نشریه علمی «علوم و فناوری‌های پدافند نوین»
سال دوازدهم، شماره ۱، بهار ۱۴۰۰؛ ص ۱۱۹- ۱۰۷

علمی- پژوهشی

بهبود امنیت پایگاه داده سیستم بیومتریک عنبیه

سمیرا نجف‌زاده کشتلی[۱]، علی آقاگل‌زاده[۲*]، سید جواد کاظمی‌تبار[۳]

۱- دانشجوی کارشناسی‌ارشد، ۲- استاد، و ۳- استادیار، دانشگاه صنعتی نوشیروانی بابل، بابل، ایران

(دریافت: ۱۳۹۹/۰۸/۰۶، پذیرش: ۱۳۹۹/۱۲/۱۲)

چکیده

امروزه برای شناسایی هویت افراد از ویژگی‌های منحصربه‌فرد افراد استفاده می‌شود. این ویژگی‌ها بیومتریک نام دارند و از پرکاربردترین آن‌ها شامل اثرانگشت، کف دست و چهره است. یکی دیگر از مهم‌ترین و پرکاربردترین بیومتریک‌ها، عنبیه می‌باشد. پژوهش‌های انجام شده در این مقاله شامل طراحی یک سیستم شناسایی جدید بر مبنای افزایش امنیت در پایگاه داده عنبیه چشم است. در این مقاله الگوریتم جدیدی برای افزایش امنیت در پایگاه داده عنبیه چشم ارائه می‌شود که در آن از الگوریتم رمزنگاری دیداری و رمزنگاری RSA استفاده می‌شود. الگوهای استخراج‌شده از عنبیه چشم با الگوریتم‌های رمزنگاری دیداری و RSA به‌صورت توأم رمز می‌شوند تا امنیت آن‌ها در پایگاه داده تضمین شود. در این مقاله از بانک تصویر CASIA-v1 استفاده شده است که مقدار EER آن بعد از اعمال روش‌های رمزنگاری تقریباً ۰/۰۱ است که مقدار قابل‌قبولی است. علاوه‌براین، نتایج شبیه‌سازی نشان می‌دهد که الگوریتم‌ها و ماسک‌های به‌کارگرفته‌شده در سامانه پیشنهادی در مقابل نویزهای فلفل‌نمکی، گوسی‌سفید و فیلترمیانگین نسبت به سامانه‌های دیگر عملکرد بهتری خواهند داشت.

کلید واژه‌ها: تشخیص هویت، بیومتریک عنبیه، رمزنگاری، رمزنگاری دیداری، RSA، داگمن

Security Improvement of the Iris Biometric System Database

S. Najafzadeh Keshteli[1], A. Aghagolzadeh[2], S. J. Kazemitabar[3]

Babol Noshirvani University of Technology

(Received: 27/10/2020; Accepted: 02/03/2021)

Abstract

Nowadays, unique identifiers are used to authenticate individuals. These identifiers are called biometrics with iris being one of the most popular ones. Research performed in this paper consist of designing a new identification system based on improved security in iris database. In this paper, we propose an iris template protection method based on Visual Cryptography (VC) and RSA. For iris template protection, the binary iris template is divided into two shares using VC, where one share is stored in the database and the other is kept with the user on a smart card. In order to provide additional security, the share that is stored in the database is encrypted with RSA encryption. In the next step the patterns obtained from each image are compared with the patterns in the database and, by defining a threshold, the identification procedure is carried out. In this paper, the CASIA - v1 image bank has been used. The EER value after encryption is approximately 0.01. We then expose the system to different noises such as salt and pepper, white Gaussian noise and mean filt.r. After applying the noises, we haveit is observed that the system has shows been better performance compared to the than other systems which we have investigated.

Keywords: Biometric, Iris, Visual Cryptography, RSA, Smart Card, Security

* Corresponding Author E-mail: aghagol@nit.ac.ir

۱- مقدمه

شناسایی هویت از گذشته تا به امروز موردتوجه تمدن بشر بوده است، در چند سال گذشته برای شناسایی هویت از کلمه عبور و یا کارت شناسایی استفاده می‌شد که سرعت و اعتماد و کارایی خود را داشتند اما این روش از شناسایی هویت با مشکلاتی همراه بوده است. ازاین‌رو امروزه علم بیومتریک به‌عنوان یک موضوع مهم در شناسایی هویت موردتوجه محققان قرارگرفته است [۱]. با پیدایش فناوری‌های جدید مانند کامپیوتر، پردازش تصویر و هوش مصنوعی بر حجم داده‌های دیجیتالی و سرعت انتقال آن‌ها افزوده‌شده است. بنابراین ذخیره‌سازی و امنیت آن‌ها نیز به راهکارهای جدید و مطمئن‌تر نیاز دارد [۲]. پیشرفت درزمینه فناوری اطلاعات و بینایی ماشین همچنین نیاز روزافزون به امنیت باعث شده است که پیشرفت‌های سریعی درزمینه تشخیص هویت افراد به‌صورت هوشمند و بر اساس بیومتریک به دست آید. اولین بار چشم‌پزشکی به نام Frank Burch در سال ۱۹۳۶ پیشنهاد تشخیص هویت از طریق الگوی عنبیه را بیان کرد. در سال ۱۹۸۵ دو چشم‌پزشک به نام‌های Aran Safir و Leonarad Flom بیان کردند که عنبیه دو شخص مختلف کاملاً متفاوت هستند. در سال ۱۹۹۳ داگمن اولین الگوریتم موفق تشخیص عنبیه را ارائه داد. بررسی‌ها نشان می‌دهند که بیومتریک عنبیه به‌عنوان برترین بیومتریک شناخته‌شده است که ازجمله دلایل آن می‌توان به دقت بالا، تشخیص واقعی و زنده‌بودن عنبیه با وجود تغییر اندازه مردمک در برابر تغییر نور، اختلاف عنبیه در دوقلوها و حتی عنبیه‌های یک شخص، عدم‌تغییر با وجود داشتن لنز، عینک و حتی عمل جراحی اشاره کرد. تشکیل عنبیه از سومین ماه زندگی جنینی شروع می‌شود. چگونگی تشکیل بافت عنبیه به‌صورت تصادفی بوده و ربطی به عامل‌های ژنتیکی ندارند. تنها عامل موجود در عنبیه که به عوامل ژنتیکی بستگی دارد سلول‌های رنگ‌دانه‌های می‌باشند که تعیین‌کننده رنگ عنبیه خواهند بود. باتوجه به اینکه بافت عنبیه به عوامل ژنتیکی بستگی ندارد، دو چشم یک نفر کاملاً دارای بافت‌های جدا از هم در عنبیه بوده و همچنین بافت چشم‌های دوقلوها باهم متفاوت‌اند؛ بنابراین عنبیه از هر فرد به فرد دیگر متفاوت است و به همین جهت گفته می‌شود عنبیه از اثرانگشت منحصربه‌فردتر است. برخی از مزایای عنبیه برای شناسایی افراد را می‌توان به‌طور خلاصه به‌صورت زیر بیان کرد:

- منحصربه‌فرد بودن به دلیل پیچیدگی ترکیبی.
- تغییر اندازه مردمک طبیعی بودن فیزیولوژی را تائید می‌نماید.
- دارای ساختار شکل‌گرفته قبل از تولد (ماه هفتم از دوران بارداری).
- الگوهای عنبیه قابلیت نفوذ ژنتیکی محدود دارند.
- الگوها در طول دوران زندگی پایدار می‌باشند.
- به رمز درآوردن و تصمیم‌گیری روی تصاویر عنبیه مشکل نیست.

۱-۱- امنیت در پایگاه‌داده عنبیه چشم

امروزه با توجه به اهمیت دست‌یابی به اطلاعات حاوی هویت اشخاص و کاربردهای بی‌شمار آن‌ها، حفاظت از پایگاه‌های داده بیومتریک در مقابله با حملات مخرب از مهم‌ترین چالش‌های پیش روی این نوع پایگاه‌ها است. یکی از مؤثرترین روش‌ها برای حفاظت از پایگاه‌های داده، استفاده از رمزنگاری اطلاعات بیومتریک موجود در پایگاه می‌باشد. در رمزنگاری هدف ساختن طرح‌ها یا پروتکل‌هایی است که بتوان با کمک آن‌ها حتی در حضور دشمن نیز کارهای خاصی را انجام داد. یک هدف اساسی در رمزنگاری این است که به افراد این امکان را بدهند که روی یک کانال ناامن با حفظ حریم خصوصی و اصالت داده‌هایشان به‌صورت کاملاً امن باهم ارتباط برقرار کنند. روش‌های مختلفی برای طبقه‌بندی الگوریتم‌های رمزنگاری وجود دارد، متداول‌ترین آن‌ها، روش‌های رمزنگاری متقارن و نامتقارن می‌باشند. رمزنگاری متقارن، رمزنگاری کلید مخفی و کلید مشترک نیز نامیده می‌شود. در این رمزنگاری فرستنده و گیرنده از یک کلید مشترک برای رمزنگاری و رمزگشایی استفاده می‌کنند. این الگوریتم توان محاسباتی بالایی ندارد و دارای سرعت بالایی است. معمولاً رمزنگاری متقارن به دو دسته‌ی رمزنگاری بلوکی و رمزنگاری جریانی تقسیم می‌شوند. در رمزنگاری بلوکی کل داده به بلوک‌های n تایی تقسیم می‌شود و سپس برای هر بلوک رمز کلید تهیه می‌شود و رمزنگاری برای هر بلوک به‌صورت جداگانه انجام می‌شود. این در حالی است که در رمزنگاری جریانی، داده‌ها به بیت‌های منفردی تبدیل می‌شوند و الگوریتم برای هر بیت به‌صورت پی‌درپی انجام می‌شود [۳]. الگوریتم استاندارد رمزنگاری پیشرفته[1] که در سال ۲۰۰۱ توسط NIST ارائه‌شده است، یک نمونه بسیار مهم در حوزه رمزنگاری متقارن می‌باشد. الگوریتم AES می‌تواند از ترکیب اطلاعات ۱۲۸ بیتی و کلیدهای ۱۲۸، ۱۹۲ و ۲۵۶ بیتی پشتیبانی کند. این الگوریتم را به‌عنوان AES-128، AES-129 و AES-256 می‌شناسند. در رمزنگاری نامتقارن دو کلید برای رمزنگاری و رمزگشایی استفاده می‌شود، کلید عمومی برای رمزنگاری و کلید خصوصی برای رمزگشایی است [۴]. RSA یک الگوریتم کلید عمومی است که در سال ۱۹۹۷ توسط Rivest-Shamir-Adleman طراحی‌شده است. این الگوریتم در پروتکل‌های امنیتی مانند امنیت داده‌های IP، امنیت اطلاعات حمل‌ونقل و امنیت ایمیل استفاده می‌شود. این الگوریتم یک الگوریتم نامتقارن است که کلید عمومی را می‌توان به اشتراک گذاشت اما کلید خصوصی باید مخفی بماند [۵ و ۶].

