. 703-712, 2018.
[24] D. Nguyen, D. Tran, D. Sharma, and W. Ma, "On the Study of Impacts of Brain Conditions on EEG-based Cryptographic Key Generation Systems", in Proc. 22nd International Conference on Knowledge-Based and Intelligent Information & Engineering Systems, Belgrade, Serbia, pp. 713-722, 2018.
[25] D. Nguyen, D. Tran, D. Sharma, "A Study on the Impact of Alcoholism on EEG-based Cryptographic Key Generation Systems", in Proc. IEEE Symposium Series on Computational Intelligence (SSCI), Canberra, Australia, pp. 79-85, 2020.
[26] D. Nguyen, D. Tran, D. Sharma, and W. Ma, "On The Study of EEG-based Cryptographic Key Generation", in Proc. International Conference on Knowledge Based and Intelligent Information and Engineering Systems, Marseille, France, pp. 936-945, 2017.
[27] R. Dwivedi, S. Dey, M.A. Sharma, A. Goel, "A fingerprint based crypto-biometric system for secure communication", Journal of Ambient Intelligence and Humanized Computing, Vol. 11, No. 4, pp. 1495-1509, 2019.
[28] S. Barman, D. Samanta, S. Chattopadhyay, "Fingerprint-based crypto-biometric system for network security", EURASIP Journal on Information Security, Vol. 3, No. 5, pp. 1-17, 2015.
[29] G. Panchal, D. Samanta, "A Novel Approach to Fingerprint Biometric-Based Cryptographic Key Generation and its Applications to Storage Security", Computers and Electrical Engineering, Vol. 69, No. 1, pp. 461-47, 2018.
[30] S. Barzut, M. Milosavljevic, S. Adamovic, M. Saracevic, N. Macek, M. Gnjatovic, "A Novel Fingerprint Biometric Cryptosystem Based on Convolutional Neural Networks", Mathematics, Vol. 9, No. 7, pp. 1-12, 2021.
[31] S. Li, X. Zhang, Z. Qian, G. Feng, Y. Ren, "Key based Artificial Fingerprint Generation for Privacy Protection", IEEE Transactions on Dependable and Secure Computing, Vol. 17, Iss. 4, pp. 828- 840, 2020.
[32] K. Suresh, R. Pal, S.R. Balasundaram, "Fingerprint Based Cryptographic Key Generation", International Conference on Intelligent Data Communication Technologies and Internet of Things, India 38, pp. 704-713, 2020.
[33] J.G. Jo, J.W. Seo, H.W. Lee, "Biometric Digital Signature Key Generation and Cryptography Communication Based on Fingerprint", International Workshop on Frontiers in Algorithmics, Lanzhou, China, pp. 38-49, 2007.
[34] P. Wang, L. You, G. Hu, L. Hu, Z. Jian, C. Xing, "Biometric Key Generation Based on Generated Intervals and Two-layer Error Correcting Technique", Pattern Recognition, Vol. 111, No. 6, pp. 1-36, 2020.
[35] A. Sarkar, B.K. Singh, "Cryptographic Key

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

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

[42] J.J. Wang, J.Y. Chen, X.Y. Yang, "Research on generating good key sequence based on chaos", Int. J. High Performance Computing and Networking, Vol. 9, No. 5, pp. 480-488, 2016.

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

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

[44] R. Nagakrishnan, and A. Revathi, "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, pp. 1070-1080, 2018.

Generation from Cancelable Fingerprint Templates", Int'l Conf. on Recent Advances in Information Technology, Dhanbad, India, pp. 1-6, 2018.

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

[37] P. Penchalaiah, and K. Ramesh Reddy, "Random multiple key streams for encryption with added CBC mode of operation", Perspectives in Science, Vol. 8, No. 2, pp. 57-60, 2016.

[38] R. Montero-Canela, E. Zambrano-Serrano, E.I. Tamariz-Flores, J.M. Munoz-Pacheco, and R. Torrealba-Melendez, "Fractional chaos based-cryptosystem for generating encryption keys in Ad Hoc networks", Ad Hoc Networks, Vol. 97, No. 4, pp. 1-21, 2020.

[39] T. Shirai, K. Shibutani, T. Akishita, "The 128 14; bit block cipher CLEFIA (extended abstract)", Proc. Int. Workshop on Fast Software Encryption, Luxembourg (LNCS, 4593), pp. 181-195, 2007

[40] V.K. Alilou, "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.

[1] Confusion
[2] Diffusion
[3] Cancelable fingerprint template
[4] Codeword
[5] Threshold
[6] Binarization
[7] Thinning
[8] Crossing Number
[9] Digital right manager (DMR)