# بیومتریک به عنوان یک روش رمزنگاری برای امنیت شبکه

**میلاد خزائی*[۱]، حمیدرضا رحمانی[۲]، علی زاغیان[۳]**

**۱- دانشگاه صنعتی مالک اشتر، کارشناسی ارشد، دانشکده مهندسی رمز، اصفهان، ایران**

**۲- دانشگاه صنعتی مالک اشتر، کارشناسی ارشد، دانشکده مهندسی رمز، اصفهان، ایران**

**۳- دانشگاه صنعتی مالک اشتر، هیئت علمی، دانشکده مهندسی رمز، اصفهان، ایران**

**چکیده**

پیش زمینه و هدف: رمزنگاری به عنوان یک روش موثر برای انتقال امن داده‌ها محسوب می‌شود و قصد ممانعت از حملات به شبکه را دارد. طرح رمزگذاری و رمزگشایی مبتنی بر بیومتریک از اثر انگشت برای تولید یک کلید منحصر به فرد استفاده می‌کند. روش: روش ارائه شده در این مقاله، بخش‌هایی از اثر انگشت فرستنده و گیرنده را برای تولید یک دنباله تصادفی ترکیب می‌کند، که به عنوان یک کلید عمومی برای رمزگذاری و همچنین رمزگشایی استفاده می‌شود. بنابراین مشخص می‌شود که کلید تولید شده با امضای بیومتریک فرستنده علامت گذاری شده است. پیام رمزگذاری شده همراه با کلید به گیرنده ارسال می‌شود و گیرنده از این کلید برای رمزگشایی پیام به متن اصلی استفاده می‌کند. یافته‌ها: این سیستم دارای مزیت قابل توجهی است، زیرا هیچ الزامی برای ذخیره کردن کلید نامتقارن در مکان محافظت شده نمی‌باشد. بنابراین تهدیدات امنیتی به حداقل ممکن کاهش می‌یابد. اثر انگشت صفت ذاتی هر فرد و متمایز از دیگران است. از این رو میلیاردها کلید منحصر به فرد ایجاد می‌شود که حدس زدن کلید را برای مهاجم بسیار سخت می‌کند. کاربرد: سیستم مبتنی بر بیومتریک به طور قابل توجهی توانایی سیستم‌های رمزنگاری سنتی را افزایش می‌دهد.

**کلید واژه ها:** سیستم مبتنی بر بیومتریک، تمایز، رمزگذاری، اثر انگشت، حملات شبکه

* **Email:** Milad.Khazaie@hotmail.com

## ۱. مقدمه

با افزایش چشم‌گیر در مبادله اطلاعات در چند سال گذشته، انتقال قابل اعتماد و ذخیره سازی اطلاعات حساس تبدیل به یک جنبه حیاتی امنیت شبکه شده است. داده‌ها حین عبور از شبکه در آسیب پذیرترین وضعیت ممکن قرار دارد، زیرا هدف بسیار آسانی برای هر مهاجم موجود در شبکه است. یک حمله غیر فعال از طریق یک شبکه مانند مسدود کردن یا خراب کردن می‌تواند به آسانی داده‌های در هر حال انتقال را از بین ببرد. برای انتقال امن اطلاعات از طریق یک کانال نا امن، رمزنگاری به عنوان موثرترین روش در نظر گرفته می‌شود. رمزنگاری از هزاران سال پیش، از حروف الفبای مصری[۱] تا ماشین انیگما [۲] و تا قرن بیست و یکم وجود داشته است. اطلاعات ارسال شده بر روی هر شبکه قابل دسترسی، باید رمزگذاری شود تا برای هر فرد دیگری غیر از گیرنده مورد نظرغیر قابل فهم باشد و این دقیقا همان چیزی است که رمزنگاری انجام می‌دهد. این فرآیند تبدیل متن اصلی[۳] یعنی متن قابل خواندن به متن غیر قابل خواندن یا رمزگذاری[۴] شده است. رمزنگاری را می‌توان برای داده‌هایی استفاده کرد که افراد یا سازمان‌ها می‌خواهند داده‌هایی را خصوصی نگه دارند یا فقط برای برخی از کاربران‌شان قابل دسترسی باشد. به عبارت دیگر، رمزنگاری مخفی کردن محتوای پیغام از کاربران ناخواسته و غیر مجاز است. رمزنگاری در هنگام ارسال اطلاعات از طریق شبکه به طرف فرستنده انجام می‌شود. گیرنده در پایان، به محض دریافت متن رمز شده فرآیند رمزگشایی را آغاز می‌کند[۱]. اما نقص در روش‌های الگوریتم رمزنگاری یک دروازه عبور برای مهاجمان است که می‌تواند بسته‌های داده را که با استفاده از ابزارهای خودکار در حال عبور از شبکه هستند، مورد حمله و رمزگشایی قرار دهد[۲]. روش رمزنگاری در ترکیب با رویکرد رمزنگاری بیومتریک، پاسخ جهانی جدید به مشکلات شبکه و امنیت اطلاعات است. بیومتریک ویژگی‌های منحصر به فرد، افراد است که فرد را از دیگران متمایز می‌کند. هویت فرد می‌تواند با استفاده از چنین روش‌هایی تأیید شود.