[1] Advance Encryption Standard (AES)

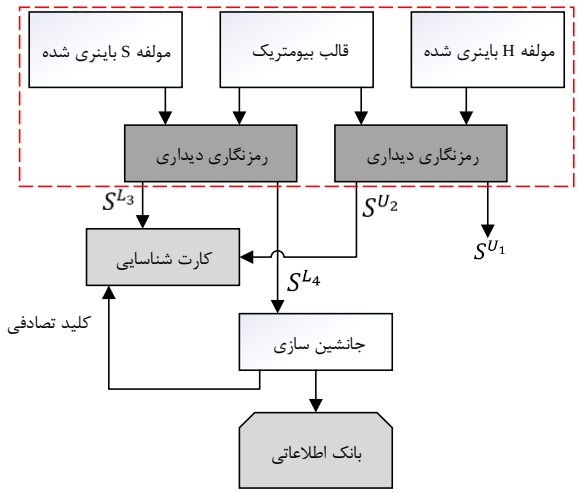
۱-۲- رمزنگاری دیداری در پایگاه‌داده عنبیه چشم

در رمزنگاری دیداری یک تصویر به سهم‌هایی تبدیل (تقسیم) می‌شود که هیچ یک از سهم‌ها، اطلاعاتی در مورد تصویر ابتدایی بیان نمی‌کنند و تنها با ترکیب آن‌ها تصویر آشکار می‌شود. رمزنگاری دیداری اولین باز توسط Naor و Shamir در سال ۱۹۹۴ مطرح شد [۷]. آن‌ها جهت تقسیم‌بندی پیکسل p در تصویر باینری I مانند شکل (۱) عمل کرده‌اند. در این شکل هر پیکسل از تصویر باینری به اندازه $(M \times N)$ به دو زیر پیکسل SR1 و SR2 تقسیم می‌شوند برای بازسازی پیکسل اصلی دو زیر سهم SR1 و SR2 باید با یکدیگر ترکیب شوند.

Pixel	Shares		*SR1* (OR) *SR2*	*SR1* (XOR) *SR2*
	SR1	*SR2*		
White				
Black				

شکل ۱. رمزنگاری‌دیداری [۸] .

هیچ‌کدام از سهم‌ها به‌تنهایی اطلاعاتی، در مورد سیاه یا سفید بودن پیکسل ارائه نمی‌دهند. به هنگام ترکیب سهم‌ها، اگر پیکسل اولیه سیاه باشد، پیکسل ترکیبی سیاه خواهد بود اما اگر پیکسل اولیه سفید باشد، نتیجه به‌صورت نصف سیاه و نصف سفید خواهد شد. اگرچه روش رمزنگاری دیداری یک روش ساده و قدرتمند برای محافظت است اما با این روش اندازه تصویر بزرگ‌تر می‌شود (به‌اندازه $M \times 2N$) و باعث کاهش تباین[1] تصویر می‌شود، اما اگر در ایجاد پیکسل اولیه به‌جای عملگر OR از XOR استفاده شود ۵۰ درصد از مشکل کاهش تباین حل می‌شود. بااین‌حال رمزنگاری دیداری ممکن است ظرفیت سیستم‌های بیومتریک در مقیاس بزرگ را محدود کند چون اندازه تصویر دو برابر می‌شود و باعث پیچیدگی محاسباتی می‌شود. همچنین این نوع از رمزنگاری نمی‌تواند حفاظت کامل را فراهم کند زیرا برای عمل مقایسه برای تشخیص عنبیه باید رمزگشایی شود که این کار خود می‌تواند باعث ایجاد خطا شود [۸]. برای رمزنگاری دیداری پیشنهادی در [۹] از دو تصویر استفاده می‌شود. مزیت این روش این است که دو تصویر به‌طور هم‌زمان رمزنگاری می‌شود. اگر به یک تصویر برای رمزنگاری نیاز داشته باشیم تصویر دوم را به‌صورت تصادفی انتخاب می‌کنیم اما باید به این نکته توجه کرد که اندازه تصویر انتخاب‌شده باید با تصویر اصلی یکسان باشد. هر تصویر ورودی باینری به دو قسمت در جهت عمودی تقسیم می‌شود، که هر دو قسمت اندازه یکسانی دارند. قسمت بالایی را با نماد U و قسمت پایینی را با نماد L مشخص می‌کنند (شکل ۲). پس از این‌که الگو عنبیه به دست آمد، از مؤلفه‌های رنگی تصویر خام، برای رمزنگاری دیداری استفاده می‌شود. ابتدا در فضای رنگی HSV، مؤلفه H تصویر نرمال‌شده‌ی عنبیه به دست می‌آید و وضوح آن بهبود داده می‌شود. تصویر حاصل با استفاده از آستانه گذاری اتسو باینری می‌شود.



شکل ۲. الگوریتم رمزنگاری‌دیداری و جانشین‌سازی [۹].

با در نظر گرفتن الگوی بیومتریک به‌عنوان تصویر اول و تصویر به دست‌آمده از تصویر H، رمزنگاری دیداری ایجاد می‌شود. تنها از دونیمه بالایی SU1 و SU2 استفاده می‌شود. نیمه یک سهم در پایگاه داده‌ها و نیمه سهم دیگر در کارت‌شناسایی ذخیره می‌شود. با ترکیب این دو نیم‌سهم نصفه بالایی الگوی بیومتریک می‌تواند بازیابی شود. هم‌زمان با این عملیات، مؤلفه S تصویر نرمال‌شده‌ی عنبیه، توسط الگوریتم اتسو باینری شده و همراه با الگوی عنبیه با رمزنگاری، دو سهم جدید ایجاد می‌کند. SL3, SL4 از دو سهم حاصل نیمه پایینی آن‌ها ایجاد می‌شود. یک نیم‌سهم در پایگاه داده‌ها و دیگری در کارت‌شناسایی ذخیره می‌شود. با ترکیب این دو نیم‌سهم نیمه‌ی پایینی الگوی بیومتریک ایجاد می‌شود.

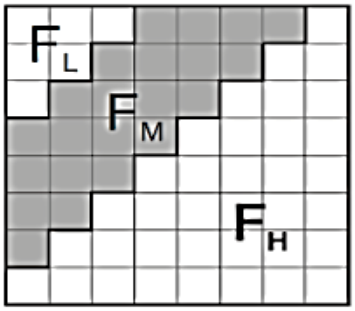
در [۱۰]، مشابه با [۹] برای افزایش امنیت در تصویر عنبیه، به‌موازات بهره بردن از رمزنگاری دیداری از نهان‌نگاری استفاده می‌شود. در روش پیشنهادی این مقاله، نویسندگان از تبدیل DCT برای نهان‌نگاری استفاده می‌کنند، تبدیل فرکانسی در حوزه DCT یک تصویر را به ۳ باند فرکانسی مختلف تقسیم می‌کند.

- F_L: فرکانس باند پایین این فرکانس دارای قسمت‌های دیداری مهم است.
- F_H: فرکانس باند بالا در معرض حذف اطلاعات از طریق فشرده‌سازی است.
- F_M: فرکانس باند میانی است که برای نهان‌نگاری از این باند فرکانسی استفاده می‌شود.

برای باند فرکانسی میانی دو مکان از بلوک $DCT_{U1,V1}$ و $DCT_{U2,V2}$ به‌عنوان منطقه‌ای برای مقایسه انتخاب می‌شوند.

[1] Conterast

برای نهان‌نگاری کردن از یک متن استفاده می‌کنند که اطلاعات این متن در تصویر عنبیه پنهان می‌شوند. تصویر متنی را با W نشان می‌دهند و شامل اطلاعاتی مانند؛ نام کاربر، شناسه و تاریخ تولد کاربر است، ابتدا این تصویر متنی باید به یک تصویر باینری تبدیل شود، در نهایت به یک آرایه یک‌بعدی از صفر و یک تبدیل می‌شود. سپس تصویر عنبیه را به بلوک‌های ۸ × ۸ تبدیل می‌کنند و هر بیت از تصویر متنی باینری شده را در یک بلوک قرار می‌دهند. در شکل (۳) یک تصویر بلوک‌بندی شده به همراه تقسیم‌بندی باند فرکانسی نشان داده‌شده است.



شکل ۳. باندهای فرکانسی مختلف بلوک‌های یک تصویر [۱۰].

اگر بیتی که می‌خواهد کدگذاری شود یک باشد از روش $DCT_{U1,V1} \geq DCT_{U2,V2}$، ولی اگر بیتی که می‌خواهد کدگذاری شود صفر باشد از روش $DCT_{U1,V1} < DCT_{U2,V2}$ استفاده می‌شود. برای کدگشایی هم اگر ضریب‌ها به‌صورت $DCT_{U1,V1} \geq DCT_{U2,V2}$ باشد بیت مورد نظر یک است و اگر ضریب‌ها به‌صورت $DCT_{U1,V1} < DCT_{U2,V2}$ باشد بیت موردنظر صفر است.

