الگوریتمهای مبتنی بر رمز برای انتقال تصویر پزشکی امن

چکیده

توسعه عظیم برنامه های کاربردی پزشکی راه دور سبب شده است، ارائه خدمات امنیتی برای چنین برنامه های کاربردی، ضروری به نظر برسد. الگوریتمهای ارائه شده در این زمینه را میتوان به سه دسته تقسیم کرد: الگوریتم های مبتنی بر نهان نگاری، الگوریتمهای مبتنی بر رمز و الگوریتم های هیبریدی. در این مطالعه، مولفین دو الگوریتم مبتنی بر رمز را ارائه میدهند که قادر به ارائه خدمات محرمانه بودن، اعتبار و یکپارچگی برای تصاویر پزشکی است که در برنامه های کاربردی پزشکی راه دور مبادله میشوند. توابع نهفته قوی با کلیدهای متقارن ایجاد شده به طور داخلی و برنامه نویسی های درهم بکار میروند. حالت شمارشگر گالوا- استاندارد رمزگذاری پیشرفته با تابع درهم (هش) گردابی برای ارائه اعتبار و یکپارچگی بکار میرود و الگوریتم امضای دیجیتالی منحنی بیضی برای ارائه اعتبار و یکپارچگی برای داده های سرامد هم چنین برای داده های پیکسل تصاویر DICOM بکار میرود. اثر بخشی الگوریتمهای ارائه شده از طریق آزمایشگری وسیع با استفاده از یک مجموعه مبنا از تصاویر DICOM ارزیابی شده و نشان داده میشود.

1. مقدمه

پزشکی از راه دور، یک شیوه مراقبت پزشکی مدرن تسهیل شده از طریق توسعه سیستم های ارتباطات و اطلاعات در زیرساخت مراقبت از سلامت است. مزایای بیشماری از طریق برنامه های کاربردی پزشکی راه دور بدست می آید، همانند تشخیص راه دور و مشاوره بین اطبا، دستیابی به بایگانی های پزشکی متمرکز و یادگیری راه دور پزشکی. با این مزایا، با این وجود، خطرات همایندی برای داده های پزشکی در گردش در شبکه های باز وجود دارد و به این ترتیب براحتی از طریق مزاحمین مورد دستیابی قرار میگیرند. لذا کارشناسانی که در این زمینه پزشکی کار میکنند، نیاز مبرم خود برای طراح های امن و روشهای قادر به ارائه مبادله بی خطر تصاویر و سوابق پزشکی را اظهار نموده اند.

اهمیت یک مبادله امن تصاویر پزشکی، راه را برای سازمانهای مراقبت از سلامت بین المللی هموار ساخته است تا استانداردهای ویژه ای را منتشر سازند که به مسائل امنیت داده های پزشکی بپردازند. یک چنین استانداردی،

تصویربرداری دیجیتالی و ارتباطات در استاندارد پزشکی (DICOM) است. این استاندارد، رهنمودها و مکانیسم هایی را برای کارشناسان و نهادهای مراقبت از سلامت ارائه میدهد تا سه سرویس امنیتی پزشکی راه دور را بدست آورند: محرمانه بودن، اعتبار و یکپارچگی. سرویس محرمانه بودن، برای پیشگیری از دستیابی غیر قانونی به تصاویر ارسال شده است، در حالیکه سرویسهای یکپارچگی و اعتبار برای تایید مالکیت و جستجوی مداخله در تصاویر دریافت شده لازم هستند. در حال حاضر، پنهان سازی و فناوری های نهان نگاری برای اجرای طرحها و الگوریتم های قادر به ارائه سرویسهای امنیتی لازم برای برنامه های کاربردی پزشکی راه دور بکار میروند.

رویکرد مبتنی بر رمز برای کسب امنیت در سیستم های مبادله اطلاعات بر مبنای کاربرد توابع پنهانی است همانند رمزگذاری متقارن، درهم سازی و امضاهای دیجیتالی. رمزگذاری متقارن، محرمانه بودن برای تصاویر ارسال شده را با استفاده از رمزگذاری های بلوکی و رمزگذاری های جاری سازی ارائه میدهد، در حالیکه درهم سازی و امضاهای دیجیتالی، اعتبار و یکپارچگی محض تصاویر دریافتی را بررسی میکند. از سوی دیگر، نهان نگاری تصویر دیجیتالی، شیوه پنهان سازی داده های سری در تصاویر پزشکی دیجیتالی است.

