مقاله پژوهشی

حفظ محرمانگی و صحت داده‌ها و جلوگیری از دسترسی غیرمجاز به تصاویر پزشکی DICOM

محمد سلطانی، حسن شاکری و محبوبه هوشمند

چکیده: با گسترش فناوری‌های مخابراتی و ارتباطی به‌ویژه ارتباطات بی‌سیم، رمزنگاری اطلاعات، یکی از ضرورت‌های ارتباطی است. امروزه از الگوریتم‌های رمزنگاری برای افزایش امنیت و جلوگیری از تغییر تصاویر پزشکی DICOM استفاده می‌شود. تغییر در تصاویر پزشکی DICOM موجب تشخیص نادرست پزشک از روند درمانی بیمار خواهد شد. در این مقاله نوعی از الگوریتم‌های رمزنگاری ترکیبی ارائه می‌شود. در الگوریتم پیشنهادی از الگوریتم رمزنگاری DNA برای رمزنگاری تصاویر DICOM و از اطلاعات بیومتریک بیمار مانند تصویر اثر انگشت و یا عنبیه چشم برای افزایش حساسیت در کلیدهای استفاده‌شده، ساخت امضای دیجیتال و تأیید اعتبار تصاویر پزشکی DICOM استفاده می‌گردد. الگوریتم رمزنگاری طراحی‌شده در مقابل حملات Brute force مقاوم بوده و Entropy تصاویر DICOM رمزنگاری‌شده در آن بیشتر از ۷٫۹۹ است.

کلیدواژه: **DICOM، رمزنگاری، امنیت، اطلاعات بیومتریک بیمار، الگوریتم رمزنگاری DNA، امضای دیجیتال.**

۱- مقدمه

امنیت اطلاعات و ایمن‌سازی شبکه‌های کامپیوتری از جمله مؤلفه‌هایی بوده که نمی‌توان آن را مختص یک فرد و یا سازمان در نظر گرفت. در پزشکی سیستم اطلاعات بیمارستانی یک سیستم پیاده‌سازی، یکپارچه تولید اطلاعات لازم برای مدیریت تمام فعالیت‌های مربوط به سلامت از قبیل برنامه‌ریزی، نظارت، هماهنگی و تصمیم‌گیری است. هدف از استقرار یک نظام اطلاعات بیمارستانی، به‌کارگیری رایانه و وسایل ارتباطی برای جمع‌آوری، ذخیره، پردازش، بازیابی و ارتباط‌دادن مراقبت بیمار و اطلاعات اداری برای تمام فعالیت‌های مربوط به بیمارستان است.

امنیت اطلاعات در علم پزشکی و انتقال ایمن اطلاعات در پزشکی از راه دور بسیار اهمیت دارد؛ زیرا تغییر در اطلاعات پزشکی بیمار موجب تشخیص نادرست پزشک و اختلال در روند درمانی بیمار خواهد شد. تهاجم به داده‌های حیاتی یک بیمار به دو گروه تهاجم از داخل و تهاجم از خارج تقسیم می‌شود. تهاجم از خارج با شنود و یا تغییر در پرونده‌های پزشکی به‌وسیله حمله‌های تحت شبکه‌های کامپیوتری مثل استراق سمع[1]، تزریق بسته[2] و یا حمله مرد میانی[3] صورت می‌گیرد [۱]. تهاجم از داخل می‌تواند توسط کلینیسین، بیمار یا هر فرد دیگر که در محل ارائه خدمات مراقبتی حضور دارد، انجام شود. تهاجم از داخل به‌منظور مخفی‌کردن خطاهای پزشکی[4] یا کلاه‌برداری از بیمه‌های درمانی صورت می‌گیرد [۲]. امروزه معمول‌ترین راه برای امنیت و حفظ حریم خصوصی، رمزگذاری پرونده‌های پزشکی است. رمزنگاری، امکانات خوبی برای امنیت اطلاعات فراهم می‌کند. از جمله روش‌های بهبودیافته می‌توان مواردی همچون تصدیق هویت[5]، فشرده‌سازی پیام[6]، امضاهای دیجیتالی[7]، قابلیت عدم انکار[8] و ارتباطات شبکه[9] را نام برد. بر اساس آخرین آمارهای به‌دست‌آمده در ۵ سال گذشته از موتورهای جستجوگر مانند گوگل[10] و نرم‌افزار آنلاین مربوط[11]، آمار درخواست جستجوی کلیدواژه Encryption و موضوع رمزگذاری داده‌های مراقبت‌های بهداشتی[12] در دنیا نشان داده شده است [۳]. در پرونده‌های پزشکی بیمار از تصویربرداری و ارتباطات دیجیتال در پزشکی یا دایکام[13] (DICOM) برای تشخیص و پیگیری مراحل درمانی بیمار استفاده می‌شود.

تصویربرداری و ارتباطات دیجیتال در پزشکی یک پروتکل استاندارد برای مدیریت و انتقال تصاویر پزشکی و داده‌های مربوط است و در بسیاری از مراکز بهداشتی درمانی مورد استفاده قرار می‌گیرد. تصاویر DICOM می‌توانند در هر زمینه پزشکی که در آنها عمدتاً از فناوری تصویربرداری پزشکی استفاده می‌شود، مانند رادیولوژی، قلب، انکولوژی، زنان و زایمان و دندانپزشکی استفاده شوند. در شکل ۱ نمونه تصویر DICOM نشان داده شده و در این مقاله نوعی از الگوریتم‌های رمزنگاری ترکیبی ارائه می‌گردد. در الگوریتم ارائه‌شده در این مقاله از الگوریتم رمزنگاری DNA[14] برای رمزنگاری تصاویر DICOM استفاده شده است. برای تأیید اعتبار تصاویر رمزگشایی‌شده و مقاومت بیشتر در مقابل حملات Brute force و افزایش فضای کلید از امضای دیجیتال و اطلاعات

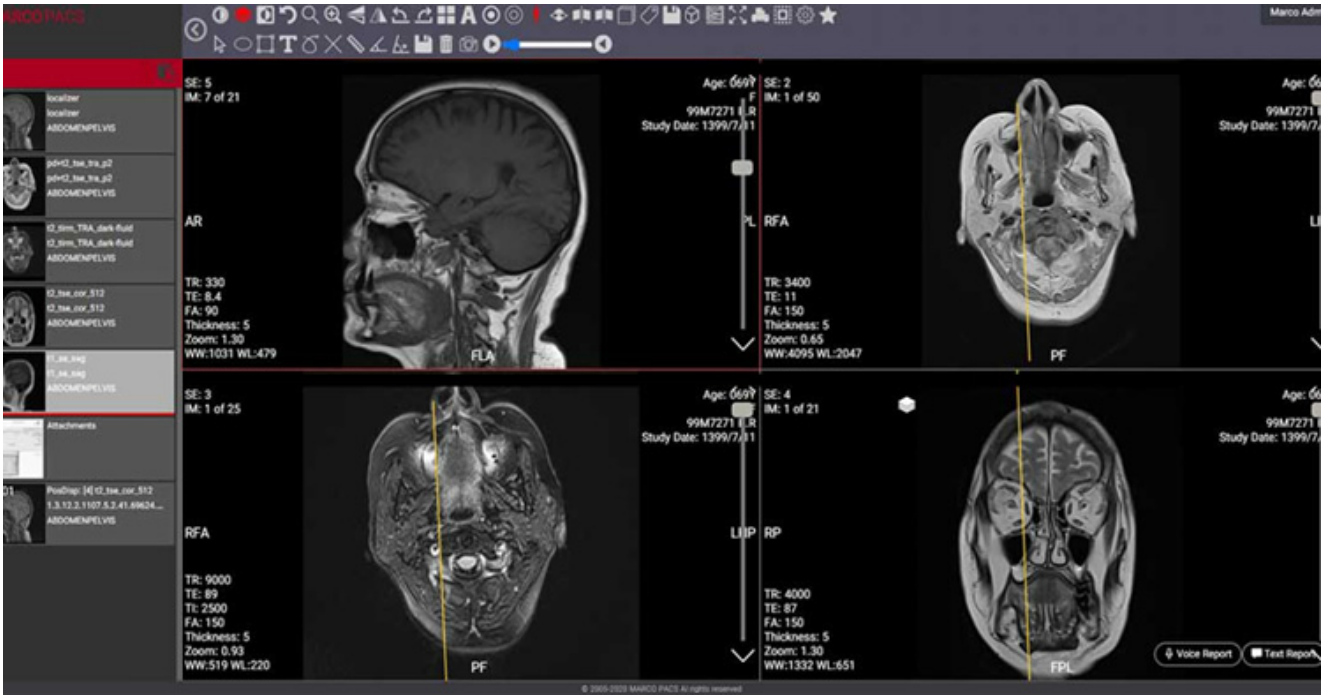
این مقاله در تاریخ ۳ دی ماه ۱۴۰۰ دریافت و در تاریخ ۴ تیر ماه ۱۴۰۱ بازنگری شد.

محمد سلطانی، گروه مهندسی کامپیوتر، واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران، (email: mohammad.soltani@mshdiau.ac.ir).

حسن شاکری (نویسنده مسئول)، گروه مهندسی کامپیوتر، واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران، (email: shakeri@mshdiau.ac.ir).

محبوبه هوشمند، گروه مهندسی کامپیوتر، واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران، (email: houshmand@mshdiau.ac.ir).

1. Eavesdropping
2. Packet Injection
3. Men in Middle Attack
4. Malpractice
5. Authentication
6. Data Compression
7. Digital Signature
8. Non Repudiation
9. Network Communication
10. Google
11. Google Trends
12. Healthcare Data Encryption
13. Digital Imaging and Communications in Medicine
14. Deoxyribonucleic Acid



شکل ۱: نمونه تصویر DICOM [۶].

بیومتریک[1] منحصربه‌فرد بیمار مانند اثر انگشت[2] و یا عنبیه چشم[3] استفاده استفاده شده است.