در [۱۱]، برای حفاظت از داده‌های عنبیه چشم، الگوی برداری عنبیه بر اساس رتبه‌بندی ارائه‌شده است. در مرحله شناسایی شخص برای محاسبه فاصله بین دو الگوی عنبیه (الگوی ذخیره‌شده در پایگاه داده و الگوی کاربر) در هنگام ورود به برنامه کاربردی یا سامانه r و r' از رابطه ۱ استفاده می‌کنند [۱۱]:

$$Dis(r,r') = \sum_{i=1}^{n} |r_i - r'_i| \quad (1)$$

بعد از این‌که الگوی جدید عنبیه در پایگاه داده‌ها ثبت شد، نویسندگان استفاده از روش جابه‌جایی و ماسک گذاری معیارهای ارزیابی برای شناسایی شخص را بهبود می‌دهند. علاوه بر این در این مقاله، روش جابه‌جایی پیشنهادی نویسندگان، جابه‌جایی داده‌های عنبیه به‌صورت دایره‌ای است.

اما هدفی که در این مقاله دنبال می‌شود، ایجاد امنیت در پایگاه داده عنبیه چشم است. با بررسی انجام‌شده تاکنون، به این نتیجه می‌توان رسید که الگوریتم رمزنگاری دیداری برای ایجاد رمزنگاری مناسب است زیرا می‌توان نصف اطلاعات یک الگوی عنبیه را در پایگاه داده‌ها و نصف دیگر را در کارت‌شناسایی کاربر ذخیره کرد. در این صورت اگر حمله‌ای به پایگاه داده وارد شود و فرد مهاجم به اطلاعات عنبیه دسترسی پیدا کند فقط به نیمی از اطلاعات عنبیه دسترسی دارد و نمی‌تواند به اهداف خود که سوءاستفاده از کد عنبیه و ورود غیرمجاز است برسد. اما باید دانست این نوع از رمزنگاری نمی‌تواند حفاظت کامل را فراهم کند زیرا برای عمل مقایسه برای تشخیص عنبیه باید رمزگشایی شود که این عمل خود می‌تواند در معرض خطا باشد. برای ایجاد امنیت بیشتر می‌توان از الگوریتم‌های دیگر به‌طور موازی به همراه رمزنگاری دیداری استفاده کرد. ازآنجایی‌که طول کد عنبیه بزرگ است الگوریتم رمزنگاری RSA مناسب‌تر است زیرا طول بلوک آن برای رمزنگاری بزرگ‌تر است و کدهای عنبیه را در مراحل کمتری کد می‌کند بنابراین، پیچیدگی محاسباتی کمتری دارد علاوه بر آن امن‌تر نیز هست زیرا دارای دو کلید خصوصی و عمومی است و در صورت حمله به کلید عمومی نمی‌توان به کلید خصوصی دسترسی داشت و درنتیجه احتمال حمله به سیستم بیومتریک کم‌تر است.

۲- روش پیشنهادی

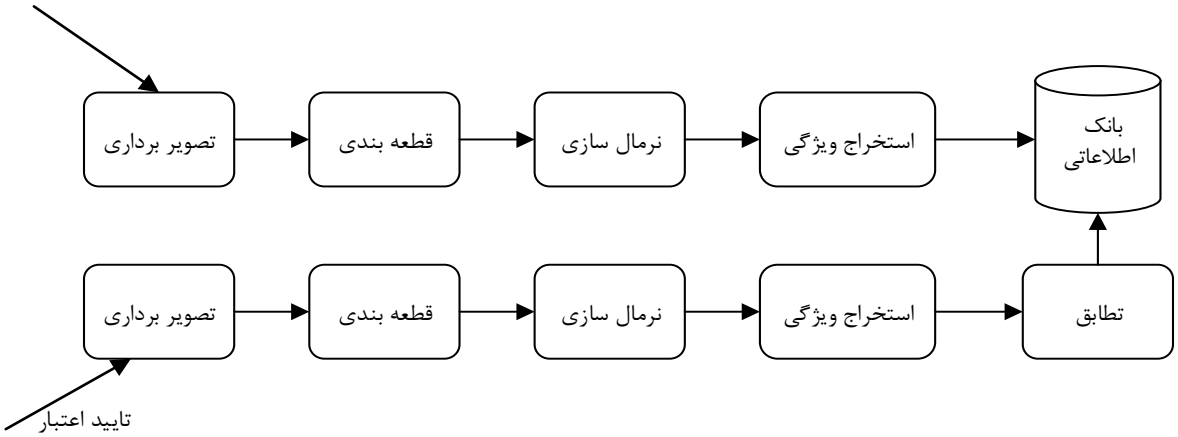
روش پیشنهادی برای ایجاد امنیت در داده‌های بیومتریک-عنبیه در دو بخش مجزا انجام می‌شود (شکل ۴):

۱. تولید کد عنبیه

۲. ایجاد امنیت برای الگو عنبیه ذخیره‌شده در پایگاه داده‌ها

۲-۱- تولید کد عنبیه

نخستین فاز در سامانه پیشنهادی، تولید کد عنبیه است. همان‌طور که در شکل (۴) مشاهده می‌شود، فاز تولید کد عنبیه از چندین بخش تشکیل می‌شود. نخستین گام تصویربرداری بوده که معمولاً توسط یک دوربین تک‌رنگ مادون‌قرمز (۷۰۰ nm - ۹۰۰) که مجهز به حسگر CCD است گرفته می‌شود. معمولاً فاصله دوربین تا چشم باید چیزی در حدود ۴۵ سانتی‌متر باشد. گام‌های بعدی قطعه‌بندی نرمال‌سازی و استخراج ویژگی می‌باشند، که در ادامه، چگونگی پیاده‌سازی هر یک از این بخش‌ها مورد بحث و بررسی قرار می‌گیرد.



شکل ۴. سامانه تشخیص هویت بیومتریک

قطعه‌بندی

از آنجایی‌که قسمت‌های بالایی و پایینی عنبیه به‌وسیله پلک‌های بالا و پایین پوشیده شده است، قسمتی از داده‌ها را از دست می‌دهیم و به‌جای آن داده‌های دیگری به دست می‌آیند. بنا بر شرایط مختلف، مقدار این پوشش و درنتیجه مقدار داده‌های ناخواسته که وارد سیستم می‌شود تغییر می‌کند، لازم است که نقاط مربوط به این مخرب‌ها شناسایی و حذف شوند. پیدا کردن ناحیه پلک‌ها علاوه بر مشخص کردن تخریب‌های ناشی از آن‌ها، پیدا کردن مرز بیرونی عنبیه را نیز آسان می‌کند، زیرا قسمت زیادی از نقطه‌های لبه ناخواسته مربوط به پلک‌ها می‌شوند. برای به دست آوردن مشخصه هر عنبیه بعد از تصویربرداری باید قسمت‌های مربوط به عنبیه استخراج شود. این روش با استفاده از پردازش تصویر انجام می‌شود. برای قطعه‌بندی تصویر روش‌های مختلفی وجود دارد در این مقاله برای قطعه‌بندی از روش داگمن استفاده می‌شود که در ادامه به آن پرداخته می‌شود.

روش داگمن رایج‌ترین روش به رسمیت شناخته برای تشخیص عنبیه است که در سال ۱۹۹۳ توسط داگمن ارائه‌شده است. و نیز اولین روشی است که به‌طور مؤثر در سیستم بیومتریک اجرا شد. به‌منظور افزایش تباین تصویر پیش از فرآیند قطعه‌بندی باید تصویر را باینری کرد زیرا مبنای کار تشخیص عنبیه و مردمک چشم به تعریف حد آستانه بستگی دارد [۱۲]. در این مقاله از قطعه‌بندی به روش انتگرال- دیفرانسیل با جستجوی سهموی به‌منظور پیدا کردن ناحیه‌های دایروی عنبیه و مردمک استفاده می‌شود، که در آن پلک‌های بالایی و پایینی را توسط دو کمان جدا می‌کند. عملگر انتگرال – دیفرانسیل به‌صورت زیر است [۱۳]:

$$Max(r,xc,yc)\left|G\,\sigma(r)*\frac{\partial}{\partial r}\oint_{(r.x0.y0)}\frac{I(x.y)}{2\pi r}\,ds\right| \qquad (۲)$$

مهم‌ترین و پیچیده‌ترین قسمت مرحله قطعه‌بندی پیدا کردن مرز خارجی عنبیه (مرز بین عنبیه و صلبیه) است، زیرا مرز کاملاً مشخصی در این ناحیه وجود ندارد و مرز موجود به‌صورت پخش‌شده است و این‌که مرزهای دیگری در تصویر چشم وجود دارند که در آن‌ها تغییرات شدت نور بسیار زیاد است درنتیجه هر روشی که بتواند مرز ضعیف ناحیه خارجی عنبیه را تشخیص دهد مطمئناً این لبه‌ها نیز در آن ظاهر خواهند شد و چون هم تعداد نقاطِ لبه ناخواسته زیاد است و هم دارای شکل‌های منظم و مشابه خود مرز خارجی عنبیه هستند. بنابراین، در مرحله جداسازی مرز خارجی عنبیه باید روشی ارائه شود که بتواند نقاط لبه ناخواسته را تشخیص داده و آن‌ها را حذف کند. ازآنجایی‌که موفقیت مراحل بعدی سامانه تشخیص هویت بستگی زیادی به این مرحله دارد لذا در به دست آوردن نتایج این مرحله باید دقت زیادی شود.

اساس روش پیاده شده در مقاله استفاده از روش لبه‌یاب Canny است، چون لبه‌یاب Canny یک لبه‌یاب قوی است و مرزهای زیادی را در تصویر پیدا می‌کند، در مرحله بعد نقاط لبه اضافی را حتی‌الامکان حذف می‌کنیم.