محرمانه بودن با جاسازی داده های خصوصی بیمار به صورت نهان نگاری های قوی بدست می آید، در حالیکه اعتبار و یکپارچگی، با پنهان ساختن نهان نگاری های قوی و ضعیف در تصاویر پزشکی بدست می آید. گرچه نهان نگاری های تعبیه شده، تقریبا برای چشم انسان غیر قابل مشاهده اند اما ایده عینی جاسازی و از آن رو تنزل بخشیدن به تصویر پزشکی، ممکن است مقاومت جدی به پذیرش آن از طریق استانداردهای پزشکی و کارشناسان را تحریک نماید.

در این مقاله، دو الگوریتم مبتنی بر رمز قادر به ارائه محرمانه بودن و اثبات اعتبار و یکپارچگی تصاویر DICOM را ارائه میدهیم. بر خلاف استاندارد DICOM و سایر طرحهای مبتنی بر رمز، الگوریتمهای ارائه شده، محرمانه بودن، اعتبار و یکپارچگی برای هر دو ترکیب تصاویر DICOM را ارائه میدهند: داده های سرامد و داده های پیکسل. توابع پنهانی قوی با کلیدهای متقارن ایجاد شده به طور داخلی و خارجی و کدهای درهم در اجرای الگوریتمها بکار میروند. بقیه این مقاله به صورت ذیل سازماندهی میشود. بخش 2، طرحها و الگوریتم های پزشکی راه دور امن اخیر مرتبط با الگوریتم های ارائه شده را شرح میدهد. توابع پنهانی بکار رفته در اجرای

الگوریتمها در بخش 3 توصیف میشوند. الگوریتمهای ارائه شده در بخش 4 توصیف میشوند و نتایج اجرای آنها در بخش 5 ارائه و تحلیل میشوند. بحث و نتیجه گیری ها در بخش 6 ارائه میشوند.

2 آثار مرتبط

با وجود توسعه عظیم پزشکی راه دور و نیاز آنی برای ارائه خدمات امنیتی برای چنین برنامه های کاربردی، اخیرا تحقیقات در این زمینه شروع به جلب توجه نموده اند. الگوریتمهای ارائه شده در این حوزه، تحت طبقه بندی های مختلف دسته بندی شده اند، در عین حال، در این مقاله، دسته بندی خود را میپذیریم که روشها را به صورت الگوریتمهای مبتنی بر نهان نگاری، الگوریتمهای مبتنی بر رمز و الگوریتمهای هیبریدی گروه بندی میکند. در این بخش، به طور مختصر با توصیف الگوریتمهای معرف طبق هر دسته، به آثار مرتبط در این زمینه اشاره می نماییم.

سه نوع روش نهان نگاری برای نهان نگاری تصویر پزشکی ارائه شده است: روشهای برگشت ناپذیر، روشهای برگشت پذیر و روشهای مبتنی بر منطقه. روشهای نهان نگاری برگشت ناپذیر، در حوزه پزشکی قابل قبول نیستند زیرا تحریف ایجاد شده به تصاویر از طریق فرایند نهان نگاری، شامل عملیات غیر معکوس شدنی میشود همانند تعویض بیت یا تدریج (کوآنتش) [15،14]. از سوی دیگر روشهای نهان نگاری برگشت پذیر، اجازه میدهند تصویر پزشکی در مقادیر پیکسل اصلی خود بازیابی شود. از اینرو، تصاویر اصلی میتوانند در فرایند تشخیص پزشکی بکار روند [20-16]. با این حال، برگشت پذیرترین الگوریتمهای نهان نگاری دچار کمبود قابلیت مکان یابی مداخله هستند که در بررسی یکپارچگی تصاویر پزشکی مطلوب است. روشهای مبتنی بر منطقه شامل بخش بندی تصویر پزشکی اصلی به دو ناحیه مجزا میشود: منطقه مورد علاقه (ROI) و منطقه غیر مورد علاقه (RONI). دو منطقه، دارای مشخصات متفاوتی هستند و از اینرو نهان نگاری های مختلفی میتوانند برای کسب عاملیت های مختلف جاسازی شوند. از همه مهم تر اینکه، روشهای مبتنی بر منطقه دارای قابلیت مکان یابی مداخله هستند که یکپارچگی مبتنی بر محتوا را برای تصاویر پزشکی مورد مبادله ارائه میدهد. در عین حال، بخش بندی تصاویر پزشکی به مناطق ROI و RONI به عوامل زیادی وابسته است و از اینرو ممکن است همیشه صحیح یا حتی کاربردی نباشد. بدون در نظر گرفتن اینکه کدامیک از این سه روش نهان نگاری