## ۲. رمزگذاری

روش‌های رمزنگاری مدرن، با استفاده از الگوریتم‌های رمزنگاری برای رمزگذاری اطلاعات، معاملات بانکی، معاملات اینترنتی آنلاین، ارتباطات بی سیم و ... استفاده می‌کنند. یک الگوریتم رمزنگاری ترکیبی از یک تابع ریاضی[۵] و یک کلید[۶] است. در اکثر موارد الگوریتم راز نیست، بلکه برای عموم شناخته شده است. قدرت تابع الگوریتمی و محرمانگی کلیدها تعیین می‌کند که چگونه داده‌های رمزگذاری شده ایمن است. بنابراین راز رمزنگاری، کلید است. مقادیر گرفته شده از فضای کلید مجاز که در یک دنباله تصادفی مرتب شده‌اند، کلیدهای رمزنگاری[۷] و رمزگشایی[۸] را تشکیل می‌دهند. تعداد کلیدهایی که به طور تصادفی در یک دنباله قرار دارند، می‌تواند از یک فضای کلید استخراج شوند که بستگی به اندازه فضای کلید دارد[۲،۳]. دو دسته گسترده از این نوع رمزنگاری‌ها بر اساس سطح امنیتی ارائه شده است. این روش‌ها رمزنگاری متقارن[۹] و نامتقارن[۱۰] است. بخش‌های زیر جزئیات این دو دسته را توضیح می‌دهند.

---

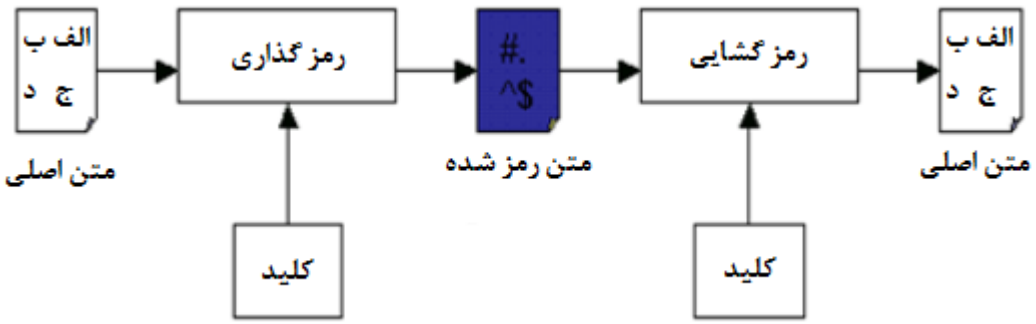
1. Egyptian Hieroglyphics
2. Enigma Machine
3. Plain Text
4. Cipher Text
5. Mathematical Function
6. Key
7. Encryption
8. Decryption
9. Symmetric
10. Asymmetric

### ۱. ۲. رمزگذاری متقارن

قدیمی‌ترین و شناخته شده‌ترین روش استفاده شده در رمزنگاری، روش رمزنگاری متقارن است[۴]. سیستم‌های رمزنگاری که از این روش استفاده می‌کنند یک کلید واحد برای فرآیندهای رمزنگاری و رمزگشایی را حفظ می‌کند. فرستنده پیامی را که می‌خواهد با یک کلید مخفی به گیرنده ارسال کند، رمزگذاری می‌کند و گیرنده با یک کپی از همان کلید، پیام را رمزگشایی می‌کند. کلید مخفی می‌تواند هر چیزی مانند یک عدد، یک کاراکتر خاص، یک کلمه باشد یا فقط یک دنباله از کاراکترهای تصادفی باشد و برای تغییر متن اصلی به متن رمزگذاری شده استفاده می‌شود تا به نحوی خاص به گیرنده ارسال شود[۵]. اگر فرستنده می‌خواهد یک پیام دیگر را رمزگذاری کند و آن را به گیرنده دیگری ارسال کند، باید کلید مخفی دیگری استفاده شود. همانطور که تعداد گیرنده‌ها و پیام‌ها در معادله افزایش می‌یابد، همچنین تعداد کلیدهای مخفی نیز افزایش پیدا می‌کند، این مشکل بزرگی برای فرستنده می‌شود.