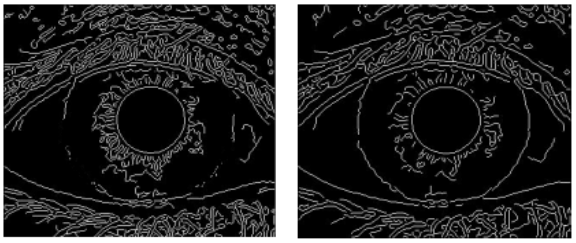
منابع اصلی مخرب‌ها در این روش عبارت‌اند از:

- نقاط لبه مربوط به مرزهای مردمک
- نقاط لبه مربوط به پلک بالا
- نقاط لبه مربوط به پلک پایین
- نقاط لبه مربوط به مژه‌ها
- نقاط لبه مربوط به طرح‌های داخلی ناحیه عنبیه
- نقاط لبه مربوط به سایه‌های موجود در تصویر به‌خصوص در گوشه‌های صلبیه

برای پیدا کردن مرز خارجی عنبیه باید همه نقاط لبه مخرب نام‌برده را حذف کنیم. ولی مشکل اصلی که هنوز حل‌نشده مسئله‌ی نبودن لبه مشخص که دارای تغییرات شدید در شدت نور

باشد در مرز بیرونی عنبیه و یا به عبارتی ضعیف بودن مرز خارجی عنبیه است که حتی لبه‌یابی مانند Canny هم قادر به تشخیص آن‌ها نیست. برای حل این مشکل ابتدا با استفاده از ماسک لاپلاسین مقادیر لبه‌ها را به‌دست می‌آوریم و سپس این مقادیر را از تصویر اصلی کم می‌کنیم، به‌این‌ترتیب نقاط لبه‌ای که تغییرات شدت نور در آن‌ها زیاد بود ضعیف می‌شوند، البته با این کار نقاط لبه مربوط به مرز خارجی عنبیه نیز ضعیف می‌شوند ولی چون تغییرات شدت نور و درنتیجه مقدار حاصل از ماسک لاپلاسی در آن‌ها کم است ضعف این نقاط کم خواهد بود.

فایده استفاده از این روش این است که اگر لبه‌یاب Canny را بر روی آن اعمال کنیم، چون مرز قوی با تغییر شدت نور زیاد در آن وجود ندارد، در مرحله آستانه‌گذاری برای انتخاب نقاط لبه آستانه‌ی پایین‌تری انتخاب می‌شود و در نتیجه نقاط بیشتری از مرز ناحیه عنبیه آشکار می‌شوند. شکل (۵) نتایج اعمال لبه‌یاب Canny را روی تصویر اصلی و همچنین تصویر بهبودیافته توسط روش بالا را نشان می‌دهد، مشاهده می‌شود که در حالت دوم مرز بیرونی عنبیه بهتر مشخص‌شده است. پس از به‌دست آوردن تصویری که در آن، مرز عنبیه به‌خوبی مشخص‌شده است باید تخریب‌های به‌وجود آمده از موارد مطرح‌شده در بالا را حذف کنیم زیرا همان‌طور که در شکل (۵) مشاهده می‌شود هنوز تعداد نقاط ناخواسته زیادی به‌عنوان لبه انتخاب‌شده‌اند.

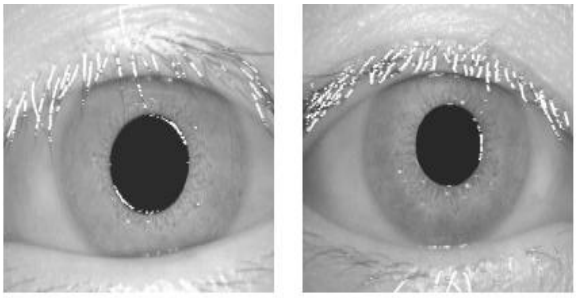


شکل ۵. اعمال لبه‌یاب Canny به تصویر چشم.

در قسمت‌های قبل توضیح داده شد که چگونه مرز داخلی عنبیه یا مرز بین عنبیه و مردمک به‌دست آورده می‌شود. حال می‌توان نقاط لبه مربوط به مرزهای مردمک را حذف کنیم. در قسمت‌های بیان‌شده مرزهای مربوط به ناحیه بین پلک‌های بالا و پایین و عنبیه را پیدا کرده بودیم درنتیجه می‌توانیم نویز ناشی از نقاط لبه مربوط به پلک بالا و پایین را حذف کنیم. نتایج این مرحله در شکل (۶) نشان داده شده است. ذکر این نکته ضروری است که منظور از نویز می‌تواند انعکاس نور، یا مشکل روشنایی محیطی باشد که برای تصویربرداری از عنبیه مورد استفاده قرار می‌گیرد. به‌علاوه در بسیاری از مواقع افرادی که عنبیه آنها مورد تصویربرداری قرار می‌گیرد همکاری لازم را به عمل نمی‌آورند و این مساله از کیفیت تصویر عنبیه می‌کاهد. در ادبیات تشخیص عنبیه از این مساله به‌عنوان نویز نام برده می‌شود [۱۴].

(الف) (ب)

شکل ۶. (الف) مرز پس از حذف لبه‌های مربوط به مردمک، (ب) پلک‌ها و مرزهای به‌دست‌آمده با استفاده از لبه‌یاب canny.



شکل ۷. تصویر اصلی که مژه‌ها در آن مشخص شده است.

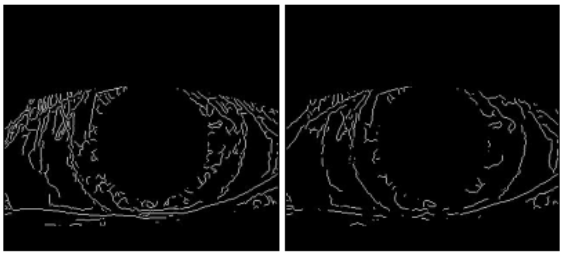
- حذف نویز ناشی از نقاط لبه مربوط به مژه‌ها

مژه‌ها معمولاً به شکل خط‌های باریک به ضخامت یک تا سه پیکسل هستند، روی یک ناحیه پس‌زمینه که معمولاً اختلاف زیادی بین این دو ناحیه (مژه و پس‌زمینه آن) وجود دارد، قرار دارند (شکل ۷). از این ویژگی مژه‌ها می‌توان برای شناسایی و حذف آن‌ها کمک گرفت. روش پیاده‌شده در این مقاله به این صورت است که مقدار شدت‌روشنایی هر تصویر را با شدت‌روشنایی چند پیکسل از هر دو طرف آن پیکسل مقایسه می‌کنیم و درصورتی‌که اختلاف زیادی بین آن‌ها بود آن نقطه را به‌عنوان یک پیکسل از مژه‌ها انتخاب می‌کنیم. تنها مشکل این روش در برخورد با مژه‌هایی است که خیلی به هم نزدیک هستند و در مورد آن مژه‌ها جواب نمی‌دهد که البته احتمال وقوع چنین حالتی خیلی کم است.

- حذف نویز ناشی از نقاط لبه مربوط به طرح‌های داخلی ناحیه عنبیه

در مورد طرح‌های داخلی ناحیه عنبیه، همان‌طور که در شکل (۸- ب) مشاهده می‌شود نقاط لبه مربوط به آن‌ها به‌صورت فشرده و در کنار هم هستند درحالی‌که نقاط مربوط به مرز خارجی عنبیه به‌صورت فشرده نیستند و در یک پنجره با طول محدود تعداد خیلی کمی از آن ها قرار می‌گیرد به‌علاوه این طرح‌ها فقط در نواحی نزدیک مرز داخلی عنبیه یا مرز مردمک قرار دارند و فاصله زیادی با مرز بیرونی عنبیه دارند. بنابراین، اگر یک پنجره با طول محدود را روی تصویر حرکت دهیم و هر جا که تعداد نقاط

بیشتر از یک حد آستانه داخل پنجره قرار داشتند، آن نقاط را از مجموعه نقاط کاندید برای لبه بودن حذف کنیم نویز ناشی از طرح‌های داخلی ناحیه عنبیه نیز حذف خواهد شد. نتایج این مرحله در شکل (۸- الف) نشان داده‌شده است.

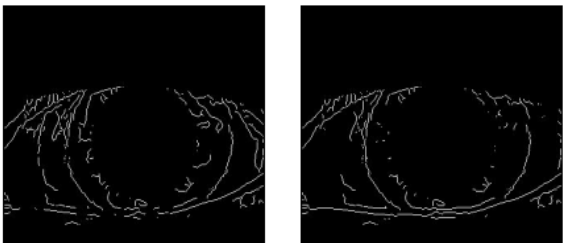


(الف) (ب)

شکل ۸. (الف) مرز به‌دست‌آمده از حذف طرح‌های داخلی عنبیه، (ب) مرز به‌دست‌آمده بعد از حذف نویز.

- حذف نویز ناشی از نقاط لبه مربوط به سایه‌های موجود در تصویر در گوشه‌های صلبیه

یکی از منابع مخرب در تصاویر عنبیه، تخریب به وجود آمده از سایه ی گوشه های چشم روی ناحیه صلبیه است. چون تغییرات شدت نور در آن‌ها مانند تغییرات شدت نور در مرز ناحیه عنبیه است با آستانه گذاری نمی‌توان آن‌ها را حذف کرد. از طرف دیگر چون مرزهای این نواحی معمولاً به شکل دایروی هستند و با شعاع و مرکزی نزدیک شعاع و مرکز عنبیه، با هیچ‌یک از روش‌های ارائه‌شده در قسمت‌های قبل نمی‌توان این تخریب را حذف کرد. نقاط لبه به‌وجود آمده ناشی از این نیز در شکل (۹-ب) نشان داده شده است برای حل این مشکل از تفاوت بین مرز خارجی عنبیه و مرز سایه استفاده می‌کنیم که هنگام حرکت از سمت مردمک به سمت بیرون، در مرز بین عنبیه و صلبیه شدت‌نور نقاط داخل ناحیه عنبیه کمتر (تیره‌تر) از شدت نور نقاط بیرون این ناحیه است درحالی‌که در مورد نقاط اطراف مرز سایه‌ها برعکس شدت نور نقاط داخل بیشتر از نقاط خارج مرز است. شکل (۹-الف) مرزهای به‌دست‌آمده پس از حذف لبه‌های مربوط به سایه‌های موجود در تصویر را نشان می دهد.