قابل قبول است، نهان نگاری با ماهیت عینی خود، تنزل تصویر را مطرح میکند و این مساله ممکن است از پذیرش احتمالی آینده آن توسط استانداردهای امنیتی و کارشناسان پزشکی جلوگیری به عمل آورد.

2.2 الگوریتمهای مبتنی بر رمز

رویکرد مبتنی بر رمز برای کسب امنیت در سیستم های اطلاعات مراقبت از سلامت بر مبنای بکارگیری توابع پنهانی است همانند رمزگذاری متقارن، درهم سازی و امضاهای دیجیتالی [27-24]. بهترین روش مبتنی بر رمز، استاندارد DICOM است که مکانیسمهای متفاوتی را برای کسب امنیت برای تصاویر پزشکی مبادله شده ارائه میدهد. این استاندارد در زیر در کنار محدودیتهای امنیتی اش توصیف میشود. محدودیتها تا حدی توسط کوبایاشی و دیگران [24] تدبیر شده اند همانطور که بعدا در این زیر بخش شرح داده میشود.

2.2.1 استاندارد DICOM: DICOM، استاندارد مورد قبول مرجع در سطح جهانی برای مبادله تصاویر پزشکی است. این استاندارد، مکانیسمهایی را برای موجودیتهای کاربردی ارائه مدهد تا به طور امن همدیگر را تصدیق کنند و هر گونه مداخله ای در داده های پزشکی مبادله شده را کشف کنند. استاندارد DICOM، استفاده از شناسنده های منحصر به فرد برای شناسایی منحصر به فرد اشیاء DICOM را ایجاد میکند همانند تصاویر. شرایط لازم امنیتی قانون قابلیت انتقال و جوابگویی بیمه بهداشتی (HIPPA) در بخش 15 استاندارد DICOM با تعریف یک مجموعه کلی از خصوصیات امنیت و مدیریت طرح ریزی شده است [29،28].

یک تصویر DICOM دارای دو جزء است: داده های سرامد و داده های پیکسل. از طریق امضای دیجیتالی به اعتبار و یکپارچگی داده های پیکسل پرداخته میشود، با این وجود، محرمانه بودن داده های پیکسل، با خصوصیت محرمانه بودن سطح برنامه کاربردی اصلی بدان پرداخته نمیشود. این یک محدودیت مهم در این استاندارد است زیرا یک تصویر منتقل شده به طور ساده همیشه ممکن است مورد مداخله قرار گیرد، ترجمه یا ویرایش شود. در واقع، با هر ویرایشگر تصویر خوبی میتوان ویژگیهای آناتومی را ویرایش کرد تا به طور کامل نتیجه تشخیصی تصویر را تغییر داد. هر ویرایش تصویری مورد کشف قرار نخواهد گرفت اگر امضای دیجیتالی آن حذف شود یا از داده های سرامد مفقود گردد. با توجه به امنیت داده های سرامد، استاندارد DICOM طبق پروفایل محرمانه بودن سطح برنامه کاربردی اصلی، به محرمانه بودن سرامد میپردازد، با این حال اعتبار و یکپارچگی سرامد مورد بررسی قرار نمیگیرند. هم چنین یک محدودیت مهم استاندارد محسوب میشود زیرا

امنیت سرامد، یک اهمیت حیاتی محسوب میشود زیرا شامل داده های امنیت و بیماران حساس میباشد. سایر محدودیتهای استاندارد DICOM در [32] توصیف میشود.