اگر چه مشکلات مطرح شده در بالا خطر امنیت داده‌ها را در پی دارد، مکانیزم‌های رمزگذاری متقارن سریع هستند و می‌توانند برای رمزگذاری بلوک‌های بزرگی داده‌ها استفاده شوند. دو نوع الگوریتم متقارن که در حال حاضر استفاده می شود، وجود دارد: رمزهای دنباله‌ای[۱] و رمزهای بلوکی[۲]. صرف نظر از الگوریتم‌های استفاده شده، روش‌های رمزنگاری متقارن بر روی یک کلید برای رمزگذاری و رمزگشایی اطلاعات به شکل ۱ نشان داده شده است.

**شکل۱. رمزنگاری و رمزگشایی متقارن با استفاده از یک کلید واحد [۱۰]**



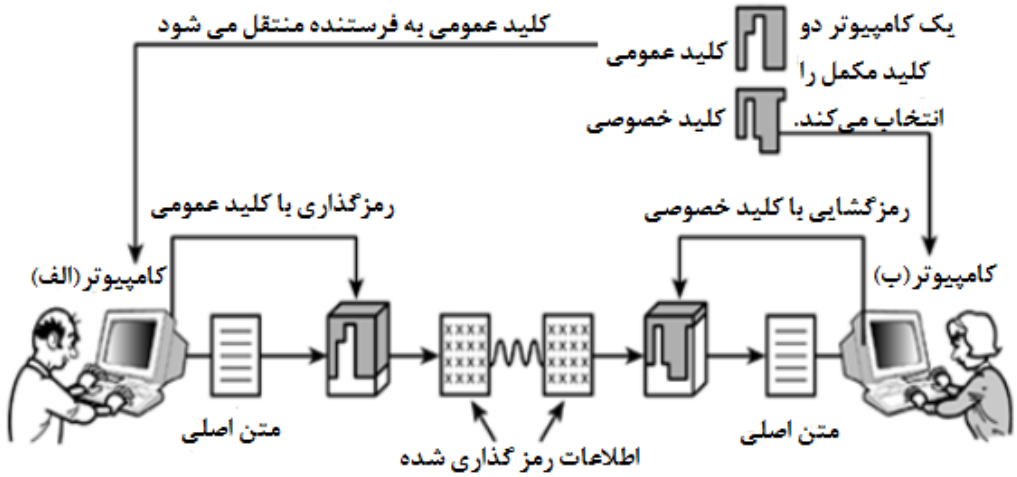

### ۲. ۲. رمزنگاری نامتقارن

اگر چه ارائه یک سطح بالایی از امنیت رمزگذاری متقارن نمی‌تواند وسیله‌ای امن برای مبادله کلید را فراهم کند و باید بر روی یک شبکه انجام شود و خطر حمله در هنگام انتقال آن را هم باید در نظرگرفت[۵]. یک پاسخ به این مسئله رمزنگاری نامتقارن است. همان‌طور که در شکل۲ نشان داده شده است، به جای یک کلید واحد، الگوریتم‌های نامتقارن از دو کلید ریاضی مرتبط استفاده می‌کنند که به عنوان یک جفت کلید شناخته می‌شوند، به طوری که یک کلید برای رمزگذاری استفاده می‌شود و رمزگشایی تنها با استفاده از کلید دوم امکان پذیر است. رویکرد رمزنگاری نامتقارن، برای رمزگذاری پیام از یک کلید عمومی که برای همه شناخته شده است استفاده می‌کند و از یک کلید خصوصی[۳] که تنها برای

[1]. Stream Cipher
[2]. Block Cipher
[3]. Private Key

گیرنده در نظر گرفته شده، برای رمزگشایی پیام استفاده می‌کند. رمزنگاری کلید عمومی[1] با استفاده از یک الگوریتم بر روی یک متن اصلی و یا داده انجام می‌شود و تنها با استفاده از یک الگوریتم مشابه توسط کلید خصوصی جفت شناخته می‌شود، که تنها گیرنده امکان رمزگشایی آن را دارد[۴].