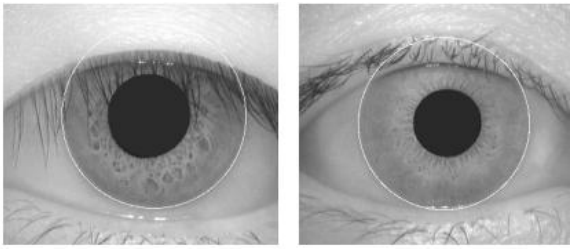
(الف) (ب)

شکل ۹. (الف) مرز به‌دست‌آمده پس از حذف لبه‌های مربوط به سایه‌های موجود در تصویر، (ب) مرز به‌دست‌آمده از بعد از حذف نویز در ناحیه عنبیه.

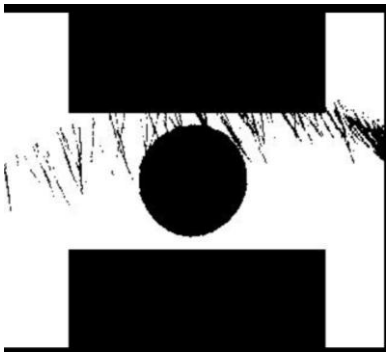
- به‌دست آوردن پارامترهای دایره‌ی بیرونی عنبیه

پس از بهبود کیفیت تصویر برای استخراج مرز بیرونی عنبیه و حذف کلیه عوامل مخرب تصویر، به مرحله پیدا کردن دایره بیرونی عنبیه می‌رسیم. در اینجا نیز همانند قسمت‌های پیشین از عملگر دیفرانسیل - انتگرال برای پیدا کردن پارامترهای دایره بیرونی استفاده می‌کنیم (شکل ۱۰). برای سرعت بخشیدن به عملیات این مرحله و با توجه به این‌که مراکز مردمک و عنبیه باوجود هم‌مرکز نبودن، به هم خیلی نزدیک هستند، ناحیه جستجو برای مرکز عنبیه را به یک پنجره دور مرکز مردمک انتخاب می‌کنیم.

در نهایت قسمت مربوط به نویزها (قسمت مردمک، پلک‌ها، مژه‌ها) را با تعریف یک حد آستانه، مقدار آن‌ها را برابر یک فرض می‌کنیم و مقدار قسمت‌های مربوط به عنبیه را صفر فرض می‌کنیم. همان‌طور که در شکل (۱۱) مشخص است قسمت فراتر از عنبیه نیز صفر فرض شده است اما چون در مراحل جداسازی مرز خارجی قسمت مربوط به این ناحیه حذف شده است مشکل ایجاد نمی‌کند.



شکل ۱۰. دایره بیرونی عنبیه برای چند تصویر مختلف.



شکل ۱۱. نویزهای چشم با مقدار صفر مشخص شده است.

نرمال‌سازی عنبیه چشم

در این مقاله برای نرمال کردن از مدل صفحه لاستیکی که توسط داگمن مطرح‌شده است استفاده می‌کنیم. نگاشت ناحیه عنبیه از مختصات کارتزین (x,y) به مدل نرمال‌شده قطبی غیر هم‌مرکز به‌صورت زیر است [۱۵]:

$$I\big(x(r,\theta),y(r,\theta)\big) \rightarrow I(r,\theta) \qquad (۳)$$

$$x(r,\theta) = (1-r)x_P(\theta) + rx_I(\theta) \qquad (۴)$$

$$y(r,\theta) = (1-r)y_P(\theta) + r y_I(\theta) \quad (۵)$$

در روابط بالا $I(x,y)$ تصویر چشم، (x,y) مختصات کارتزین اصلی، (r,θ) مختصات قطبی نرمال‌شده، (x_p,y_p) و (x_I,y_I) به ترتیب مختصات مردمک و عنبیه در جهت θ است.

تعداد خطوط شعاعی نیز وضوح زاویه‌ای می‌باشد. تعداد نقاط ثابت انتخاب شده روی هر خط شعاعی، بدون توجه به این‌که در زاویه‌ی مشخص، ناحیه عنبیه چقدر باریک یا ضخیم است، تعداد ثابتی نقاط اطلاعات از عنبیه به‌دست می‌دهد. به دلیل آن‌که مردمک و عنبیه غیر هم‌مرکز هستند، یک تابع نگاشت لازم است تا نقاط را با توجه به زاویه‌شان تغییر مقیاس دهد.

$$r' = \sqrt{\alpha\beta} \pm \sqrt{\alpha\beta^2 - \alpha - r_I^2} \quad (۶)$$

$$\alpha^2 = {o_x}^2 + {o_y}^2 \quad (۷)$$

$$\beta = cos(\pi - tan^{-1}\frac{o_y}{o_x} - \theta) \quad (۸)$$

در روابط بالا تفاوت بین مرکز عنبیه و مرکز مردمک با o_x و o_y نشان داده شده است و r' فاصله بین لبه مردمک و لبه عنبیه در زاویه θ است. r_I نیز شعاع عنبیه می‌باشد. رابطه نگاشت، شعاع عنبیه را به‌صورت تابعی از θ می‌دهد. درنهایت از یک شکل دونات مانند، یک صفحه دو بعدی با طولی برابر با وضوح زاویه‌ای و عرضی برابر با وضوح شعاعی ایجاد می‌شود. هرچه مقدار وضوح شعاعی و زاویه‌ای بیشتر باشد، دقت نرمال‌کردن بیشتر است، اما حجم محاسبات در مرحله استخراج ویژگی، کد کردن و مقایسه بیشتر می‌شود. در این مقاله اندازه صفحه نرمال شده ۲۰×۴۸۰ است و در شکل (۱۲) یک نمونه صفحه نرمال‌شده نشان داده می‌شود.

شکل ۱۲. عنبیه نرمال‌شده.

شکل (۱۱) عنبیه جداشده‌ای است که قسمت‌های نویز آن با مقدار یک و مقدار عنبیه با صفر مشخص شده است بنابراین، این شکل را نیز به شکل نرمال‌شده تبدیل می‌کنیم و تبدیل به یک ماتریس ۲۰ در ۴۸۰ می‌شود به این ماتریس ماسک می‌گویند شکل (۱۳) ماسک نرمال‌شده را نشان می‌دهد. اکنون ما دو ماتریس داریم که یکی برای الگوی عنبیه است و دیگری ماتریسی است که محل نویزها را نشان می‌دهد و از این دو ماتریس در قسمت مقایسه استفاده می‌شود.

شکل ۱۳. عنبیه نرمال‌شده به همراه نویز.

استخراج ویژگی

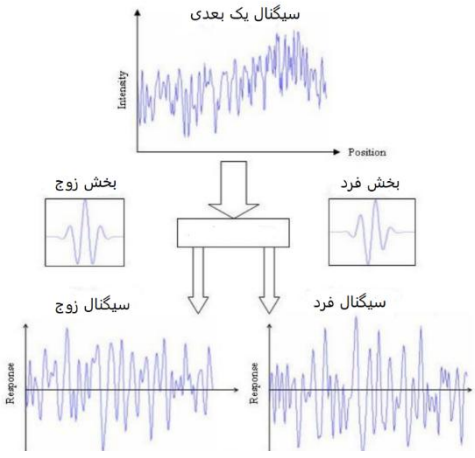
در این مقاله از سامانه داگمن برای استخراج ویژگی استفاده شده است. الگوی عنبیه نرمال‌شده با موجک‌های لگاریتمی گابور یک‌بعدی اجرا می‌شود. الگوی نرمال‌شده دوبعدی در تعدادی از سیگنال‌های یک‌بعدی شکسته شده و سپس این سیگنال‌های یک‌بعدی یا موجک لگاریتمی گابور با استفاده از FFT و معکوس FFT محاسبه می‌شوند. فیلتر گابور با مدوله‌کردن موج سینوسی/کسینوسی گوسی ایجاد می‌شود. این فیلتر قادر به ارائه محلی‌سازی پیوسته بهینه در هر دو حوزه فضا و فرکانس است. موج سینوسی در فرکانس، کاملا محلی‌سازی شده است، اما در فضا محلی‌سازی نمی‌شود. مدولاسیون سینوسی با یک سیگنال گوسی، محلی‌سازی در فضا را با از دست دادن محلی‌سازی در فرکانس ارائه می‌دهد. تجزیه سیگنال با استفاده از جفت مربع فیلترهای گابور انجام می‌شود. فرآیند استخراج ویژگی در شکل (۱۴) نشان داده شده است. سطرهای الگوی نرمال‌شده که اکنون به‌عنوان سیگنال یک‌بعدی درنظر گرفته می‌شود در واقع مربوط به حلقه دایره‌ای روی فضای عنبیه می‌باشد.

۲-۲- رمزنگاری الگوی عنبیه

این مقاله همانند بقیه سیستم‌های شناسایی هویت دارای دو بخش است بخش اول قسمت ثبت‌نام و بخش دوم قسمت تائید هویت است که هر مرحله به‌صورت جداگانه توضیح داده می‌شود.