2.2.2 طرح کوبایاشی: به خاطر محدودیتهای فوق الذکر، همه اجراهای بازرگانی پروفایلهای امنیتی DICOM بیانگر مطابقت با بخش 15 این استاندارد نیستند. لذا، پذیرش وسیعتر این استاندارد، مستلزم بهبودهایی در پروفایلهای امنیتی بر حسب محرمانه بودن، اعتبار و یکپارچگی نسبت به هر دو جز فایل DICOM است: داده های پیکسل و داده های سرامد. کوبایاشی و دیگران [24] طرح نوینی را ارائه نمودند که محدودیتهای امنیتی 3.15 پروفایل مکمل پروپوزال DICOM را بررسی میکنند. این طرح بر مبنای رمزگذاری داده هاست و از ساختارهای داده استاندارد DICOM بهره میبرد. محرمانه بودن برای داده های پیکسل با ارائه یک نسخه رمزگذاری شده از تصویری که باید منتقل شود، ارائه میگردد. با این حال، از آنجاییکه کلیدهای الگوریتم رمزگذاری بدون رمزگذاری در سرامد ذخیره میشوند، محرمانه بودن ارائه شده برای داده های پیکسل، ممکن است تضمین نشود. اعتبار و یکپارچگی برای داده های پیکسل با استفاده از امضاهای دیجیتالی با کلیدهای ایجاد شده داخلی ارائه میگردد. با این حال، طرح ارائه شده، محرمانه بودن، اعتبار و یکپارچگی را برای داده سرامد فراهم نمی آورد.

2.2.3. الگوریتمهای مبتنی بر رمز ارائه شده: الگوریتمهای مبتنی بر رمزی که در این مقاله ارائه میدهیم، محدودیتهای امنیتی استاندارد DICOM و طرح کوبایاشی را حل میکند [24]. الگوریتمها، محرمانه بودن، اعتبار و یکپارچگی را برای داده های پیکسل هم چنین داده های سرامد تصاویر DICOM ارائه میدهند. توصیف دقیق الگوریتمهای ارائه شده و نتایج ارزیابی عملکرد آنها در بخشهای ذیل ارائه میگردد.

2.3 الگوریتمهای هیبریدی

برای استفاده از مزایای ترکیبی این دو رویکرد، بسیاری از الگوریتمهای نهان نگاری- رمز در ادبیات ارائه شده اند که به شرایط لازم امنیتی برنامه های کاربردی پزشکی راه دور میپردازند [36-33]. در رویکرد هیبریدی، نهان نگاری به عنوان پایگاه اجرایی بکار میرود و نهان نگاری های اعتبار و یکپارچگی به صورت مقدمات پنهانی اجرا میشوند همانند کدهای درهم، کدهای افزونگی چرخه ای (CRCs) و امضاهای دیجیتالی. به طور کلی، کدهای درهم برای ارائه یکپارچگی محض تصویر پزشکی بکار میروند، در حالیکه کدهای افزونگی چرخه ای به طور

مناسب تری برای کشف نواحی مورد مداخله در تصویر دریافت شده استفاده میشوند. با این وجود، الگوریتمهای هیبریدی دچار کمبود متمرکز بر محاسبه بودن هستند. افزون بر آن، یک تغییر یک بیتی در یک کد افزونگی چرخه ای یا یک کد درهم به اثبات اعتبار و یکپارچگی نادرست منجر خواهد شد.