کلید الگوریتم رمزنگاری DNA استفاده‌شده در الگوریتم پیشنهاد داده شده، کاملاً وابسته به نتیجه هش‌شده[4] اطلاعات بیومتریک بیمار و نتیجه هش‌شده امضای دیجیتال خواهد بود. برای مقاومت بیشتر در مقابل حملات Brute force، مسایلی مثل طول کلید و استفاده از الگوریتم‌های هش بسیار مؤثر خواهد بود و باید توجه داشت که با کلیدهای طولانی‌تر، اندازه فضای کلید به‌طور نمایی[5] بزرگ‌تر خواهد شد [۴] و [۵]. در رمزنگاری، طول و قدرت کلید استفاده‌شده بسیار مهم بوده و به همین دلیل مدیریت کلید رمزنگاری، موضوعی با اهمیت زیاد است. در این مقاله در قسمت ۴-۴، فضای کلید در الگوریتم ارائه‌شده تحلیل گردیده است. با توجه به تحلیل فضای کلید و ساختار الگوریتم رمزنگاری، فقط در قسمت رمزنگاری DICOM با استفاده از الگوریتم رمزنگاری DNA، فضای کلید برای این قسمت برابر با $(۱۰^{۱۴})^{۴} = ۱۰^{۵۶}$ است. برای جلوگیری از حملات Brute force علاوه بر بالابودن فضای کلید الگوریتم رمزنگاری DNA، قسمت‌های دیگر الگوریتم پیشنهاد داده شده مانند استفاده از الگوریتم RSA[6] برای ساخت امضای دیجیتال، اطلاعات بیومتریک بیمار، عملگر XOR و هش‌شدن تعدادی از کلیدها برای استفاده، در جلوگیری از حملات Brute force بسیار مؤثر خواهند بود. ساختار الگوریتم رمزنگاری پیشنهاد داده شده در ادامه آمده است.

در بخش ۲، پیشینه تحقیق در مورد الگوریتم‌های رمزنگاری تصاویر DICOM و در بخش ۳، الگوریتم رمزنگاری مطرح‌گردیده در این مقاله بررسی دقیق شده است. در بخش ۴ برای ارزیابی الگوریتم پیشنهاد داده شده و مقاومت الگوریتم رمزنگاری در برابر حملات، مهم‌ترین پارامترهای مورد نیاز بررسی و ارزیابی گردیده‌اند. در بخش ۵ نیز به جمع‌بندی و پیشنهادهایی برای کارهای آتی پرداخته شده است.

۲- پیشینه تحقیق

در ادامه ساختار یکی از الگوریتم‌های رمزنگاری متقارن تصاویر آمده است. در شکل ۲ یک طبقه‌بندی از مجموعه الگوریتم‌های استفاده‌شده در مورد موضوع امنیت و رمزنگاری تصاویر پزشکی نشان داده شده است. با توجه به شکل، چندین الگوریتم رمزنگاری تصاویر پزشکی بر مبنای الگوریتم‌های رمزنگاری کلاسیک[7] و الگوریتم‌های نقشه آشوب[8] مورد بررسی قرار داده می‌شوند.

۲-۱ ساختار الگوریتم رمزنگاری کلاسیک

در این قسمت، ۶ نوع از الگوریتم‌های کلاسیک بررسی شده‌اند:

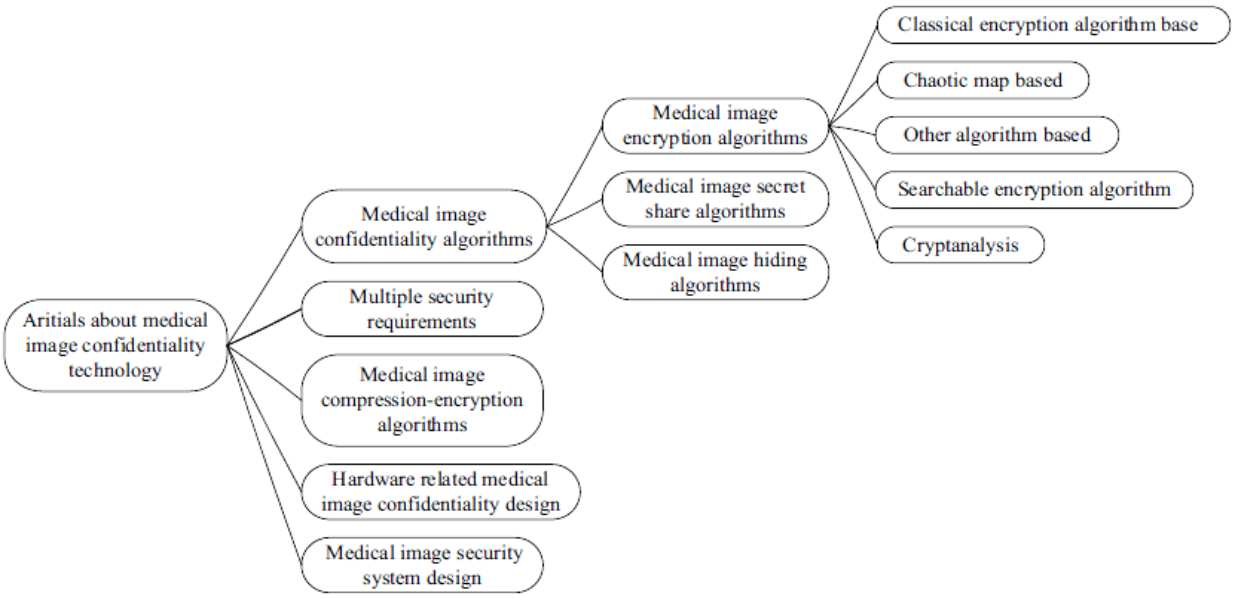
۱) الگوریتم RSA بهبود یافته شده برای رمزنگاری تصویربرداری سونوگرافی [۸]

۲) الگوریتم استفاده از AES[9] که از طرف Q. n. Natsheh و سایر همکارانش پیشنهاد داده شده است. در این الگوریتم می‌توان به شکل هم‌زمان چندید تصویر پزشکی را رمزنگاری کرد [۹].

۳) K. M. Ranjith و همکارانش نوعی از الگوریتم‌های رمزنگاری تصویر مبتنی بر اعداد غیرمنطقی و یا گنگ[10] را استفاده می‌کنند. در الگوریتم پیشنهاد داده شده از تبدیل خطی[11] و عملگر XOR برای به هم زدن موقعیت‌های پیکسل‌های تصویر استفاده می‌شود [۱۰].

۴) طبق ویژگی‌های تصاویر DICOM، O. Dorgham و همکارانش از الگوریتم رمزنگاری منحنی بیضوی (ECC)[12] استفاده کرده‌اند.

1. Biometric Information
2. Fingerprint
3. Iris
4. Hash
5. Exponential
6. Rivest-Shamir-Adleman
7. Classic Image Encryption
8. Chaotic Map
9. Advanced Encryption Standard
10. Irrational Numbers
11. Linear Transformation
12. Elliptic Curves Cryptography



شکل ۲: طبقه‌بندی مجموعه الگوریتم‌های استفاده‌شده در مورد موضوع امنیت و رمزنگاری تصاویر پزشکی [۷].

در الگوریتم پیشنهاد داده شده، الگوریتم رمزنگاری کلید متقارن و نامتقارن با یکدیگر ترکیب خواهند شد و الگوریتم مورد نظر را سریع‌تر و ایمن‌تر خواهند کرد [۱۱].

۵) در [۱۲] الگوریتم‌های رمزنگاری AES، ECC، امضای دیجیتال و الگوریتم هش[1] Whirlpool با یکدیگر ترکیب شده‌اند.

۶) در [۱۳] تصویر DICOM به قسمت‌های مختلفی تقسیم‌بندی خواهد شد و از الگوریتم رمز ویژنر[2] برای رمزنگاری قسمت‌های تقسیم‌بندی شده استفاده خواهد گردید.

۲-۲ ساختار الگوریتم رمزنگاری بر اساس نقشه آشوب

در اوایل سال ۱۹۸۹، Matthew یک الگوریتم رمزنگاری را بر اساس نقشه آشوب لجستیک[3] پیشنهاد داد [۱۴] و در سال ۱۹۹۸، Fridrich برای اولین بار معماری جایگشت- انتشار[4] رمزگذاری تصویر را مبتنی بر نقشه‌های آشفته پیشنهاد داد [۱۵]. امروزه از نقشه آشوب در الگوریتم‌های متفاوتی استفاده می‌شود. در ادامه چندین نوع از الگوریتم‌های پیشنهاد داده شده در زمینه نقشه آشوب را بررسی می‌کنیم.

۱) در [۱۶] الگوریتم‌های آشوب لجستیک دوبعدی و جریان رمز[5] ترکیب‌شده و برای رمزنگاری DICOM پیشنهاد داده شده است.

۲) در [۱۷] تصاویر پزشکی DICOM در بلاک‌های ۱۶ پیکسل در ۱۶ پیکسل تقسیم‌بندی خواهند شد و سپس از الگوریتم لجستیک برای رمزنگاری هر بلاک از تصویر استفاده می‌شود.

۳) در [۱۸] تصاویر پزشکی DICOM با استفاده از ترکیب الگوریتم‌های نگاشت آشوب لجستیک و معماری انتشار جایگشت به شکل کلاسیک[6] رمزنگاری می‌شوند.

۴) در [۱۹] تصاویر پزشکی DICOM با استفاده از ترکیب الگوریتم‌های نگاشت آشوب سه‌بعدی[7]، الگوریتم دوبعدی Arnold cat map، الگوریتم لجستیک یک‌بعدی[8] و الگوریتم دوبعدی Henon map صورت خواهد گرفت.

۵) محاسبات و پردازش بر مبنای ساختار DNA موازی‌سازی قوی داشته و ویژگی‌هایی مثل مصرف انرژی کم و ظرفیت ذخیره‌سازی اطلاعات زیاد را شامل می‌شود. ترکیبی از محاسبات DNA و سیستم‌های آشوب می‌تواند سیستم رمزنگاری قوی‌ای را فراهم آورد [۲۰] و [۲۱]. در سال‌های اخیر تحقیقات زیادی همچون [۱۸] و [۲۲] تا [۲۸] بر اساس این موضوع پیشنهادهای خود را ارائه داده‌اند.