ثبت‌نام

در مرحله ثبت‌نام الگوی عنبیه به‌دست‌آمده، ابتدا توسط رمزنگاری‌دیداری رمزنگاری می‌شود و تبدیل به دو سهم می‌شود سهم اول در پایگاه داده و سهم دوم در کارت‌شناسایی کاربر ذخیره می‌شود. اما برای ایجاد امنیت بیشتر از الگوریتم RSA استفاده می‌شود در این الگوریتم دو کلید عمومی و خصوصی تولید می‌شود.

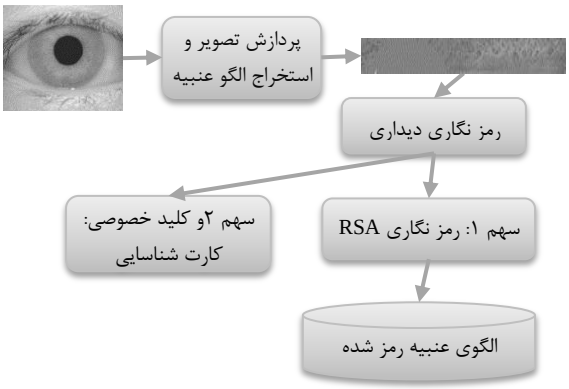


شکل ۱۴. فرآیند استخراج ویژگی [۱۶].

کلید عمومی نیاز به ذخیره‌سازی ندارد. اما برای رمزگشایی نیاز به کلید خصوصی داریم بنابراین، کلید خصوصی همراه با سهم دوم در کارت‌شناسایی کاربر ذخیره می‌شود. در این مرحله برای رمزنگاری از کلید عمومی استفاده می‌شود.

تائیدهویت

در قسمت تائید هویت، کاربر کارت‌شناسایی خود را ارائه می‌دهد. در نهایت با کلید خصوصی که در کارت‌شناسایی قرار دارد الگوی رمزشده در پایگاه‌داده رمزگشایی می‌شود. الگوی ذخیره شده در کارت‌شناسایی و الگوی رمزگشایی شده باهم مقایسه می‌شوند اگر باهم تطابق داشتند، این دو سهم با عمل XOR کردن باهم ترکیب می‌شوند. اما طول الگوی ترکیب شده دو برابر طول الگوی اصلی است. بنابراین، با عمل نمونه‌برداری پایین، بیت‌های الگوی عنبیه بازسازی می‌شوند. از طرفی برای تائید اعتبار باید از چشم کاربر عکس‌برداری شود سپس با مراحلی که قبلا بحث شده است الگوی عنبیه استخراج شود سپس دو الگو، یعنی الگوی ذخیره شده در پایگاه داده و کارت‌شناسایی با الگوی کاربر که قصد عبور از سیستم را دارد مقایسه می‌شود اگر شباهت وجود داشت، کاربر می‌تواند وارد سیستم شود.



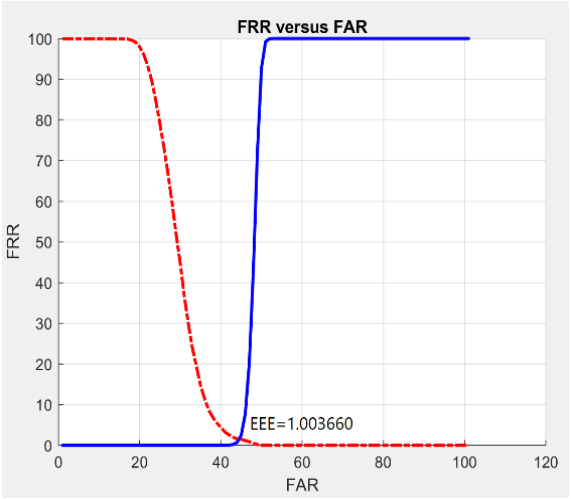
شکل ۱۵. فرآیند ثبت‌نام در الگوریتم ارائه‌شده در این مقاله

۳- نتایج شبیه‌سازی

در این بخش به بررسی و ارزیابی سامانه پیشنهادی جهت حفاظت از پایگاه داده بیومتریک عنبیه خواهیم پرداخت. برای این هدف، در ابتدا یک ارزیابی از ویژگی‌های استخراج شده ارائه خواهد شد. سپس عملکرد سامانه در حضور نویز مورد تجزیه و تحلیل و بررسی قرار خواهد گرفت. در انتها نیز، سامانه پیشنهادی در این مقاله، با سایر سامانه‌های موجود، مورد مقایسه قرار می‌گیرد.

۳-۱- استخراج ویژگی و مقایسه

شبیه‌سازی در این مقاله در بانک تصویر CAISA-v1 انجام شده است پیش از این مشخصات این بانک تصویر ذکر شده است. که دارای ۱۰۸ کلاس (هر کلاس برای یک شخص) است در هر کلاس ۷ تصویر عنبیه برای هر شخص وجود دارد که از ۳ تصویر برای آموزش و ۴ تصویر برای آزمایش استفاده می‌شود. بعد از قطعه‌بندی اندازه فضای نرمال‌شده عنبیه ۲۰ در ۴۸۰ است بنابراین تعداد بیت‌های کد عنبیه ۹۶۰۰ بیت می‌شود. برای ارزیابی عملکرد این مقاله، دو حالت تائید و شناسایی هویت بررسی می‌شود. در هنگام تائید هویت، مقایسه بین گروهی و مقایسه درون‌گروهی انجام خواهد شد. ارزیابی عملکرد تائید هویت روش مقاله با استفاده از معیارهای تصمیم‌گیری دو توزیع درون‌گروهی و بیرون‌گروهی، خطای پذیرش به اشتباه و خطای رد به اشتباه صورت می‌گیرد. در شکل‌های (۱۶) و (۱۷) مقدار EER سامانه ارائه‌شده در این مقاله را مشاهده می‌کنیم که در حدود یک درصد است.



شکل ۱۶. مقدار EER بر حسب مقادیر FRR،FAR برای الگوریتم ارائه‌شده در این مقاله.

۳-۲- افزودن نویز به سامانه ارائه‌شده در این مقاله

یکی از عوامل مهم یک سامانه شناسایی هویت بیومتریک این است که عملکرد آن سامانه در مقابل نویز ایده‌آل باشد. بنابراین، برای این‌که عمل‌کرد سامانه بیومتریک ارایه شده در این مقاله را در مقابل نویز بسنجیم، هر تصویر چشم در پایگاه داده‌ها را در معرض نویزهای فلفل‌نمکی و نویز سفید گوسی قرار می‌دهیم و یک فیلتر ۳ بعدی میانگین هم بر روی تصاویر اعمال می‌کنیم. در شکل‌های (۱۸ -۲۳) مقدار EER سامانه، بعد از اعمال نویزها و فیلتر میانگین نشان داده شده است.

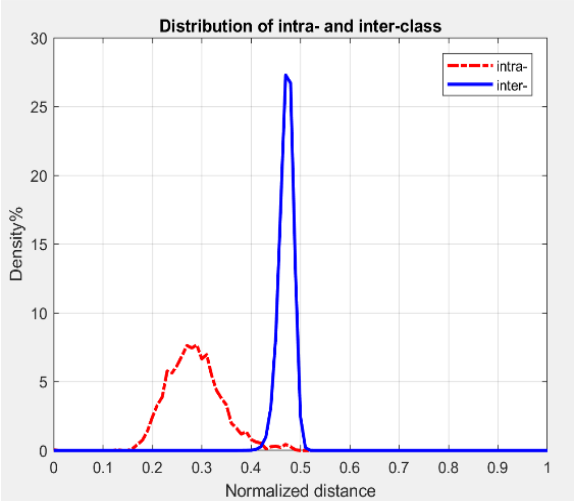
۴-۵- مقایسه سامانه ارائه‌شده در این مقاله با سایر روش‌های بررسی شده

سامانه تشخیص هویت را با روش تبدیل هاف نیز پیاده‌سازی

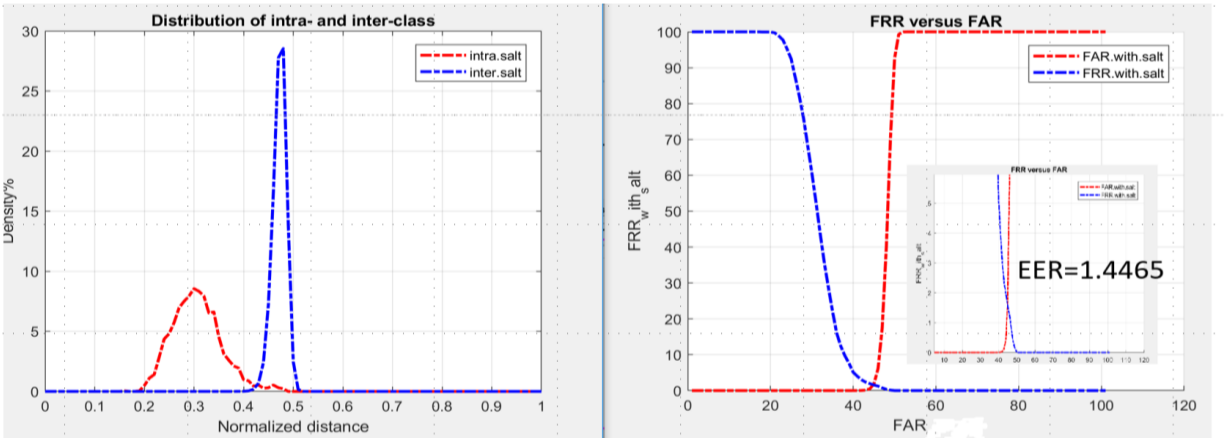
کردیم. در خروجی شبیه‌سازی مشاهده کردم مقدار ERR در این روش برابر ۳/۳۶ یا ۳/۳۶ درصد است که در این مقاله مقدار EER برابر یک درصد است. از لحاظ سرعت اجرای برنامه روش تبدیل هاف سرعت بسیار بالایی دارد در صورتی‌که سرعت اجرای الگوریتم این مقاله بسیار بالاست. در شکل (۲۱) نمودار ERR و نمودار توزیع بین‌گروهی و درون‌گروهی روش تبدیل هاف مشاهده می‌شود.