**شکل۲. طرح رمزنگاری و رمزگشایی نامتقارن [۱۱]**




رمز گذاری نامتقارن این مشکل را در مورد به اشتراک گذاشتن کلید با گیرنده حل می‌کند، و این کلید قرار است عمومی باشد. با این وجود این روش به دلیل کندتر بودن در مقایسه با رمزنگاری متقارن با مشکل مواجه می‌شود[۶،۷]. هر دو رمزگذاری و همچنین فرایندهای رمزگشایی نیاز به پردازش بیشتری دارند. برخی از الگوریتم‌های کلید نامتقارن عبارتند از: RSA[2]، دیفی- هلمن[3] و امضای دیجیتال[4] [۴].

### ۳. سیستم های رمزنگاری بیومتریک

اگر چه رمزنگاری در انتقال امن داده‌ها از طریق یک کانال ناامن، دارای نقایص قابل ملاحظه‌ای است. پیام رمزگذاری شده بر اساس کلید است و نه اصالت کاربر. برای رمزنگاری قدرتمند، طول کلیدی که برای رمزگذاری و رمزگشایی استفاده می‌شود بسیار بزرگ است. اما هنوز هم این کلیدها می‌توانند توسط حملات لغت‌نامه[5] ساده حدس زده و یا شکسته شوند. علاوه بر این، نگهداری و به اشتراک گذاشتن چنین کلیدهای طولانی و تصادفی یک مشکل مهم در سیستم رمزنگاری است. این مشکلات با استفاده از سیستم‌های رمزنگاری بیومتریک[6] به خوبی حل می‌شود[۴،۸]. ادغام بیومتریک با الگوریتم‌های رمزنگاری یک سیستم رمزنگاری بیومتریک بسیار شناخته شده و قدرتمند را به ارمغان می‌آورد. این شامل استفاده از هر دو زمینه برای تقویت طرح رمزگذاری است. چنین

1. Public Key
2. Rivest–Shamir–Adleman
3. Diffie-Hellman
4. Digital Signature
5. Dictionary Attacks
6. Biometric Crypto Systems

سیستم‌هایی از امنیت رمزنگاری و منحصر به فرد بودن ویژگی‌های بیومتریک کاربر استفاده می‌کنند. بیومتریک نیاز به حفظ کلید و یا حتی تبادل آن را در یک شبکه قابل دسترسی حذف می‌کند. در چنین سیستمی، فرآیند تولید کلید شامل استفاده از صفات بیومتریک کاربر (به طور کلی اثر انگشت[1] یا عنبیه[2]) است و در پایگاه داده قابل دسترس برای هر فرستنده و گیرنده ذخیره می‌شود، که توسط سطح دیگری از احراز هویت بیومتریک تأمین می شود[۵،۹].

یکی از مزایای قابل توجه که همچنین یک ناکارآمدی است، سیستم یکپارچگی قالب و الگوی داده‌های بیومتریک در طول زمان است. همان‌طور که صفات بیومتریک به طور ذاتی غیرقابل تغییر هستند، زمانی که صاحب اثر به خطر افتاده، غیرقابل برگشت است و آن‌ها را غیر قابل استفاده و بالقوه تهدید می‌کند. این نتایج در داده‌های بیومتریک آن را به طور دائم بی فایده می‌کند. برای لغو یک قالب یا الگوی بیومتریک غیرقابل برگشت، یک تبدیل قابل لغو از همان مورد نیاز است. این مسئله یک مشکل از یک قالب سازنده را حل خواهد کرد. همچنین اطلاعات مربوط به الگو اصلی و حریم خصوصی داده‌های بیومتریک را بدون هیچ نشتی تضمین می‌کند. استفاده از راه دور داده‌های بیومتریک نیاز به انتقال آن از یک کانال نا امن (مانند اینترنت) دارد، از این رو ضروری است که کلید رمزنگاری قابل لغو از بیومتریک دو کاربر مختلف تولید شود[۱۰]. این روش تبدیل نتایج داده‌های بیومتریک را که توسط کاربر غیر مجاز یا مهاجم به دست می‌آید، غیرقابل برگشت می‌کند. تمرکز این مقاله تولید کلید رمزنگاری با استفاده از اثر انگشت به عنوان بیومتریک و انتخاب بدون به خطر انداختن حریم خصوصی و امنیت در فرآیند تولید کلید است.