۳- روش پیشنهادی

در این پژوهش برای افزایش امنیت و صحت داده در تصاویر پزشکی DICOM و جلوگیری از دسترسی غیرمجاز به این تصاویر، یک الگوریتم ترکیبی رمزنگاری مطرح گردیده است. الگوریتم پیشنهاد داده شده دارای سه بخش کلی بوده و هر سه بخش پیشنهاد داده شده برای فرایند رمزنگاری و رمزگشایی، به اطلاعات بیومتریک بیمار وابستگی دارند. الگوریتم رمزنگاری روش پیشنهاد داده شده در شکل ۳ آمده و ساختار گرافیکی روندنمای الگوریتم طراحی‌شده در شکل با استفاده از نرم‌افزار Micosoft visio است.

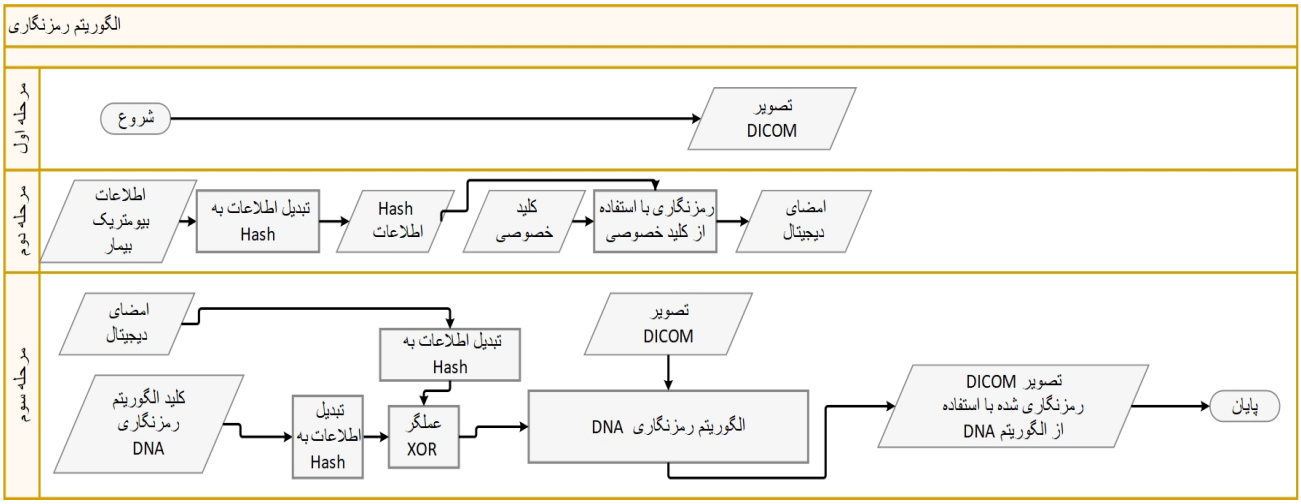
الگوریتم در سه بخش کلی تقسیم‌بندی می‌شود و در ادامه با توجه به ساختار الگوریتم پیشنهاد داده شده، هر یک از بخش‌ها به شکل دقیق توضیح داده خواهند شد:

۱) در بخش اول تصویر DICOM از طرف بیمار دریافت خواهد شد. در این بخش فرمت تصویر DICOM دریافت‌شده از طرف بیمار BMP[9] است.

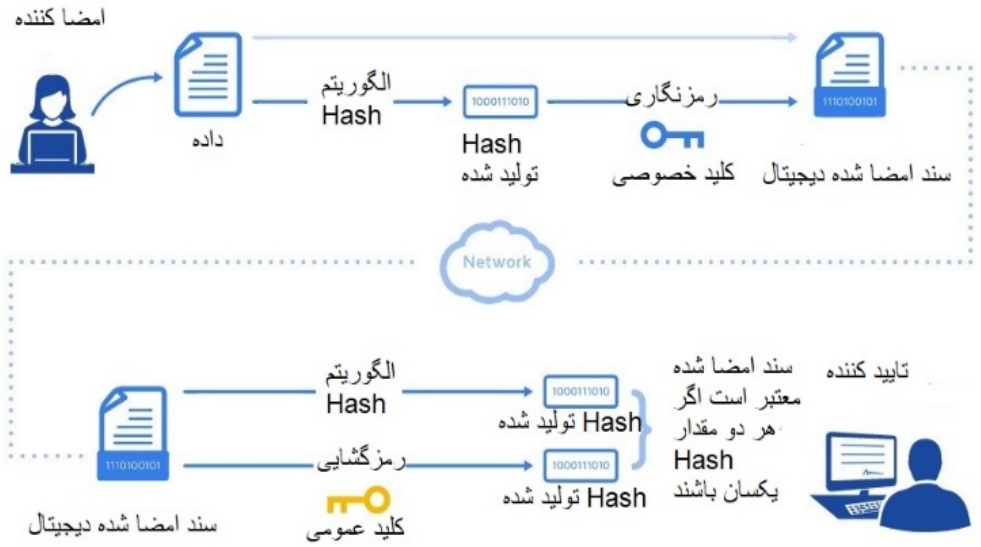
۲) در بخش دوم تأیید اعتبار با استفاده از امضای دیجیتال صورت خواهد پذیرفت.

به‌طور خلاصه با توجه به شکل ۴ می‌توان فرایند امضای دیجیتال را در دو بخش قرار داد. بخش اول ایجاد امضای دیجیتال و ارسال پیغام به همراه امضا است که توسط فرستنده پیغام انجام می‌شود. بخش دوم بازبینی

1. Hash Function
2. Vigenere Cipher
3. Logistic Chaotic Map
4. Permutation-Diffusion Architecture
5. Stream Cipher
6. Classical Permutation-Diffusion
7. Three Chaotic Systems
8. 1D Logistic Map
9. The BMP file format, also known as bitmap image file.



شکل ۳: فرایند اجرا در الگوریتم رمزنگاری پیشنهاد داده شده.



شکل ۴: فرایند اجرا در امضای دیجیتال [۲۹].

پیغام و امضا برای تأیید آن است که توسط گیرنده پیغام انجام می‌شود. در بخش اول الگوریتم امضای دیجیتال فرد امضاکننده به کمک تابع درهم‌سازی، چکیده پیام خود را محاسبه می‌کند که برای هر پیام، مقدار به‌دست‌آمده از تابع درهم‌سازی مقدار یکتایی است. در مرحله بعد فرستنده باید چکیده به‌دست‌آمده از پیام را به شکل رمزشده درآورد. از الگوریتم رمزنگاری نامتقارن[1] برای ایجاد رمز از پیام استفاده می‌شود [۲۹]. الگوریتم الگوریتم رمزنگاری نامتقارن دارای ۳ بخش برای تولید کلید، ایجاد رمز و رمزگشایی است. امضاکننده به کمک الگوریتم تولید کلید، دو کلید عمومی[2] و خصوصی[3] را به دست می‌آورد. کلید خصوصی کاملاً محرمانه است و نزد فرستنده نگهداری می‌شود و کلید عمومی باید در دسترس افرادی که امضا را دریافت می‌کنند، قرار گیرد [۳۰].

چکیده با استفاده از کلید خصوصی و یک الگوریتم رمزنگاری نامتقارن به یک عبارت رمزی تبدیل می‌شود. رمز به‌دست‌آمده در این مرحله همان امضای دیجیتال است که به همراه پیام و کلید عمومی به گیرنده پیام ارسال می‌شود [۳۱].

شکل ۴ [۳۰] و [۳۱] این فرایند را نشان می‌دهد. در بخش دوم از فرایند امضا، فردی که امضا را دریافت کرده است ابتدا مقدار درهم‌سازی پیام دریافتی را به کمک تابع درهم‌سازی که فرستنده استفاده کرده است، به دست می‌آورد.

در مرحله در مرحله‌ی تایید مدرک امضاشده، امضای دیجیتال را که یک عبارت رمزی است به کمک کلید عمومی و الگوریتم رمزگشایی به چکیده پیام تبدیل می‌کند. چکیده‌ای که از رمزگشایی به دست می‌آید با چکیده تابع درهم‌سازی مقایسه می‌شود و در صورتی که این دو مقدار برابر باشند، امضا و پیام، صحیح و مورد تأیید است. اگر پیام یا امضا توسط فرد دیگری تغییر کرده باشد، مقدار چکیده‌های به‌دست‌آمده یکسان نخواهد بود زیرا مقدار درهم‌سازی برای هر پیام منحصربه‌فرد است [۳۱].

فرایند امضای دیجیتال در شکل ۴ نشان داده شده است. با توجه به شکل در الگوریتم پیشنهاد داده شده در مرحله دوم برای ساخت امضای دیجیتال، کلید خصوصی و اطلاعات بیومتریک بیمار دریافت خواهد شد؛ به عبارت دیگر در این بخش اطلاعات بیومتریک بیمار مانند تصویر اثر انگشت و یا تصویر عنبیه چشم از ورودی دریافت خواهد شد.

علت اصلی استفاده از اثر انگشت بیمار بر مبنای منحصربه‌فردی این اطلاعات خواهد بود. دلیل این ویژگی، الگوهای خط و شیارهایی است که در تمامی قسمت‌های انگشت وجود دارد. این خطوط برجسته روی انگشت را خطوط اصطکاکی می‌نامیم که به‌وسیله همین خطوط اصطکاکی، هویت

1. Asymmetric Cryptography
2. Public Key
3. Private Key

افراد تشخیص داده می‌شود؛ زیرا این خطوط برای هر یک از انگشتان دست هر فرد منحصربه‌فرد و غیرقابل تغییر است. به طور کلی الگوهای اصلی اثر انگشت به سه دسته کمانی، حلقه‌ای و مارپیچی تقسیم می‌شوند که توسط این الگوها می‌توان خصوصیاتی از قبیل مینوشیا[1] را دریافت نمود. به محل‌هایی که خطوط اصطکاکی ناگهان قطع یا به دو یا چند شاخه تقسیم شده‌اند مینوشیا می‌گویند که این نقاط برای تفکیک کاربران مختلف مورد استفاده قرار می‌گیرد [۳۲]. از دیگر اطلاعات بیومتریک بیمار می‌توان به عنبیه چشم بیمار اشاره کرد. عنبیه انسان دارای ساختار منحصربه‌فردی است؛ به‌گونه‌ای که هر عنبیه هر چشم دارای ساختار متفاوتی است. با توجه به منحصربه‌فردی ساختار عنبیه و همچنین عدم تغییرپذیری و ثبات آن در طول زمان، استفاده از این شیوه برای احراز هویت مورد استقبال قرار گرفته است [۳۳] و [۳۴].