روش ایجاد امنیت در پایگاه داده عنبیه چشم به وسیله رمزنگاری دیداری و نهان‌نگاری که توسط Mohammad A.M و همکارانش در سال ۲۰۱۶ ارائه شده است، از دو بانک تصویر UBIRIS V1 و CASIA استفاده کرده است [۹]. همان‌طور که در شکل (۲۲) مشاهده می‌شود بدون ایجاد امنیت در این پایگاه داده‌ها مقدار ERR به ترتیب برای بانک تصویر UBIRIS-V1 و CASIA برابر۱/۱۴۶درصد و ۲/۵۵۷ است. بعد از اعمال نهان‌نگاری در این روش مقدار ERR برای هر پایگاه تصویر به‌ترتیب برابر ۱/۲۰۶ و۲/۶۵۴ درصد شده است. در این روش همانند روش ارائه‌شده در این مقاله به تصویر نویزهای مختلف اعمال کرده است که در شکل (۲۳) مقدار ERR برای هر پایگاه تصویر بعد از اعمال نویز مشاهده می‌شود. در الگوریتم بررسی شده دیگر، به نام ایجاد امنیت در پایگاه داده عنبیه چشم با استفاده از روش رتبه‌بندی محلی، که توسط DongdongZhao و همکارانش در سال ۲۰۱۸ ارائه شده است[۱۷]، زمانی‌که هیچگونه راهبرد امنیتی در این روش ایجاد نمی‌شود مقدار ERR برابر ۸/۴۳ درصد است که می‌توان گفت درصد بسیار بالایی است. اما با اعمال روش جابه‌جایی که قبلا ذکر شده است این میزان به ۱/۳۶ می‌رسد.

در همین الگوریتم از روش ماسک‌گذاری نیز استفاده شده بود که بعد از اعمال روش ماسک‌گذاری به همراه روش جابه‌جایی مقدار ERR برابر ۱/۳۲ درصد می‌شود. در جدول‌های (۱ و ۲) خلاصه‌ای از مطالب بررسی شده بالا نشان داده شده است.

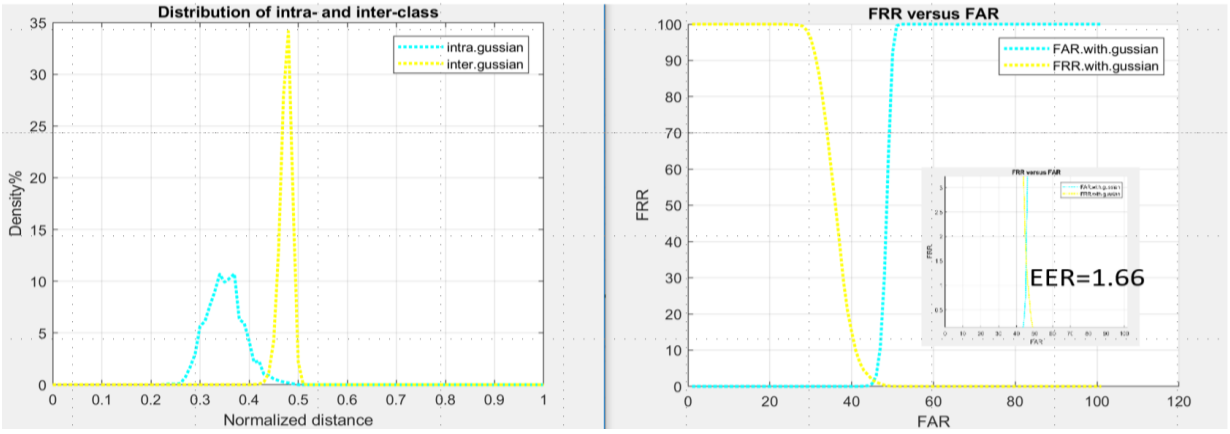


شکل ۱۷. نمودار توزیع بین‌گروهی و درون‌گروهی.



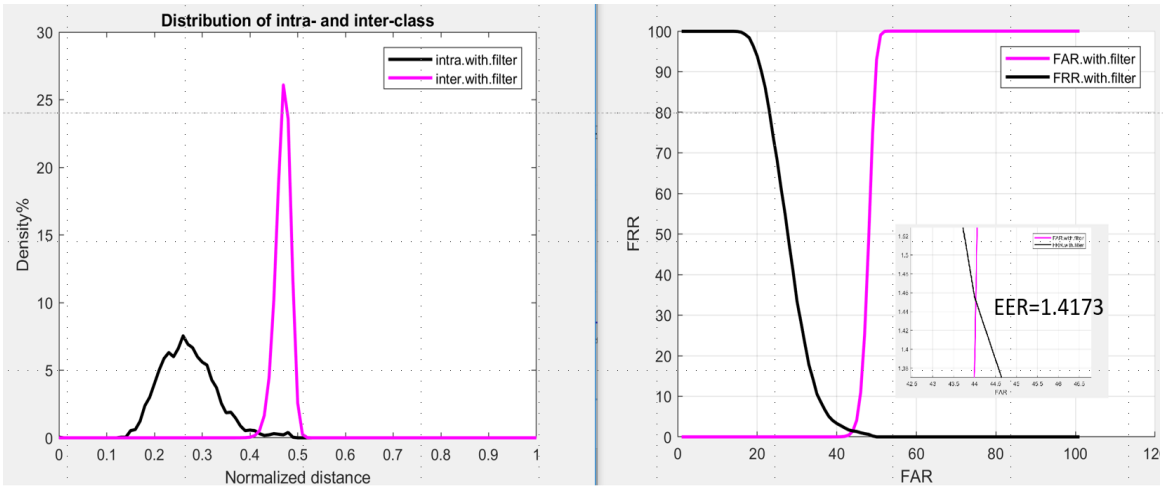
(ب) (الف)

شکل ۱۸. (الف) مقدار ERR بعد از اعمال نویز فلفل نمکی، (ب) توزیع بین‌گروهی و درون‌گروهی بعد از اعمال نویز فلفل نمکی.



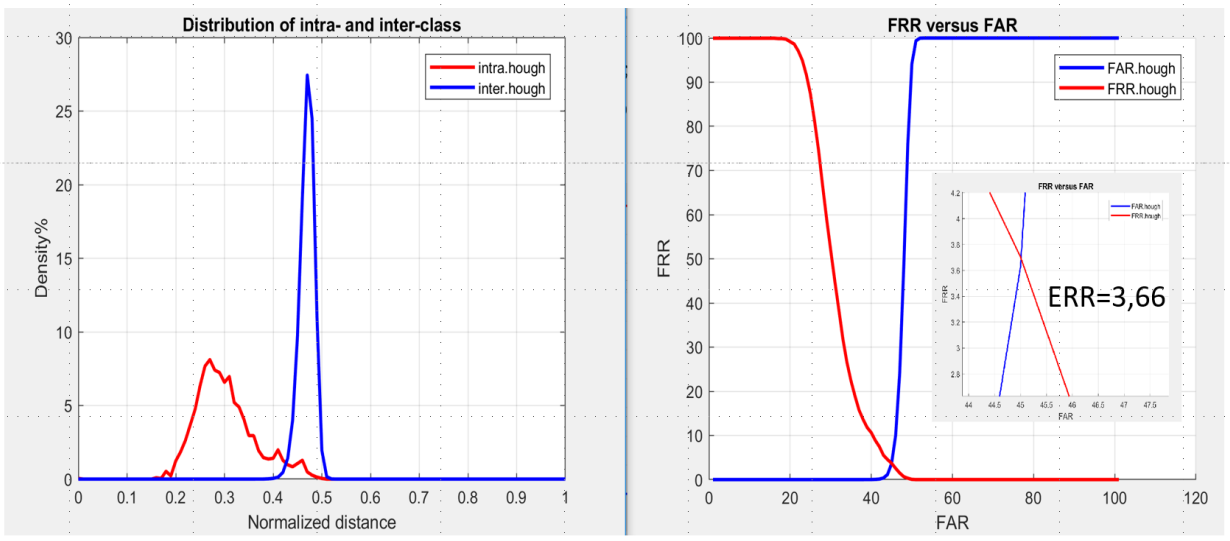
(ب) (الف)

شکل ۱۹. (الف) مقدار ERR بعد از اعمال نویز نویز سفید گوسی، (ب) توزیع بین‌گروهی و درون‌گروهی بعد از اعمال نویز سفید گوسی.



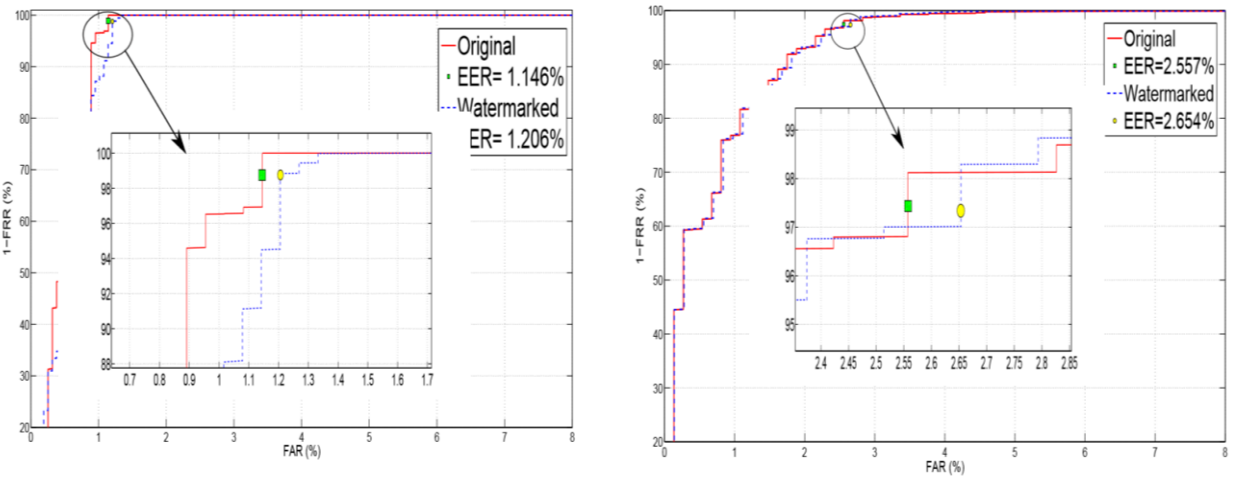
(ب) (الف)

شکل ۲۰. (الف) مقدار ERR بعد از اعمال فیلتر میانگین، (ب) توزیع بین‌گروهی و درون‌گروهی بعد از اعمال فیلتر میانگین.