2. توابع پنهانی

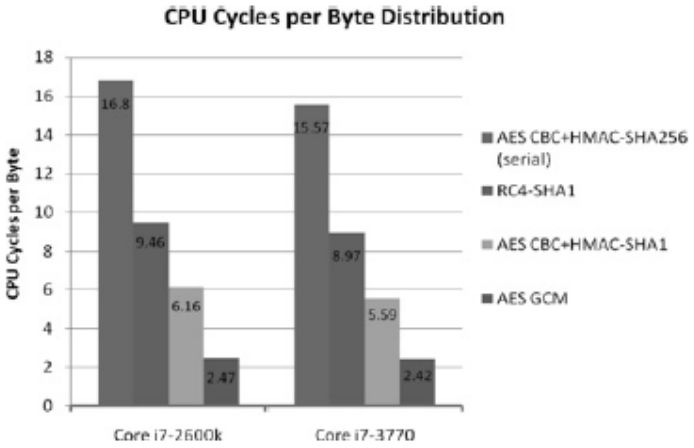
دو الگوریتم ارائه شده، محرمانه بودن، یکپارچگی و اعتبار برای داده های سرامد و پیکسل تصاویر DICOM را از طریق استفاده از سه تابع پنهانی موثر ارائه میدهد. سه تابع، حالت شمارنده گالوای- استاندارد رمزگذاری پیشرفته (AES-GCM)، تابع درهم گردابی و الگوریتم امضای دیجیتالی منحنی بیضی هستند. توابع و معیارهای انتخاب آنها در این بخش توصیف میشود.

2.1 حالت شمارنده گالوای- استاندارد رمزگذاری پیشرفته

حالت شمارنده گالوای- استاندارد رمزگذاری پیشرفته (AES-GCM) یک تابع رمزگذاری تایید شده است که در اصل در برنامه های کاربردی مستلزم محرمانه بودن، یکپارچگی و اعتبار بکار میرود. عملیات حالت شمارنده گالوای- استاندارد رمزگذاری پیشرفته، بر مبنای یک درهم سازی کلی بر روی یک فیلد گالوای دودوئی است تا رمزگذاری تایید شده ای را ارائه نماید که خروجی رمز را برای محرمانه بودن و برچسب تایید اعتبار را برای اثبات اعتبار و یکپارچگی ایجاد نماید. برای درست کار کردن، حالت شمارنده گالوای- استاندارد رمزگذاری پیشرفته به سه ورودی نیاز دارد: داده هایی که رمزگذاری یا رمزگشایی میشوند، یک کلید رمزگذاری 256 بیتی و یک بردار اولیه 256 بیتی. خروجی های ایجاد شده، داده های رمزگذاری شده یا رمزگشایی شده و یک برچسب تایید اعتبار 256 بیتی هستند [37].

انتخاب حالت شمارنده گالوای- استاندارد رمزگذاری پیشرفته بر مبنای این واقعیت است که رمزگذاری و تایید اعتبار متقارن به طور همزمان را ارائه میدهد. چنین عاملیت رمزگذاری تایید شده ای از رمزگذاری ترتیبی و تایید اعتبار مرسوم بهتر عمل میکند و از اینرو امنیت کلی برنامه های کاربردی مبتنی بر رمز را بهبود میبخشد. به علاوه، اخیرا نشان داده شده است حالت شمارنده گالوای- استاندارد رمزگذاری پیشرفته از بسیاری از الگوریتمهای تایید شده استاندارد شده موسسه ملی استانداردها و فناوری (NIST) مثل AES CBC

HMAC – SHA1, AES CBC + HMAC – SHA256 + و RC4 –SHA1 بهتر عمل میکند، همانطور که در شکل 1 نشان داده شده است [38].



شکل 1

2.2 تابع درهم گردابی

گرداب، یک تابع درهم است که در طرح های اروپایی جدید برای امضاها، یکپارچگی و پروژه رمزگذاری توسعه یافته است و توسط سازمان استانداردهای بین المللی، استاندارد شده است [39]. این تابع بر روی پیامهای به طول $<2^{256}$ بیت کار میکند تا یک کد درهم 512 بیتی را ایجاد نماید. این کد در اجرای الگوریتمهای ارائه شده ما به دو بخش تقسیم میشود: 256 بیتی برای کلیدهای رمزگذاری و 256 بیتی برای بردارهای شروع. درهم سازی گردابی، یک تابع قوی است زمانیکه با سایر توابع درهم مقایسه شود همانند MD5, SHA-1, SHA-224, SHA-256 و SHA-384. یک تابع درهم قوی به طور مشابه، درهم SHA-512 است، با این وجود ما استفاده از تابع درهم گردابی را با خاطر این واقعیت برگزیدیم که هیچ حمله ای بر روی نسخه های اولیه این تابع گزارش نشده است.