اطلاعات بیومتریک بیمار با استفاده از تابع هش، هش خواهد شد و نتیجه اطلاعات هش‌شده با کلید خصوصی الگوریتم RSA رمزنگاری می‌شود و امضای دیجیتال را خواهد ساخت.

۳) در این بخش از الگوریتم آشوب DNA برای رمزنگاری تصویر DICOM دریافت‌شده استفاده خواهد گردید.

کلید استفاده‌شده برای الگوریتم DNA به امضای دیجیتال مرحله شماره دوم وابسته خواهد بود به‌گونه‌ای که نتیجه هش شده امضا با نتیجه هش کلید الگوریتم DNA، XOR خواهد شد و نتیجه XOR کلید نهایی الگوریتم DNA را خواهد ساخت.

ساختار الگوریتم رمزنگاری پیشنهاد داده شده به شکل شبه‌کد:

```
1. START
2. PROGRAM DICOM_Encryption
3. DISPLAY "ENTER THE DICOM IMAGE:"
4. Create variable DICOM
5. READ INPUT into DICOM
6. Create variable Patient_Biometric_Information
7. Create variable Hash_result_of_the_Patient_Biometric_Information
8. DISPLAY "ENTER THE Patient Biometric Information:"
9. READ INPUT into Patient_Biometric_Information
10. FUNCTION Patient_Biometric_Information_Hash
11.     Pass IN: Patient_Biometric_Information
12.     Pass Out: Hash_result_of_the_Patient_Biometric_Information
13. END FUNCTION
14. CALL: Patient_Biometric_Information_Hash
15. Create variable Private_Key
16. Create variable Digital_Signature
17. DISPLAY "ENTER THE private key:"
18. READ INPUT into Private_Key
19. FUNCTION Digital Signature
20.     Pass IN: Private Key
21.     Pass IN: Hash_result_of_the_Patient_Biometric_Information
22.     Pass Out: Digital_Signature
23. END FUNCTION
24. CALL: Digital Signature
25. Create variable DNA_Key
26. Create variable Hash_result_of_the_DNA_Key
27. DISPLAY "ENTER THE DNA key:"
28. READ INPUT into DNA_Key
29. FUNCTION DNA_Key_Hash
30.     Pass IN: DNA_Key
31.     Pass Out: Hash_result_of_the_DNA_Key
32. END FUNCTION
33. Create variable: Digital_Signature
34. Create variable: Hash_result_of_the_Digital_Signature
35. DISPLAY "ENTER THE Digital signature:"
36. READ INPUT into Digital_Signature
37. FUNCTION Digital_Signature_Hash
38.     Pass IN: Digital_Signature
39.     Pass Out: Hash_result_of_the_Digital_Signature
40. END FUNCTION
41. Call: DNA_Key_Hash
42. Call: Digital_Signature_Hash
43. Create variable XOR_Result
44. FUNCTION XOR
45.     Pass IN: Hash_result_of_the_DNA_Key
46.     Pass IN: Hash_result_of_the_Digital_Signature
47.     Pass Out: XOR_Result
48. END FUNCTION
49. Call: XOR
50. Create variable Encrypted_Image
51. FUNCTION DNA_Encryption
52.     Pass IN: XOR_Result
53.     Pass IN: DICOM
54.     Pass Out: Encrypted_Image
55. END FUNCTION
56. END
```

٤- تحلیل و ارزیابی

در تحلیل و ارزیابی دقیق، لازم است تعدادی از عوامل مورد نیاز در مشخص‌شدن کیفیت الگوریتم‌های رمزنگاری تصویر معرفی شوند.

۱) مدل رنگی RGB[2]: در RGB رنگ‌ها با ترکیب‌کردن نورهای آبی، سبز و قرمز ایجاد می‌شوند. فرایند ایجاد رنگ‌ها با توجه به تنوعی که می‌توان در رنگ‌های استفاده‌شده دریافت کرد بسیار زیاد است و با این سه رنگ اصلی می‌توان میلیون‌ها ترکیب رنگی جدید ایجاد نمود [۳۵] و [۳۶].

۲) Histogram: این پارامتر، یک نمودار ساده است و نشان می‌دهد که سطوح مختلف روشنایی موجود در صحنه (از تاریک‌ترین تا روشن‌ترین سطح)، در چه محدوده‌ای واقع شده‌اند. هرچه Histogram یک تصویر رمزنگاری‌شده بیشتر مسطح باشد نشان‌دهنده عملکرد بهتر الگوریتم رمزنگاری است [۳۵] و [۳۶].

۳) MSE[3]: خطای میانگین مربع مشخص‌کننده میزان تفاوت تصویر رمزنگاری‌شده با تصویر اصلی است. هرچه مقدار MSE بیشتر باشد عملکرد الگوریتم رمزنگاری بهتر بوده است [۳۵] و [۳۶]. در (۱) محاسبه MSE نشان داده شده است

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j)-K(i,j)]^2 \qquad (1)$$

که در آن I مقادیر پیکسل[4] تصویر اصلی، K مقادیر پیکسل تصویر رمزنگاری‌شده، (i,j) موقعیت پیکسل‌ها و m و n ابعاد تصویر هستند. در زمانی می‌توان گفت سامانه رمزنگاری موفق عمل کرده که تصویر رمزنگاری‌شده دارای میانگین خطای مربعات زیاد و ماکسیمم نسبت سیگنال به نویز کم باشد [۳۵] و [۳۶].

۴) PSNR[5]: پارامتر ماکسیمم نسبت سیگنال به نویز، پارامتری است که برای اندازه‌گیری کیفیت کمّی تصویر دیجیتال استفاده می‌شود. هرچه مقدار PSNR کمتر باشد عملکرد الگوریتم رمزنگاری بهتر بوده است [۳۵] و [۳۶]. در رابطه زیر محاسبه PSNR نشان داده شده است

$$PSNR = 10\log_{10}\frac{MAX^2}{MSE} \qquad (2)$$

در (۲)، MAX معرف بیشترین مقدار پیکسل موجود در تصویر است.

1. Minutiae

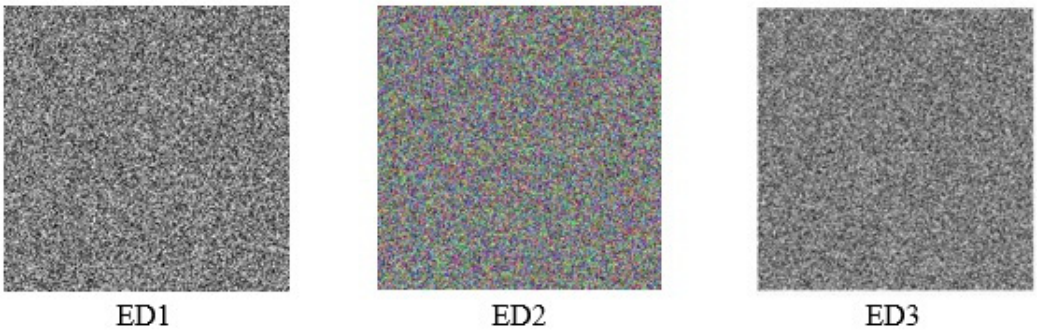
2. Red, Green, Blue

3. Mean Square Error

4. Pixel

5. Peak Signal to Noise Ratio

شکل ۵: نمونه تصاویر DICOM انتخاب‌شده برای رمزنگاری.



شکل ۶: خروجی رمزنگاری تصاویر DICOM.

۵) NPCR[1]: نرخ تعداد پیکسل‌های تغییریافته تصویر رمز را در حالتی محاسبه می‌کند که تصاویر اصلی آنها در یک پیکسل با هم تفاوت دارند.

دو تصویر C و C' را که تصویر اصلی آنها در یک پیکسل با هم اختلاف دارند در نظر بگیرید. W و H به ترتیب عرض و ارتفاع تصاویر هستند [۳۵] و [۳۶]. در (۳) محاسبه $NPCR$ نشان داده شده است

$$NPCR = \frac{۱۰۰}{W \times H} \sum_{i=۰}^{H-۱} \sum_{j=۰}^{W-۱} D(i,j) \qquad (۳)$$

$$D(i,j) = \begin{cases} ۰ & , \text{ if } C(i,j) = C'(i,j) \\ ۱ & , \text{ if } C(i,j) \neq C'(i,j) \end{cases} \qquad (۴)$$

۶) $UACI$[2]: این معیار امنیتی بیانگر میانگین یکنواخت تغییر شدت است و هرچه مقدار $UACI$ بیشتر باشد، الگوریتم رمزنگاری عملکرد بهتری دارد [۳۵] و [۳۶]. در (۵) محاسبه $UACI$ آمده است

$$UACI = \frac{۱}{W \times H} [\sum_{i,j} \frac{[C_۱(i,j) - C_۲(i,j)]}{۲۵۵}] \times ۱۰۰\% \qquad (۵)$$

که H و W طول و عرض تصاویر و $C_۱$ و $C_۲$ دو تصویر رمزنگاری‌شده هستند که از دو تصویر با یک پیکسل اختلاف گرفته شده‌اند.

۷) Entropy: این معیار امنیتی یکی از خصوصیت‌های برجسته برای تصادفی‌بودن است. آنتروپی اطلاعات یک تئوری ریاضی برای ارتباط داده و ذخیره‌سازی است که توسط Claude E Shannon در سال ۱۹۴۹ معرفی شده [۳۷] تا [۳۹] و می‌تواند به‌عنوان معیاری برای به‌دست‌آوردن میزان آشفتگی سطوح خاکستری پیکسل‌ها استفاده شود. Entropy یک تصویر از (۶) محاسبه می‌شود

$$H(m) = \sum_{i=۰}^{۲^n-۱} \mathrm{P}(m_i) \log_۲ \frac{۱}{\mathrm{P}(m_i)} \qquad (۶)$$

در این رابطه $\mathrm{P}(m_i)$ احتمال وقوع سطح خاکستری m_i و ۲^n تعداد سطوح خاکستری ممکن است.