### ۴. تجزیه و تحلیل اثر انگشت

هر انگشت دارای یک الگوی متمایز است و از سایر انگشت‌ها متفاوت است. این ویژگی دائمی و منحصر به فرد یک شخص است[۱۱]. با وجود اینکه الگوها بر روی هر انگشتی بر اساس طراحی رگه‌ها متفاوت‌اند و با چشم غیر مسلح قابل دیدن نمی‌باشند، از طریق تحقیقات فشرده در زمینه مینیاتور (نقاط غیر طبیعی در رگه‌ها که در شکل۳ نشان داده شده است) نشان می‌دهد که فاکتور تشخیصی نسبت به رگه‌ها[3] و شیارها[4] است. خاتمه دادن و پایان فوری یک رگه و شاخه، نقاط مبدأ دو شاخه رگه از جمله انواع مختلف مینیاتوری هستند و از مهم‌ترین و برجسته‌ترین آن‌ها استفاده می شود[۸،۱۲]. شکل کلی اثر انگشت به طور کلی برای پیش پردازش تصاویر استفاده می‌شود. این چاپ‌ها به ۳ طبقه تقسیم می‌شوند: حلقه[5]، پیچ[6] و قوس[7].

1. Fingerprint
2. Iris
3. Ridge
4. Furrow
5. Loop
6. Whorl
7. Arch

**شکل ۳. کلاس‌های اثر انگشت**


### ۵. ویژگی منحصر به فرد اثر انگشت[11]

- هر اثر انگشتی به افراد منحصر می‌شود، یعنی هیچ دو انگشت دارای ویژگی‌های یکسان نیستند.
- اکثر مردم دارای اثر انگشت قابل خواندن هستند و از این رو در طبیعت جهانی هستند.
- آنها مشخص هستند و بنابراین در شناسایی فرد بسیار مؤثر هستند.
- آنها در تمام طول عمر افراد بدون تغییر باقی می‌مانند.
- دقت در تشخیص افراد، اثر انگشت را به شکل گسترده‌ای از بیومتریک قابل استفاده می‌کند.

### ۶. تولید کلید رمزنگاری با استفاده از بیومتریک

یک طرح غیر قابل لغو تولید کلید رمزنگاری است که از طریق الگوریتم زیر ارائه شده است. بازده آن در توانایی برای تولید کلید از نقاط مینیاتوری استخراج شده از بیومتریک اثر انگشت است[۱۳]. روش استخراج نقطه مینیاتوری[1] با استفاده از یک ماتریس برای نشان دادن تصویر اسکن شده از اثر انگشت است. ماتریس شامل اطلاعات مربوط به تعداد رگه‌ها و شیارها می‌باشد. بنابراین هر عنصر در ماتریس مجموعه‌ای از تعداد رگه‌ها و شیارها در یک منطقه کوچک از تصویر اثر انگشت اسکن شده است.

[1]. Minutiae Points

### ۱. ۶. استخراج نقاط مینیاتور

این رویکرد سه مرحله‌ای است که در زیر آمده است:

- پیش پردازش[1]- مرحله اولیه اسکن اثر انگشت می‌باشد که با استفاده از یک اسکنر اثر انگشت به طوری یک نسخه دیجیتالی برای پردازش بیشتر بر روی کامپیوتر بارگذاری می‌شود.
- استخراج مینیاتور[2]- کپی دیجیتال از اثر انگشت اسکن شده برای استخراج نقطه مینیاتور پردازش می‌شود. از رگه و شیارها در این سیستم پیشنهادی به دلیل کاراکترهای متمایز آن‌ها استفاده می‌شود.
- پس پردازش[3]– مرحله نهایی ریز کردن رگه‌ها برای تشخیص مینیاتور می‌باشد.