2.3 الگوریتم امضای دیجیتالی منحنی بیضی

الگوریتم امضای دیجیتالی منحنی بیضی (ECDSA) یک نوع دیگر الگوریتم امضای دیجیتالی (DSA) است. هر دو الگوریتم بر مبنای پنهان شناسی کلید عمومی هستند، با این حال ECDSA از پنهان سازی منحنی بیضی (ECC) برای تولید امضاهای کوتاهتر از DSA اصلی استفاده میکنند، در حالیکه همان سطوح امنیتی را حفظ

میکند [40]. این ویژگی، یک اهمیت خاص برای الگوریتمهای ارائه شده ماست زیرا امضاهای دیجیتالی 256 بیتی ایجاد شده توسط ECDSA میتواند براحتی در سرامد DICOM ذخیره شود، همانطور که در بخش الگوریتمهای ارائه شده توضیح داده خواهد شد. به علاوه، ECDSA، شرایط لازم محاسباتی را کاهش میدهد در حالیکه همان میزان امنیت تامین شده توسط طرحهای کلید عمومی دیگر با کلیدهای بهمان نسبت بزرگتر را حفظ میکند. جدول 1 نشان میدهد یک ECC 256 بیتی، همان سطح ایمنی را ارائه میدهد که یک طرح دیفی-هلمن (Diffie–Hellman) 3072 بیتی با هزینه محاسبه بسیار پایین تر ارائه میدهد.

Diffie–Hellman key size, bits	ECC key size, bits	Cost ratio between Diffie–Hellman and ECC
1024	160	3:1
2048	224	6:1
3072	256	10:1
7680	384	32:1
15 360	512	64:1

جدول 1

4 الگوریتمهای ارائه شده

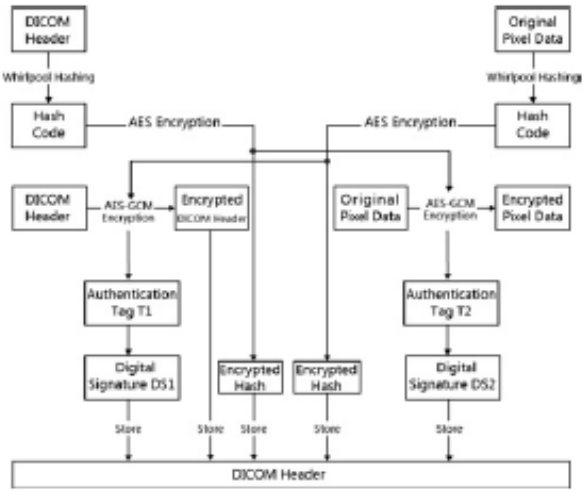
دو الگوریتم ارائه میشود، هر یک از دو راه کار تشکیل میشود: راه کار رمزگذاری و خلق امضا و راه کار رمزگشایی و تایید امضا. الگوریتم نخست ازAEC-GCM ، تابع درهم گردابی و ECDSA استفاده میکند، در حالیکه الگوریتم دوم فقط از AEC-GCM و ECDSA استفاده میکند. یک توصیف از این دو الگوریتم در این بخش ارائه میشود.

4.1 الگوریتم اول

این الگوریتم از رمزگذاری متقارن، درهم سازی و امضاهای دیجیتالی برای ارائه محرمانه بودن، یکپارچگی و اعتبار برای داده های سرامد و پیکسل تصاویر DICOM استفاده میکند. داده های پیکسل و صفات خاصه محرمانه داده های سرامد با استفاده از AES-GCM رمزگذاری میشوند که داده های پیکسل رمز و یک برچسب تایید اعتبار را به طور همزمان تولید میکنند. کلیدهای رمزگذاری و بردارهای شروع به طور داخلی با استفاده از تابع درهم گردابی تولید میشوند آنگاه. برچسب تایید اعتبار ECDSA امضا میشود. راه کار رمزگذاری و خلق امضا و راه کار رمزگشایی و تایید امضا در ذیل توصیف میشوند.