در یک تصویر غیریکنواخت که احتمال وقوع تمام پیکسل‌ها یکسان است، مقدار Entropy بیشترین مقدار خود یعنی ۸ خواهد بود که این به معنای وجود بیشترین بی‌نظمی در میان پیکسل‌های تصویر است. نزدیک‌بودن مقدار Entropy تصویر رمزشده به ۸ به‌منزله کارایی روش ارائه‌شده در رمزنگاری است [۴۰] و [۴۱]. برای جلوگیری از انواع حملات مختلف باید تضمین شود که تصویر اصلی و تصویر رمزنگاری‌شده هیچ گونه تشابه آماری نداشته باشند. تحلیل Histogram، چگونگی توزیع پیکسل‌ها را در تصویر با استفاده از ترسیم تعداد مشاهدات هر میزان از شدت روشنایی‌ها بیان می‌کند. توزیع به نسبت یکنواخت تصویر، نشان‌دهنده کیفیت خوب روش رمزنگاری است [۴۰] تا [۴۳]. در این پژوهش، جامعه آماری بر اساس تصاویر DICOM [۴۴] و [۴۵] انتخاب گردیده و بر اساس الگوریتم پیشنهاد داده شده، چندین تصویر DICOM بر اساس پارامترهای Entropy، MSE، PSNR، NPCR، UACI، Elapsed time و Histogram مورد ارزیابی قرار خواهند گرفت.

مشخصات سیستم استفاده‌شده برای ارزیابی:

CPU : Intel Core i۷ , ۲٫۱۰ GHz
RAM : ۸ GB
Operator system : Microsoft Windows ۱۰
System type : ۶۴ bit
Simulation software and programming language : MATLAB (R۲۰۱۶b), Python

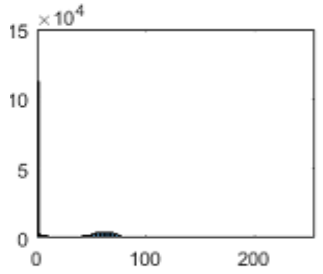
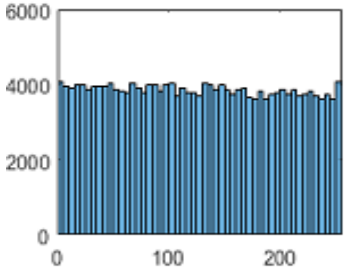
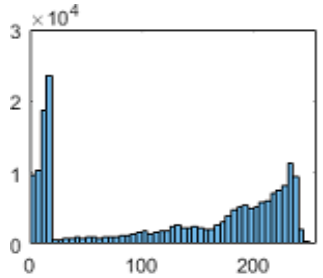
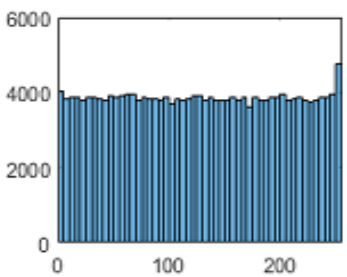
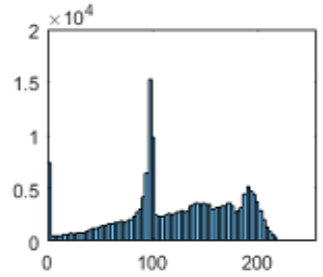
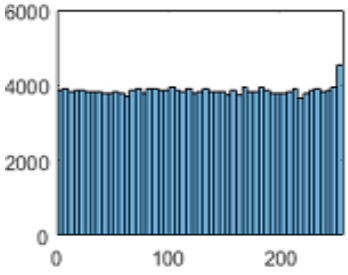
با توجه به الگوریتم پیشنهاد داده شده در این مقاله و شکل‌های ۵ و ۶ برای ارزیابی، تصاویر D۱، D۲ و D۳ به‌عنوان نمونه تصاویر DICOM انتخاب شده‌اند. همچنین تصاویر ED۱، ED۲ و ED۳ به‌ترتیب خروجی نهایی رمزنگاری تصاویر D۱، D۲ و D۳ خواهند بود. مهم‌ترین دلیل استفاده از این تصاویر به دلیل استفاده مکرر آنها برای ارزیابی در مقالات مربوط به رمزنگاری DICOM در سال‌های اخیر بوده است.

1. Number of Pixel Change Rate
2. Unified Average Changing Intensity

جدول ۱: پارامترهای نهایی تصاویر رمزنگاری‌شده.

تصویر	تصویر رمزنگاری‌شده	مدت زمان رمزنگاری (S)	Entropy (bits/pixel)	MSE	PSNR	UACI (%)	NPCR (%)
D۱	ED۱	۲۳٫۹۸۰۳۸۲۴۴۲۴۷۴۳۶۵	۷٫۹۹۷۷۰۶۳۷۳۹۵۵۰۹۹	۱٫۶۷۷۱۱۱۲۴۶۷۴۴۷۹۱e+۰۴	۵٫۸۸۵۱۸۴۸۹۵۲۸۹۸۵۴	۴۲٫۲۵۵۳۱۸۱۶۴۸۲۵۴	۹۹٫۵۸۸۰۱۲۶۹۵۳۱۲۵
D۲	ED۲	۲۹٫۱۲۵۹۱۱۴۷۴۲۲۷۹۰۵	۷٫۹۹۸۹۷۲۷۷۹۴۲۶۱۸۹	۱٫۳۵۹۲۲۵۸۴۷۳۷۱۴۲۰e+۰۴	۶٫۷۹۷۸۸۷۳۶۲۷۸۲۲۳۱	۳۷٫۳۹۹۹۷۱۴۸۵۱۳۷۹	۹۹٫۶۰۹۸۸۳۶۲۶۳۰۲۱
D۳	ED۳	۲۹٫۴۵۳۴۰۷۷۶۴۴۳۴۸۱۴	۷٫۹۹۹۰۰۸۷۳۸۰۶۰۷۹۳	۸٫۳۹۷۸۲۹۳۱۵۱۸۵۵۴۹e+۰۳	۸٫۸۸۹۱۳۳۱۷۴۵۶۴۸۳۸	۲۹٫۴۷۶۲۶۹۰۸۶۲۰۲۰	۹۹٫۶۱۶۴۹۵۷۶۸۲۲۹۲

جدول ۲: HISTOGRAM تصاویر D۱، D۲ و D۳ قبل از رمزنگاری و بعد از رمزنگاری.

تصویر	Histogram تصویر قبل از رمزنگاری	Histogram تصویر بعد از رمزنگاری
D۱		
D۲		
D۳		

٤-۱ تمایز بین تصویر اصلی و تصویر رمز

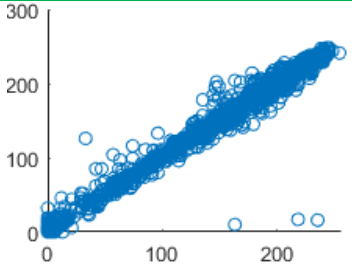
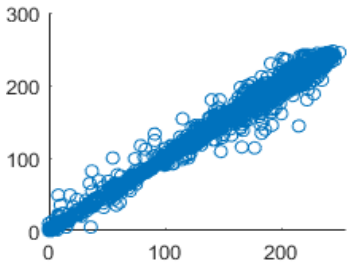
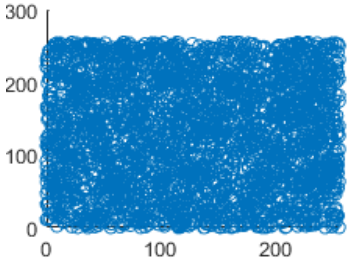
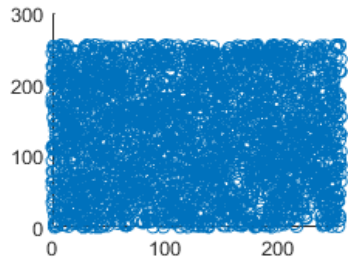
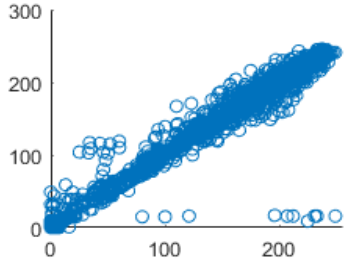
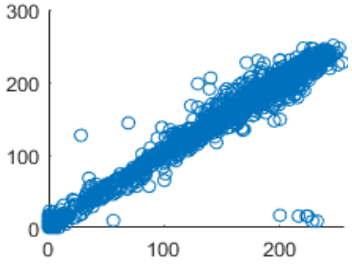
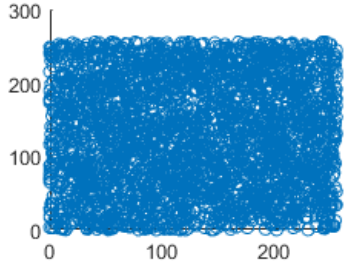
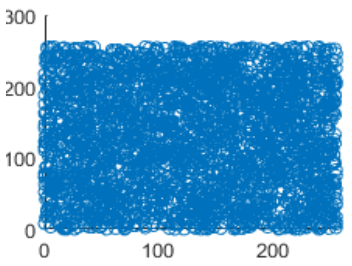
به‌طور کلی یک خاصیت مناسب برای یک تصویر رمز، حساس‌بودن نسبت به تغییرات جزئی در تصویر اصلی، یعنی فقط تغییر یک پیکسل است. برای آزمودن اثر تغییر یک پیکسل ورودی روی تمام تصویر رمزشده به‌وسیله الگوریتم پیشنهادی، معیارهای Entropy، MSE، PSNR، UACI، NPCR و Histogram مورد بررسی قرار داده می‌شوند. در جدول ۱ پارامترهای نهایی Entropy، MSE، PSNR، UACI و NPCR تصاویر رمزنگاری‌شده آمده است.

با توجه به تعاریف معیارهای Entropy، MSE، PSNR، UACI و NPCR می‌توان در جدول ۱ نزدیک‌بودن مقدار Entropy تصویر رمزشده به ۸ را به‌منزله کارایی روش ارائه‌شده در رمزنگاری [۴۰] و [۴۱] مشاهده کرد. همچنین برای تعیین میزان تأثیر تغییرات جزئی پیکسل‌های تصویر ورودی روی پیکسل‌های تصویر خروجی از معیارهای NPCR و UACI استفاده خواهد شد.