### ۲. ۶. تقسیم‌بندی اثر انگشت اسکن شده

اثر انگشت اسکن شده یک تصویر سیاه و سفید هشت بیتی تولید می‌کند. این تصویر نیازمند تبدیل به تصویر یک بیتی برای پردازش دیجیتال است که در آن پیکسل نماینده یک نقطه رگه به آن صفر و همچنین پیکسل نماینده یک شیار به آن یک اختصاص داده شده است، در شکل۴ مشاهده می‌شود. روش تقسیم‌بندی[4] تصویر دیجیتال اسکن شده اثر انگشت را به مقادیر قابل تفسیر برای دستگاه تبدیل می‌کند. چنین روشی هر مقدار پیکسل را بررسی می‌کند و آن را با میانگین مقدار شدت مقایسه می‌کند. اگر مقدار بیشتری پیدا شود، مقدار پیکسل را به یک تغییر می‌دهد[۵،۹].

**شکل۴. اثر انگشت قبل و بعد از تقسیم بندی**

### ۳. ۶. نقاط مینیاتوری بدست آمده

اسکلت مجموعه‌ای از خطوط متصل از رگه‌ها با داشتن عرض واحد هستند. برای حفاظت از توپولوژی رگه‌ها و اتصال آن‌ها، روند نازک شدن اعمال می‌شود. فرایند نازک شدن رگه‌ها (اسکلت) با فرسایش تکراری مشخص می‌کند که پیکسل به عرض یک می‌رسد. پس از فرآیند تقسیم‌بندی و ریز شدن، مینیاتورها با استفاده از الگوی۳×۳ تعیین می‌شوند. اگرچه فرایند به نظر ساده می‌رسد، احتمال شناسایی‌های نادرست مینیاتور وجود دارد که نیاز به حذف لازم دارد. پس از استخراج

1. Preprocessing
2. Minutiae Extraction
3. Post Processing
4. Binarization

موفقیت آمیز از چندین مینیاتور، نیاز است که در قالبی ذخیره‌سازی انجام شود. موقعیت مینیاتور، جهت (به عنوان مثال زاویه[1]) و نوع (به عنوان مثال دوگانگی[2] و پایان‌دهی[3]) برخی از ویژگی‌های موجود در قالب است[۱۲].

### ۴. ۶. تولید کلید

در بخش زیر سیستم تولید کلید بر اساس الگوریتم پیشنهاد شده با استفاده از نقاط مینیاتور نشان داده شده است[۱،۱۴]. که با الهام از تعداد تحقیقات مرتبط در زمینه رمزنگاری و روش‌های بیومتریک قابل تعویض است. الگوریتم پیشنهاد شده در زیر آمده است که همان شکل۵ نشان داده شده است .

پیش فرض الگوریتم:

Mp → مجموعه نقاط مینیاتور

Kl → طول کلید

Np → اندازه مجموعه نقاط مینیاتور

S → مقدار دانه

Sl → حد دانه

M → (x, y)مینیاتور مختصات یک نقطه

Kv → بردار کلید

مراحل درگیر:

مرحله ۱: نمایش نقاط مینیاتور استخراج شده:

$$Mp\ \{mi\}i = 1.....Np \qquad (1)$$

مرحله ۲: تعیین بردار کلید (اولیه):

$$Kv = \{xi: p(xi)\}, \qquad i = 1 \ldots Kl$$

$$P(x) = Mp\ [I\ \%\ Np] + Mp[(i + 1)\ \%\ Np] + S \qquad (2)$$

مرحله ۳: مقادیر متغیر S به صورت زیر تعریف می‌شود که مقدار اولیه برابر با تعداد نقاط مینیاتور است:

$$S = Kv\ (i)\ \%\ S1, \qquad -1 < i < Kl \qquad (3)$$

[1]. Angle
[2]. Bifurcation
[3]. Termination

مرحله ۴: تبدیل بردار کلید (Kv) به ماتریس Km از اندازه $\frac{Kl}{2} * \frac{Kl}{2}$ به شرح زیر است:

$$Km = \frac{(aij)Kl}{2} * \frac{Kl}{2} \qquad (4)$$

مرحله ۵: تولید بردار کلید (متوسط):