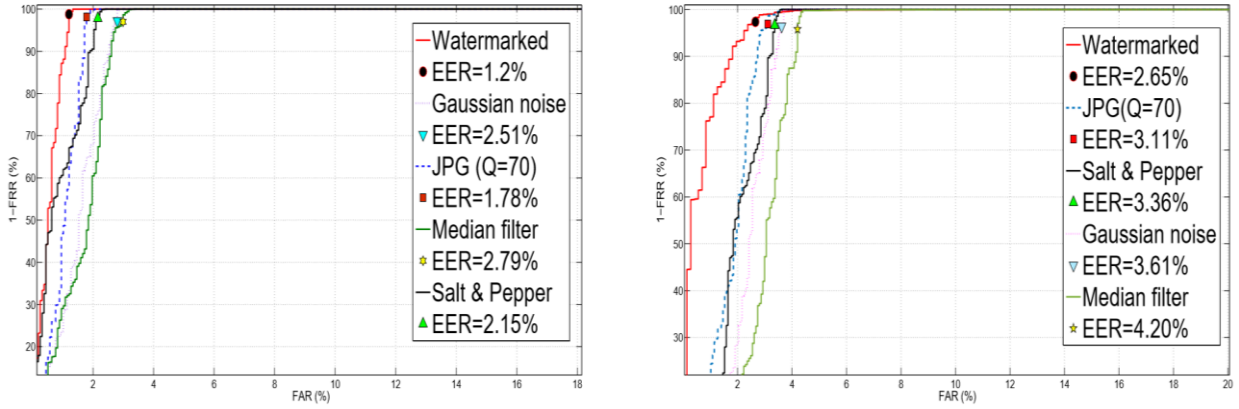
(ب) (الف)

شکل ۲۱. (الف) مقدار ERR برای الگوریتم قطعه‌بندی با تبدیل هاف، (ب) توزیع بین‌گروهی و درون‌گروهی برای الگوریتم قطعه‌بندی با تبدیل هاف.



(ب) (الف)

شکل ۲۲. (الف) مقدار ERR در بانک تصویر UBIRIS ، (ب) مقدار ERR در بانک تصویر بانک تصویر CASIA.



(ب) (الف)

شکل ۲۳. (الف) مقدار ERR بعد از اعمال نویز در بانک تصویر UBIRIS، (ب) مقدار ERR بعد از اعمال نویز در بانک تصویر بانک تصویر CASIA.

جدول ۱. مقدار ERR برای سامانه‌های بررسی شده.

الگوریتم	EER
رمزنگاری دیداری و RSA	۱/۰۰۳۶۶
رمزنگاری دیداری و نهان‌نگاری (UBIRIS)	۱/۲۰۶
رمزنگاری دیداری و نهان‌نگاری (CASIA)	۲/۶۵۴
الگوریتم رتبه‌بندی محلی	۸/۴۳
الگوریتم رتبه‌بندی محلی بهبودیافته	۱/۳۲
تبدیل هاف	۳/۶۶

جدول ۲. مقدار ERR برای هر سامانه بعد از اعمال نویز.

الگوریتم	نویز سفید گوسی با واریانس ۰/۰۰۱	نویز فلفل نمکی با واریانس ۰/۰۰۵	فیلتر median 3*3
الگوریتم رمزنگاری دیداری و RSA	۱/۶۶	۱/۴۴	۱/۱۴۶
رمزنگاری دیداری و نهان‌نگاری (UBIRIS)	۳/۶۱	۳/۳۶	۴/۲۰
رمزنگاری دیداری و نهان‌نگاری (CASIA)	۲/۵۱	۱/۷۸	۲/۷۹

۴- نتیجه‌گیری

در این مقاله، یک سیستم شناسایی جدید بر مبنای افزایش امنیت در پایگاه داده عنبیه چشم طراحی گردید. در این طرح پیشنهادی، پس از معرفی تکنیک‌های پردازش تصویر عنبیه و چگونگی استخراج ویژگی‌ها، برای افزایش امنیت اطلاعات پایگاه داده، استفاده از الگوریتم رمزنگاری دیداری و RSA به‌صورت توأم پیشنهاد گردید. در رمزنگاری دیداری چون نیمی از اطلاعات الگوی عنبیه در کارت‌شناسایی و نیمی دیگر در پایگاه داده ذخیره می‌شود سوءاستفاده از سامانه در صورت عدم وجود کارت شناسایی امکان‌پذیر نخواهد بود. اما در رمزنگاری RSA با استفاده از تجزیه n به عوامل اول و حدس‌زدن پیام می‌توان رمز را شکاند اما باید

گفت این روش‌ها به راحتی عملی نیست، چرا که اگر فرض بر این گذاشته شود که فرد مهاجم دسترسی به کلید عمومی دارد و قصد حدس زدن کلید خصوصی را دارد، برای عدد n با ۱۵۵ رقم (RSA-155) با قوی‌ترین کامپیوترهای موجود بیش از ۷ ماه زمان لازم است تا بتوان عوامل اول تشکیل دهنده n را مشخص کرد. علاوه‌بر این در بخش شبیه‌سازی به ارزیابی الگوریتم ارائه‌شده در این مقاله پرداخته شد و با سایر الگوریتم‌های مشابه مورد مقایسه گردید. نتایج شبیه‌سازی نشان داد که الگوریتم پیشنهادی مقدار ERR کمتری دارد و در نهایت مقدار خطای آن در تشخیص هویت کمتر است.

۶- مرجع‌ها

[1] Liu, S.; Silverman, M. "A Practical Guide to Biometric Security Technology," IT Prof. 2001, 3(1), 27–32.

[2] Wang, Q.; Zhang, X.; Li, M.; Dong, X.; Zhou, Q.; Yin, Y. "Adaboost and Multi-Orientation 2d Gabor-Based Noisy Iris Recognition," Pattern Recognit. Lett. 2012, 33(8), 978–983.

[3] Singh, G. "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security," Int. J. Comput. Appl. 2013, 67(19),33-38.

[4] Wildes, R. P. "Iris Recognition: An Emerging Biometric Technology," P. IEEE. 1997, 85(9), 1348–1363.

[5] Kalpana, P.; Singaraju, S. "Data Security in Cloud Computing Using RSA Algorithm," Int. J. Res. Comput. Commun. Technol. 2012, 278–5841.

[6] Padmavathi, B.; Kumari, S. R. "A Survey on Performance Analysis of DES, AES And RSA Algorithm along with LSB Substitution," Int. J. Sci. Res., India, 2013, 2(4), 170-174.

[7] Abdullah, M. A. M.; Dlay, S. S.; Woo, W. L.; Chambers, J. A. "A Framework for Iris Biometrics Protection: A Marriage Between Watermarking and Visual Cryptography," IEEE Access 2016, 4, 10180–10193.

[8] Zare, A.; Aghagolzadeh, A.; Kazemitabar, S. J. "A Novel Metaheuristic Based Visual Cryptography"; Adv. Defence Sci. Technol. 2019, 10(3), 297-306 (In Persian).

[9] Shamsafar, F.; Seyedarabi, H.; Aghagolzadeh, A. "Securing the Iris Database Using Visual Cryptography and Substitution" 21st Iranian Conf. Elec. Eng. 2013 (In Persian).

[10] Abdullah, M. A. M. "Advancing Iris Biometric Technology." Newcastle Univ. 2017.

[11] Jin, Z.; Hwang, J. Y.; Lai, Y.-L.; Kim, S.; Teoh, A. B. J. "Ranking-Based Locality Sensitive Hashing-Enabled Cancelable Biometrics: Index-of-Max Hashing," IEEE Trans. Inf. Forensics Secur. 2017, 13(2), 393–407.

[12] Dubey, R. B.; Madan, A. "Iris Localization Using Daugman's Intero-Differential Operator," Int. J. Comput. Appl. 2014, 93(3), 6–12.

[13] Shah; S.; Ross, A. "Iris Segmentation Using Geodesic Active Contours," IEEE Trans. Inf. Forensics Secur. 2009, 4(4), 824–836.

[14] Proença H., Alexandre L.A., ICIAP 2005: Image Analysis and Processing – ICIAP 2005 pp 970-977

[15] Harakannanavar, S. S.; Prabhushetty, K. S.; Hugar, C.; Sheravi, A.; Badiger, M.; Patil, P. "IREMD: An Efficient Algorithm for Iris Recognition," Int. J. Adv. Netw. Appl. 2018, 9, (5), 3580–3587.

[16] Boukhari, A.; Chitroub, S.; Bouraoui, I. "Biometric Signature of Private Key by Reliable Iris Recognition Based on Flexible-ICA Algorithm," Int. J. Commun. Netw. Syst. Sci. 2011, 4(12), 778.

[17] Zhao, D.; Fang, S.; Xiang, J.; Tian, J.; Xiong, S. "Iris Template Protection Based on Local Ranking," Secur. Commun. Netw. 2018, 2018,1-9.