باید توجه داشت که حداکثر مقدار نظری NPCR برابر ۱۰۰٪ است و هرچه مقدار NPCR بزرگ‌تر باشد، تغییرات پیکسل بیشتر است [۴۶]. دو معیار MSE و PSNR از معیارهای متداول جهت اندازه‌گیری کیفیت یک الگوریتم رمزنگاری می‌باشد که بر اساس این دو معیار، هرچه MSE بین دو تصویر اصلی و رمزشده بزرگ‌تر باشد (به عبارتی دیگر PSNR کوچک‌تر باشد)، بدین معنا خواهد بود که اختلاف بین دو تصویر اصلی و رمزشده زیاد می‌باشد که این حالت نشان‌دهنده یک الگوریتم رمزنگاری مناسب است [۴۷].

در جدول ۲ Histogram تصاویر D۱، D۲ و D۳ قبل از رمزنگاری و بعد از رمزنگاری نشان داده شده است. با توجه به جدول و ویژگی Histogram تصاویر قبل و بعد از رمزنگاری می‌توان نشان داد که سطوح مختلف روشنایی موجود در صحنه از تاریک‌ترین تا روشن‌ترین سطح در چه محدوده‌ای واقع شده‌اند و هرچه Histogram تصویر رمزنگاری‌شده بیشتر مسطح باشد نشان‌دهنده عملکرد بهتر الگوریتم رمزنگاری است [۳۵] و [۳۶].

جدول ۳: ضرایب همبستگی تصویر D۲ قبل از رمزنگاری و بعد از رمزنگاری.

تصویر	Vertical	Horizontal
D۲		
ED۲		
D۲		
ED۲		

٤-۲ تحلیل ضرایب همبستگی

برای نمونه در جدول ۳ همبستگی‌های عمودی[1]، افقی[2]، قطری[3] و ضد قطری[4] تصویر D۲ و ED۲ نشان داده شده است. در داده تصویری هر پیکسل به‌شدت با پیکسل‌های همسایه خودهمبستگی دارد و یک الگوریتم رمزنگاری مناسب باید تصاویر رمزی تولیدکننده که همبستگی بین پیکسل‌های آن کم باشد [۴۰]، [۴۱] و [۴۳].

٤-۳ تحلیل اطلاعات بیومتریک

اطلاعات بیومتریک با توجه به وابسته‌بودن به هر انسان می‌توانند به‌گونه‌ای مستقل برای شناسایی هر فرد استفاده شوند. از جمله اطلاعات بیومتریک می‌توان مواردی مثل اثر انگشت و یا عنبیه چشم را نام برد. در الگوریتم پیشنهادی، امضای دیجیتال ساخته‌شده در قسمت الگوریتم رمزنگاری RSA با توجه به کلید خصوصی و نتیجه هش اطلاعات بیومتریک بیمار ساخته خواهد شد و کلید استفاده‌شده در قسمت الگوریتم رمزنگاری DNA برای استفاده به نتیجه هش اطلاعات بیومتریک بیمار که تصویر DICOM متعلق به او است، وابسته خواهد بود.

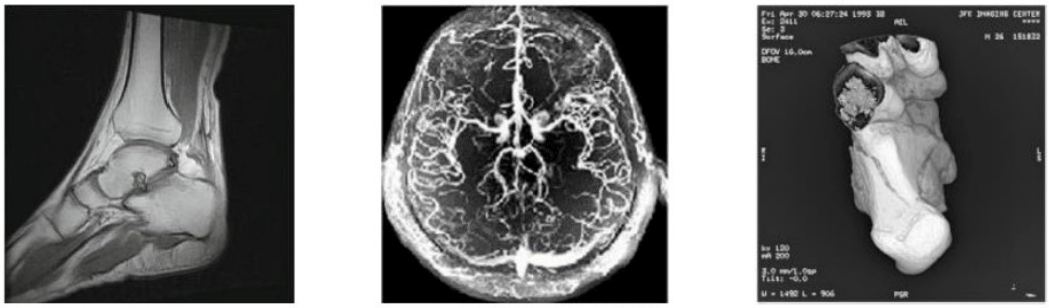
٤-٤ تحلیل فضای کلید

برای جلوگیری از جستجو و یافتن کلید الگوریتم رمزنگاری، فضای کلید الگوریتم رمزنگاری باید به‌اندازه کافی بزرگ باشد. در واقع قدرت اجرای یک حمله جستجو وابسته به فضای کلید است. سازمان NIST[5] حداقل طول کلید ممکن برای برقراری امنیت محاسباتی در برابر حملات جستجو را تا سال ۲۰۱۵، ۸۰ بیت پیش‌بینی کرده است [۴۸].

اگر در الگوریتم رمزنگاری DNA دقت محاسباتی 10^{14} فرض شود [۴۹] تا [۵۱] و از آنجایی که ۴ نوکلئوتید DNA در کلید الگوریتم پیشنهاد

1. Vertical
2. Horizontal
3. Diagonal
4. Anti-Diagonal

5. National Institute of Standards and Technology



D4 D5 D6

شکل ۷: نمونه تصاویر DICOM انتخاب‌شده برای رمزنگاری.

جدول ۴: مقایسه مختصر الگوریتم پیشنهاد داده شده با [۲۳]، [۲۶]، [۵۲] و [۵۳].

الگوریتم / مرجع	Dual hyperchaos map	PWLCM*	نگاشت آشوب یک‌بعدی	نگاشت آشوب دوبعدی	نگاشت آشوب سه‌بعدی	Latin square	Hash function	RSA	Digital signature	Zigzag map	Biometric information	DNA
[۵۳]			✓			✓	✓					
[۲۶]		✓	✓									✓
[۲۳]				✓			✓			✓		✓
[۵۲]	✓											✓
الگوریتم پیشنهادی							✓	✓	✓		✓	✓

* Piecewise Linear Chaotic Map

جدول ۵: مقایسه تصویر DICOM رمزنگاری‌شده با [۲۳]، [۵۳] و [۵۴].

مرجع	تصویر	Entropy (bits/pixel)	UACI (%)	NPCR (%)	Histogram تصویر رمزنگاری‌شده
[۵۳]	D۴	۷٫۹۰۴۵	۳۳٫۴۱	۹۹٫۶۱	H۱
الگوریتم پیشنهاد داده‌شده	D۴	۷٫۹۹۷۹	۳۵٫۷۵	۹۹٫۶۴	H۲
[۲۳]	D۵	۷٫۹۹۶۹	۳۳٫۶۹	۹۹٫۶۰	H۳
الگوریتم پیشنهاد داده‌شده	D۵	۷٫۹۹۷۰	۳۵٫۴۵	۹۹٫۶۱	H۴
[۵۴]	D۶	۷٫۹۴۳۲	NA	۹۹٫۶۵	H۵
الگوریتم پیشنهاد داده‌شده	D۶	۷٫۹۹۹۵	۳۱٫۷۸	۹۹٫۶۹۵	H۶

داده شده در این مقاله ذخیره شده‌اند، فقط در قسمت رمزنگاری DICOM با استفاده از DNA، فضای کلید برای این قسمت برابر است با $(۱۰^{۱۴})^{۴} = ۱۰^{۵۶}$. برای جلوگیری از حملات Brute force علاوه بر بالابودن فضای کلید الگوریتم DNA، قسمت‌های دیگر الگوریتم پیشنهاد داده شده مانند استفاده از الگوریتم RSA برای ساخت امضای دیجیتال، اطلاعات بیومتریک بیمار، عملگر XOR و هش‌شدن تعدادی از کلیدها برای استفاده، بسیار مؤثر خواهند بود.

٤-٥ مقایسه با چندین کار تحقیقاتی بر مبنای الگوریتم مورد استفاده

کار تحقیقاتی انجام‌شده بر اساس الگوریتم پیشنهادی با [۲۳]، [۲۶]، [۵۲] و [۵۳] مقایسه گردیده است. مهم‌ترین دلایل انتخاب این مراجع برای مقایسه در موارد زیر تقسیم‌بندی می‌شوند:

۱) در این مراجع برای رمزنگاری تصاویر DICOM یک الگوریتم ترکیبی پیشنهاد شده است.

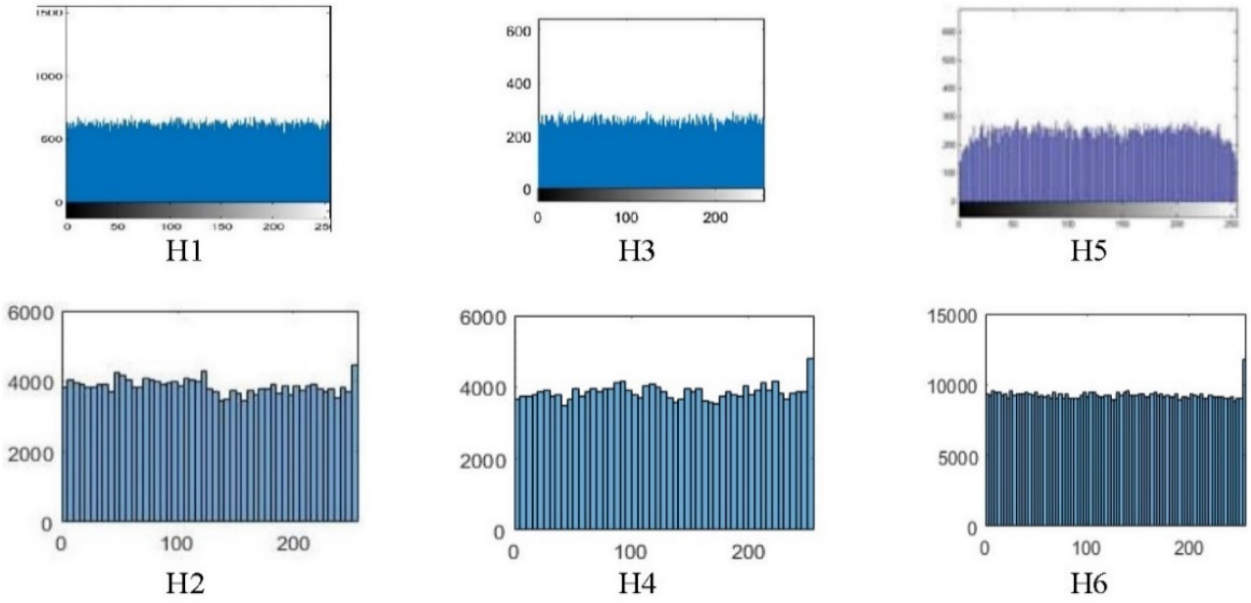
۲) در هر یک از فعالیت‌های تحقیقاتی مورد مقایسه، پارامتر Entropy بالای ۷٫۹۹ بوده و این موضوع نشان‌دهنده طراحی دقیق و مؤثر الگوریتم‌های پیشنهاد داده شده است.