KIV = {Ki: (m (Ki)}, i = 1.... .....Kl,

m(k) = |Aij|, Aij = Km i, j : i + sizw, j + siz

$$-1 < i < \frac{Kl}{2} \qquad (5)$$

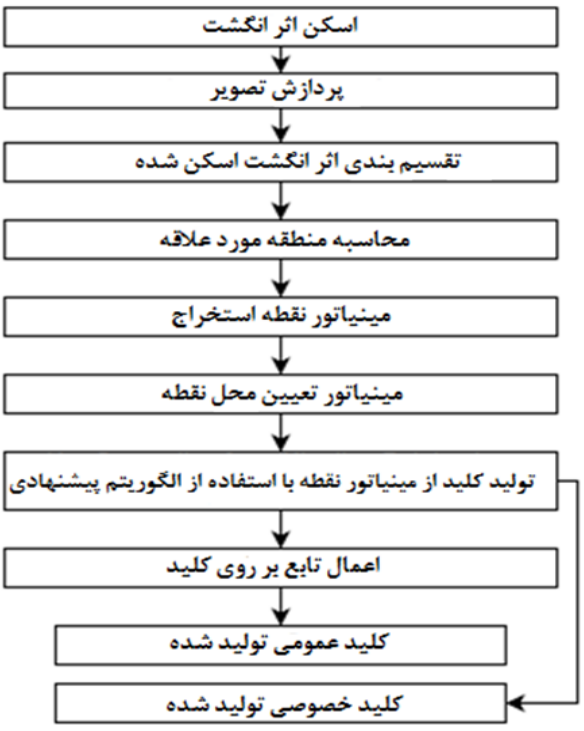
توجه: زیر ماتریس Aij از ماتریس کلید تولید می شود.

مرحله ۶: ایجاد کلید خصوصی (بردار کلید نهایی):

Kv = 1, if KIV[i] > mean (KIV), else 0 (6)

اگر چه دو اثر انگشت مشابه نیستند، شانس وجود داشتن تعداد رگه ها برابر با تعداد حفره ها است. از این رو ماتریس$N \times N$ استفاده می شود که به طور دقیق رگه و حفره ها را در قالب الگوی بایت با توجه به تصویر اسکن شده ذخیره می کند. این به طور واضح اثر انگشت فردی را شناسایی می کند؛ زیرا داده ها در فرم ماتریس الگوهای مختلفی از مجموعه داده ها را دارند[5,15].

**شکل۵. روند تولید کلید**



از این رو کلید عمومی براساس مجموعه داده‌ای که در زیر نشان داده شده، محاسبه می شود:

فرضیه ها:

d → Aij تعداد کل یک های شیارها در زیرماتریس

e → Aij تعداد کل صفرهای رگه ها در زیرماتریس

i,j → 1, 2.....Np

$s = (d - e)$ (7)

$Pb = Kv * (mod(s)) * e$ (8)

e → بردار کلید عمومی

بنابراین کلید تولید شده با استفاده از الگوریتم بالا هر دو کلید عمومی و خصوصی را از نقاط مینیاتور اثر انگشت فرد ایجاد می کند. علاوه بر این، یک روش شبیه به الگوریتم RSA است که می تواند از جفت کلید اصلی تولید شده به جای رویکرد کاملا سنتی بر اساس الگوریتم برای محاسبه جفت کلید استفاده شود. بر اساس نتایج تجربی، ممکن است به این نکته اشاره شود که مهاجم، در صورت وجود یک سیستم رمزنگاری بیومتریک، قادر نخواهد بود بدون داشتن دانش کاملی از الگوریتم تولید کلید و اثر انگشت هر دو فرستنده و گیرنده یک کلید مشابه و جعلی تولید کند[۱۰].

## 7. نتایج

عملیات زمان در ثانیه که برای الگوریتم پیشنهاد شده در این‌جا به صورت زیر است:

- استخراج ویژگی از قالب بیومتریک حدود ۰,۰۵ ثانیه طول کشید.
- ولید یک الگو از بیومتریک استخراج شده ۰,۰۰۲ ثانیه انجام شد.
- رمزگذاری و رمزگشایی الگو به یک تابع که برای تولید کلید استفاده می‌شود، ۰,۱۵ ثانیه است.
- رمزنگاری عمومی و تولید کلید خصوصی ۰,۰۰۲ ثانیه صورت گرفت
- در نتیجه کل زمان مورد نیاز برای عملکرد کل ۰,۲۰۴ ثانیه صورت گرفت

## 8. آثار آینده

افزایش نیاز به انتقال امن بر روی کانال‌های ناامن، استفاده واقعی از رمزنگاری بیومتریک یا ادغام بیومتریک به سیستم‌های رمزنگاری سنتی بسیار مهم شده است. استفاده از چنین سیستمی که ترکیبی از بیومتریک‌ها و الگوریتم‌های رمزنگاری است، امنیت و حفظ حریم خصوصی در سیستم‌های سنتی را بسیار بهبود می‌بخشد. بیومتریک نرم با استفاده از ویژگی‌های رفتاری یک کاربر است که توسط مهاجمان قابل تکرار نیست[۵]. پیشرفت‌های آینده چنین رمزنگاری بیومتریک تمرکز بر توسعه اقتصادی سیستم است که امنیت را در هر شبکه یا رسانه ارتباطی تضمین می‌کند.