۳) هر یک از این مقالات بعد از سال ۲۰۱۹ در ژورنال‌های معتبر چاپ شده‌اند و همچنین برای طراحی از جدیدترین الگوریتم‌های آشوب نیز استفاده کرده‌اند. در جدول ۴، الگوریتم پیشنهاد داده شده با هر یک از [۲۳]، [۲۶]، [۵۲] و [۵۳] به شکل مختصر مورد مقایسه قرار داده شده است.

سرستون‌های انتخاب‌شده در جدول ۴ بر مبنای الگوریتم‌هایی است که در این مقالات بیشترین تأثیر را در جلوگیری از حملات Brute force و ارتقای فضای کلید داشته‌اند.

٤-٦ مقایسه با چندین کار تحقیقاتی بر مبنای نتایج خروجی

در شکل ۷ نمونه تصاویر DICOM انتخاب‌گردیده برای رمزنگاری و تحلیل بر اساس پارامترهای جدول ۵ نشان داده شده است. در شکل ۸، Histogram تصاویر رمزنگاری‌شده با استفاده از روش پیشنهادی در این مقاله و سایر مقالات آمده است. در جدول ۵ کار تحقیقاتی پیشنهادی با [۲۳]، [۵۳] و [۵۴] مقایسه شده‌اند. با توجه به نتایج حاصل از مقایسه الگوریتم پیشنهادی با آزمون‌های استاندارد مثل Entropy، Histogram و غیره و نتایج حاصل از این آزمون‌ها از قبیل نزدیک‌بودن میزان بی‌نظمی به عدد ۸ و مسطح‌بودن Histogram تصویر رمزنگاری‌شده، همگی کارآمدی سیستم رمزنگاری پیشنهادی را به‌وضوح نشان می‌دهند.



شکل ۸: Histogram تصاویر رمزنگاری‌شده.

۵- نتیجه‌گیری

امروزه برای رمزنگاری تصاویر پزشکی با توجه به اهمیت موضوع امنیت و صحت داده در مدارک پزشکی، الگوریتم‌های متنوعی پیشنهاد شده است. در این مقاله با توجه به ویژگی‌های الگوریتم رمزنگاری DNA، امضای دیجیتال و اطلاعات بیومتریک بیمار، نوعی از الگوریتم‌های رمزنگاری ترکیبی، طراحی و پیشنهاد گردیده که دارای سه قسمت اصلی بر مبنای رمزنگاری تصاویر DICOM می‌باشد. قسمت اول بر اساس دریافت یک تصویر استاندارد DICOM از ورودی است. قسمت دوم الگوریتم بر اساس دریافت اطلاعات بیومتریک بیمار و ساخت امضای دیجیتال با استفاده از یک کلید خصوصی و نتیجه هش‌شده داده بیومتریک بیمار است. در قسمت سوم تصویر DICOM دریافت‌شده از ورودی توسط الگوریتم رمزنگاری DNA رمزنگاری خواهد گردید. در مرحله سوم، کلید استفاده‌شده در الگوریتم DNA بر اساس نتیجه XOR، هش‌شده امضای دیجیتال و هش‌شده کلید اولیه الگوریتم DNA است. نتایج به‌دست‌آمده از آزمون بصری و تحلیل Histogram نشان دادند که در تصاویر رمزنگاری‌شده هیچ گونه الگو و ناحیه بافت قابل تشخیص نیست و همچنین هیچ گونه شباهت آماری و بین ظاهر تصویر اصلی و تصویر رمزنگاری‌شده وجود ندارد. جهت ارزیابی الگوریتم پیشنهادی از آزمون‌های استانداردی مثل Entropy، Histogram، NPCR، UACI، PSNR و MSE استفاده شده که نتایج حاصل از آنها از قبیل نزدیک‌بودن میزان بی‌نظمی به عدد ۸، همگی کارآمدی سیستم رمزنگاری پیشنهادی را به‌وضوح نشان می‌دهند. در الگوریتم پیشنهادی، وابستگی امضای دیجیتال و کلید الگوریتم رمزنگاری DNA به اطلاعات بیومتریک بیمار، موجب افزایش امنیت و صحت داده در تصاویر پزشکی DICOM خواهد شد. در مقالات بعدی تصمیم بر آن است که برای مقاومت بالاتر در مقابل حملات Brute force و افزایش فضای کلید و حساسیت بالاتر[1] نسبت به تغییر کلید، به‌گونه‌ای الگوریتم رمزنگاری ترکیبی طراحی گردد تا بتوان در الگوریتم طراحی‌شده از الگوریتم رمزنگاری RNA[2] نیز استفاده کرد.

1. Key Sensitivity
2. Ribonucleic Acid

مراجع

[1] J. Andersen, B. Lo, and G. Z. Yang, "Experimental platform for usability testing of secure medical sensor network protocols," in *Proc. 5th Int. Summer School and Symp. on Medical Devices and Biosensors,* pp. 179-182, Hong Kong, China, 1-3 Jun. 2008.

[2] C. C. Lin, *et al*., "A healthcare integration system for disease assessment and safety monitoring of dementia patients," *IEEE Trans. on Information Technology in Biomedicine*, vol. 12, no. 5, pp. 579-586, Sept. 2008.

[3] -, *Encryption, Google Trends*, https://www.google.com/trends (accessed).

[4] F. Ayankoya and B. Ohwo, "Brute-force attack prevention in cloud computing using one-time password and cryptographic hash function," *International J. of Computer Science and Information Security*, vol. 17, no. 2, pp. 7-19, Feb. 2019.

[5] E. Tirado, *et al*., "A new distributed brute-force password cracking technique," in *Proc. Int. Conf. on Future Network Systems and Security, Springer*, vol. 878, pp. 117-127, Jun. 2018.

[6] "DICOM Conformance Tests," *Aliza Medical Imaging*. https://www.aliza-dicom-viewer.com/ (accessed), 2022.

[7] B. Zhang, B. Rahmatullah, S. L. Wang, A. Zaidan, B. Zaidan, and P. Liu, "A review of research on medical image confidentiality related technology coherent taxonomy, motivations, open challenges and recommendations," *Multimedia Tools and Applications*, vol. 82, pp. 21867-21906, Aug. 2023.

[8] S. H. Shin, W. S. Yoo, and H. Choi, "Development of modified RSA algorithm using fixed mersenne prime numbers for medical ultrasound imaging instrumentation," *Computer Assisted Surgery*, vol. 24, no. 2, pp. 73-78, Oct. 2019.

[9] Q. Natsheh, B. Li, and A. G. Gale, "Security of multi-frame DICOM images using XOR encryption approach," *Procedia Computer Science*, vol. 90, no. 1, pp. 175-181, Jul. 2016.

[10] R. M. Kumar and M. Viswanath, "A symmetric medical image encryption scheme based on irrational numbers," *Biomedical Research*, vol. 1, no. 5, pp. 494-498, Jan. 2018.

[11] O. Dorgham, B. Al-Rahamneh, A. Almomani, and K. F. Khatatneh, "Enhancing the security of exchanging and storing DICOM medical images on the cloud," *International J. of Cloud Applications and Computing*, vol. 8, no. 1, pp. 154-172, Jan. 2018.

[12] A. Al-Haj, G. Abandah, and N. Hussein, "Crypto-based algorithms for secured medical image transmission," *IET Information Security*, vol. 9, no. 6, pp. 365-373, Mar. 2015.

[13] P. Subhasri and A. Padmapriya, "Enhancing the security of DICOM content using modified vigenere cipher," *International J. of Applied Engineering Research*, vol. 10, no. 55, pp. 1951-1956, Jan. 2015.

[14] R. Matthews, "On the derivation of a "chaotic" encryption algorithm," *Cryptologia*, vol. 13, no. 1, pp. 29-42, Jan. 1989.

[15] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *International J. of Bifurcation and Chaos*, vol. 8, no. 6, pp. 1259-1284, Jun. 1998.
[16] S. M. Ismail, L. A. Said, A. G. Radwan, A. H. Madian, and M. F. Abu-Elyazeed, "Generalized double-humped logistic map-based medical image encryption," *J. of Advanced Research*, vol. 10, no. 1, pp. 85-98, Mar. 2018.
[17] R. Gupta, R. Pachauri, and A. K. Singh, "An effective approach of secured medical image transmission using encryption method," *Molecular & Cellular Biomechanics*, vol. 15, no. 2, pp. 63-83, May 2018.
[18] M. M. Parvees, J. A. Samath, and B. P. Bose, "Protecting large size medical images with logistic map using dynamic parameters and key image," *Int. J. Netw. Secur.*, vol. 19, no. 6, pp. 984-994, Jan. 2017.
[19] Y. Dai, H. Wang, and Y. Wang, "Chaotic medical image encryption algorithm based on bit-plane decomposition," *International J. of Pattern Recognition and Artificial Intelligence*, vol. 30, no. 4, Article ID: 1657001, May 2016.
[20] X. Li, L. Wang, Y. Yan, and P. Liu, "An improvement color image encryption algorithm based on DNA operations and real and complex chaotic systems," *Optik*, vol. 127, no. 5, pp. 2558-2565, Mar. 2016.
[21] Q. Zhang, L. Guo, and X. Wei, "Image encryption using DNA addition combining with chaotic maps," *Mathematical and Computer Modelling*, vol. 52, no. 11, pp. 2028-2035, Dec. 2010.
[22] A. Belazi, M. Talha, S. Kharbech, and W. Xiang, "Novel medical image encryption scheme based on chaos and DNA encoding," *IEEE Access*, vol. 7, pp. 36667-36681, 2019.
[23] J. C. Dagadu, J. P. Li, and E. O. Aboagye, "Medical image encryption based on hybrid chaotic DNA diffusion," *Wireless Personal Communications*, vol. 108, no. 1, pp. 591-612, Apr. 2019.
[24] R. S. Devi, K. Thenmozhi, J. B. B. Rayappan, R. Amirtharajan, and P. Praveenkumar, "Entropy influenced RNA diffused quantum chaos to conserve medical data privacy," *International J. of Theoretical Physics*, vol. 58, no. 6, pp. 1937-1956, Mar. 2019.
[25] A. Kumari, B. Akshaya, B. Umamaheswari, K. Thenmozhi, R. Amirtharajan, and P. Praveenkumar, "3D lorenz map governs DNA rule in encrypting DICOM images," *Biomedical and Pharmacology J.*, vol. 11, no. 2, pp. 897-906, Jun. 2018.
[26] P. Praveenkumar, *et al.*, "Transreceiving of encrypted medical image-a cognitive approach," *Multimedia Tools and Applications*, vol. 77, no. 7, pp. 8393-8418, Apr. 2018.
[27] N. Sasikaladevi, K. Geetha, and A. Revathi, "EMOTE-multilayered encryption system for protecting medical images based on binary curve," *J. of King Saud University-Computer and Information Sciences*, vol. 34, no. 3?, pp. 676-686, Mar. 2019.
[28] S. Sheela, K. Suresh, and D. Tandur, "Secured transmission of clinical signals using hyperchaotic DNA confusion and diffusion transform," *International J. of Digital Crime and Forensics*, vol. 11, no. 3, pp. 43-64, Jul. 2019.
[29] N. Yuvaraj, K. Praghash, and T. Karthikeyan, "Data privacy preservation and trade-off balance between privacy and utility using deep adaptive clustering and elliptic curve digital signature algorithm," *Wireless Personal Communications*, vol. 124, pp. 655-670, Nov. 2021.
[30] J. Katz, "Digital signatures,"in *Digital Signatures*, Springer Science & Business Media, pp. 3-33, Jan. 2010.
[31] R. Kaur and A. Kaur, "Digital signature," in *Proc. Int. Conf. on Computing Sciences,* pp. 295-301, Phagwara, India, 14-15 Sept. 2012.
[32] D. M. Davide Maltoni, A. K. Jain, and Salil Prabhakar, *Handbook of Fingerprint Recognition*, Springer London, 2009.
[33] R. Agarwal and A. S. Jalal, "Presentation attack detection system for fake Iris: a review," *Multimedia Tools and Applications*, vol. 80, no. 10, pp. 15193-15214, Feb. 2021.
[34] J. Jayanthi, E. L. Lydia, N. Krishnaraj, T. Jayasankar, R. L. Babu, and R. Suji, "An effective deep learning features based integrated framework for iris detection and recognition," *J. of Ambient Intelligence and Humanized Computing*, vol. 12, no. 3, pp. 3271-3281, Jun. 2021.
[35] R. Amirtharajan, R. Akila, and P. Deepikachowdavarapu, "A comparative analysis of image steganography," *International J. of Computer Applications*, vol. 2, no. 3, pp. 41-47, May. 2010.
[36] T. Morkel, J. H. Eloff, and M. S. Olivier, "An overview of image steganography," *ISSA*, vol. 1, no. 2, pp. 1-11, Jan. 2005.
[37] R. Ahlswede, "A short course on cryptography," in *Hiding Data-Selected Topics: Springer*, vol. 12, pp. 1-54, Apr. 2016.
[38] M. J. Durand-Richard, "Probability, cryptology and meaning in Claude Shannon (1916-2001)'s works," in *Proc. Cryptologic History Symp.: Global Perspectives on Cryptologic History*, 12 pp., Baltimore, Washington, USA,15-16 Oct 2009.
[39] R. G. Gallager, "Claude E. Shannon: A retrospective on his life, work, and impact," *IEEE Trans. on Information Theory*, vol. 47, no. 7, pp. 2681-2695, Nov. 2001.
[40] M. Soltani, "A new secure image encryption algorithm using logical and visual cryptography algorithms and based on symmetric key encryption," *J. of Basic and Applied Scientific Research*, vol. 3, no. 6, pp. 1193-1201, 2013.
[41] M. Soltani and A. K. Bardsiri, "Designing a novel hybrid algorithm for QR-code images encryption and steganography," *J. Comput.*, vol. 13, no. 9, pp. 1075-1088, Sept. 2018.
[42] S. Lian, J. Sun, and Z. Wang, "Security analysis of a chaos-based image encryption algorithm," *Physica A: Statistical Mechanics and its Applications*, vol. 351, no. 2-4, pp. 645-661, Jun. 2005.
[43] O. F. Mohammad, M. S. M. Rahim, S. R. M. Zeebaree, and F. Ahmed, "A survey and analysis of the image encryption methods," *International J. of Applied Engineering Research*, vol. 12, no. 23, pp. 13265-13280, Dec. 2017.
[44] Sample DICOM Images. [Online]. Available: http://deanvaughan.org
[45] DICOMs category. [Online]. Available: https://www.nitrc.org/
[46] H. Khanzadi, M. Eshghi, and S. E. Borujeni, "Image encryption using random bit sequence based on chaotic maps," *Arabian J. for Science and Engineering*, vol. 39, no. 2, pp. 1039-1047, Feb. 2014.
[47] H. Arora, G. K. Soni, R. K. Kushwaha, and P. Prasoon, "Digital image security based on the hybrid model of image hiding and encryption," in *Proc IEEE. 6th Int. Conf. on Communication and Electronics Systems*, vol. 6, pp. 1153-1157, 8-10 Jul. 2021.
[48] 2015, "Key space in cryptiography," http://csrc.nist.gov (accessed).
[49] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using DNA sequence operations," *Optics and Lasers in Engineering*, vol. 88, pp. 197-213, Jan. 2017.
[50] J. Wu, X. Liao, and B. Yang, "Image encryption using 2D Hénon-Sine map and DNA approach," *Signal Processing*, vol. 153, pp. 11-23, Dec. 2018.
[51] G. Ye, K. Jiao, C. Pan, and X. Huang, "An effective framework for chaotic image encryption based on 3D logistic map," *Security and Communication Networks*, vol. 2018, pp. 1-11, Oct. 2018.
[52] P. T. Akkasaligar and S. Biradar, "Selective medical image encryption using DNA cryptography," *Information Security J.: a Global Perspective*, vol. 29, no. 2, pp. 91-101, Mar. 2020.
[53] X. Chai, J. Zhang, Z. Gan, and Y. Zhang, "Medical image encryption algorithm based on Latin square and memristive chaotic system," *Multimedia Tools and Applications*, vol. 78, no. 24, pp. 35419-35453, Dec. 2019.
[54] A. Mahmood, R. Dony, and S. Areibi, "An adaptive encryption based genetic algorithms for medical images," in *Proc. IEEE Int. Workshop on Machine Learning for Signal Processing*, 6 pp., Southampton, UK, 20-25 Sept. 2013.

محمد سلطانی مدرک کارشناسی در رشته مهندسی کامپیوتر، گرایش نرم‌افزار و مدرک کارشناسی ارشد در رشته فناوری اطلاعات، گرایش طراحی و تولید نرم‌افزار خود را به ترتیب در سال‌های ۱۳۹۴ و ۱۳۹۶ از دانشگاه شهید باهنر کرمان و دانشگاه آزاد اسلامی واحد کرمان دریافت کرد. وی هم‌اکنون دانشجوی دکتری مهندسی کامپیوتر، گرایش نرم‌افزار در دانشگاه آزاد اسلامی واحد مشهد است و از سال ۱۳۹۸ به تدریس در مباحث برنامه‌نویسی پیشرفته و پایگاه داده در دانشگاه آزاد اسلامی واحد کرمان و دانشگاه شهید چمران کرمان پرداخته است. زمینه‌های تحقیقاتی مورد علاقه او عبارتند از امنیت و الگوریتم‌های رمزنگاری. به‌واسطه فعالیت‌های پژوهشی و مقالات چاپ‌شده وی در دوران کارشناسی و کارشناسی ارشد، عضویتش در باشگاه پژوهشگران دانشجو و باشگاه پژوهشگران جوان و نخبگان مورد تأیید قرار گرفته است.

حسن شاکری مدارک کارشناسی، کارشناسی ارشد و دکتری خود را در رشته مهندسی کامپیوتر به ترتیب از دانشگاه‌های فردوسی مشهد، صنعتی شریف و فردوسی مشهد در سال‌های ۱۳۷۴، ۱۳۷۶ و ۱۳۹۳ دریافت کرد و در حال حاضر به عنوان عضو هیأت علمی با گروه کامپیوتر دانشگاه آزاد اسلامی مشهد همکاری می‌کند. زمینه‌های تحقیقاتی مورد علاقه وی عبارتند از مدیریت اعتماد، سیستم‌های پیشنهاددهنده و امنیت سیستم‌های کامپیوتری. او بیش از ۱۰۰ مقاله علمی در مجلات و کنفرانس‌های داخلی و بین‌المللی به چاپ رسانده است.

محبوبه هوشمند کارشناسی و کارشناسی ارشد خود را در رشته مهندسی کامپیوتر، گرایش نرم‌افزار به ترتیب در سال‌های ۱۳۸۶ و ۱۳۸۹ از دانشگاه فردوسی مشهد و دکترای خود را در رشته مهندسی کامپیوتر، گرایش معماری کامپیوتر از دانشگاه صنعتی

امیرکبیر در سال ۱۳۹۳ دریافت کرده است. او از آخر تابستان ۱۳۹۵ تا آخر تابستان ۱۳۹۶ محقق پسادکترا در زمینه رمزنگاری کوانتومی به طور مشترک در دانشگاه ملی سنگاپور و دانشگاه تکنولوژی و طراحی سنگاور بوده است. دکتر هوشمند در حال حاضر استادیار گروه مهندسی کامپیوتر دانشگاه آزاد اسلامی مشهد است. علایق پژوهشی ایشان شامل نظریه اطلاعات و محاسبات کوانتومی، رمزنگاری، سیستم‌های چندعاملی و داده‌کاوی است.