## ۹. نتیجه گیری

سیستم رمزنگاری بیومتریک در این مقاله بسیار قدرتمند است و یک رویکرد تضمین امنیت برای رمزگذاری و رمزگشایی بهتر فراهم می کند که با استفاده از یک کلید جفت تولید شده از طریق برداشت اثر انگشت ارائه شده است.

طرح رمزگذاری که ممکن است بیشتر مورد استفاده قرار گیرد به دلیل شباهت های کاربردی جفت کلید به رمزگذاری و رمزگشایی می تواند الگوریتم رمزنگاری RSA باشد[۶،۱۴]. منحصر به فرد بودن سیستم پیشنهادی، نهفته در تمایز کلیدهای تولید شده است که کاملا بر اساس این واقعیت است که صفات بیومتریک انسان به طور جداگانه متمایز هستند و در نتیجه یک رویکرد بسیار بهتر برای تأمین امنیت پیغام انتقال داده شده از یک انتقال غیرمجاز یا قابل دسترس را فراهم می کند.

## 10. مراجع

[1]. Chandra Sayani, Paul Sayan, Saha Bidyutmala, Mitra Sourish - Generate an Encryption Key by using Biometric Cryptosystems to secure transferring of Data over a Network. IOSR Journal of Computer Engineering.

[2]. Michael T Simpson. Hands-on ethical hacking and network security. India: Cengage Learning Publications. 2012.

[3]. Cryptography in VB.NET. Date accessed: 10/09/2015: Available from: http://www.c-sharpcorner.com/cryptography-in-VB-Net-part-1

[4]. Encryption key generation. Date accessed: 05/08/2015: Available from: http://www.slidesearch.org/slide/ d01211622

[5]. Biometric Cryptosystem. Date accessed: 12/08/2015: Available from: http://www.academia.edu/4814389/D01211622

[6]. Barman Subhas, Samanta Debasis and Chattopadhyay Samiran. Fingerprint-based crypto-biometric system for network security EURASIP. Journal on Information Security. 2015 April; Doi: 10.1186/s13635-015-0020-1.

[7]. Processing Standards Publication: Announcing the ADVANCED ENCRYPTION STANDARD (AES) – Federal Information. 2001 November 26; 197.

[8]. Soutar Colin, Roberge Danny, Stoianov Alex, Gilroy Rene and Vijaya Kumar BVK. Biometric Encryption™. McGraw-Hill publications: In: ICSA Guide to Cryptography. 1999; Ch-22.

[9]. Mahalakshmi U, Shankar Sriram VS. An ECC Based Multibiometric System for Enhancing Security. Indian Journal of Science and Technology. 2013 Apr; 6(4). Doi: 10.17485/ ijst/2013/v6i4/31857.

[10]. Fingerprint-based crypto-biometric system. Date accessed: 06/08/2015: Available from: http://www.jis.eurasipjournals. com/content/2015/1/3

[11]. Nagati Khaled. LAP Lambert Academic Publication: Contribution to the Solution of Fingerprint Identification Problem: 2012 April.

[12]. Understanding Biometrics. Date accessed: 12/09/2015: Available from: http://www.griaulebiometrics.com/en-us/book/understanding-biometrics/types/feature-extractio/ minutiae

[13]. Ratha NK, Chikkerur S, Connell JH, Bolle RM. Generating Cancellable Fingerprint Templates. IEEE Trans. Pattern Anal. Mach. Intell. 2007; 29(4):561–72.

[14]. Balakumar P and Venkatesan R. Secure Biometric Key Generation Scheme for Cryptography. International Journal on Computer Science and Engineering. 2010; 02(06):199295.
[15]. TCP/IP tutorial. Date accessed: 07/10/2015: Available from:
http://www.yaldex.com/tcp_ip/0672325659_ch20lev1sec1. html
[16]. Fingerprint Verification Competition FVC2002. [Online] Available from:
http://bias.csr.unibo.it/fvc2002