4.1.1 راه کار رمزگذاری و خلق امضا: این راه کار، داده های پیکسل و صفات خاصه محرمانه داده های سرامد را به صورت ورودیها و خروجی های خود میگیرد که به صورت داده های پیکسل کاملا رمزگذاری شده و سرامد DICOM نیمه رمزگذاری شده هستند. مراحل عملیاتی این راه کار در شکل 2 نشان داده شده است.

1. **محرمانه بودن داده های سرامد**: برای مطابقت با سطح برنامه کاربردی اصلی، خصوصیت محرمانه بودن در DICOM PS 3.15 توصیف شده است، این راه کار کل صفات خاصه محرمانه سرامد را میخواند، ارزشهای اصلی آنها را با استفاده از AES-GCE رمزگذاری میکند و نتیجه را در "دنباله صفات خاصه اصلاح شده (0400, 0550)" ذخیره میکند در حالیکه مقادیر موجود در موقعیتهای اصلی را با مقادیر ساختگی جایگزین میسازد. یک خروجی اضافی AES-GCE ، برچسب تایید اعتبار سرامد است که در مرحله بعدی بکار خواهد رفت. کلید رمزگذاری و بردار شروع بکار رفته توسط AES-GCE برای رمزگشایی داده های سرامد از کد درهم ایجاد شده ، با بکارگیری تابع درهم گردابی بر روی داده های پیکسل گرفته میشود. آنگاه کد درهم با AES رمزگذاری میشود و در سرامد DICOM برای استفاده بعدی در سمت گیرنده ذخیره میشود. ایجاد کلید رمزگذاری و بردار شروع از کد درهم داده های پیکسل، یک پیوند قوی را بین داده های پیکسل، سرامد و امنیت ایجاد میکند. بنابراین، کاربر نمیتواند صفات خاصه سرامد صحیح را ببیند چنانچه داده های پیکسل، مورد مداخله قرار گیرند یا خراب شوند. به علاوه، فایلهای DICOM مختلف دارای صفات خاصه سرامد محرمانه مختلفی هستند و به این ترتیب کلید رمزگذاری و بردار شروع از یک تصویر به تصویر دیگر فرق دارد



شکل 2

این امر سبب کاهش ریسکهای امنیتی شده و از معرفی آسیب پذیری احتمالی در فرایند رمزگذاری جلوگیری میکند.

2. **اعتبار و یکپارچگی داده های سرامد**: برچسب تایید اعتبار ایجاد شده توسط AES-GCE در مرحله قبلی با کلید خصوصی موجودیت ارسال با استفاده از ECDSA امضا میشود. امضای دیجیتالی ایجاد شده در سرامد DICOM ذخیره میشود. اعتبار و یکپارچگی داده های سرامد در بخش 15 استاندارد DICOM مورد بررسی قرار نمیگیرد.

3. **محرمانه بودن داده های پیکسل**: داده های پیکسل با AES-GCE رمزگذاری میشود: همین الگوریتم رمزگذاری برای رمزدار کردن داده های سرامد بکار رفت. با این حال، کلید رمزگذاری و بردار شروع، کد درهم تولید شده با بکارگیری تابع درهم گردابی بر روی صفات خاصه محرمانه سرامد هستند. آنگاه کد درهم (کلید رمزگذاری و بردار شروع) با AES رمزدار میشود و در سرامد DICOM برای استفاده بعدی در سمت گیرنده ذخیره میشود. یک خروجی اضافی AES-GCE ،برچسب تایید اعتبار داده های پیکسل است که در مرحله بعدی بکار خواهند رفت. رمزگذاری و از اینرو محرمانه بودن داده های پیکسل، در بخش 15 استاندارد DICOM مورد بررسی قرار نمیگیرد.

4. **اعتبار و یکپارچگی داده های پیکسل**: برچسب تایید اعتبار ایجاد شده توسط AES-GCE در مرحله قبلی با کلید خصوصی موجودیت ارسال امضا میشود، که یک امضای دیجیتالی داده های پیکسل را ایجاد مینماید. امضا در سرامد DICOM طبق خصوصیات امضاهای دیجیتالی توصیف شده در بخش PS 3.15 از استاندارد DICOM ذخیره میشود.

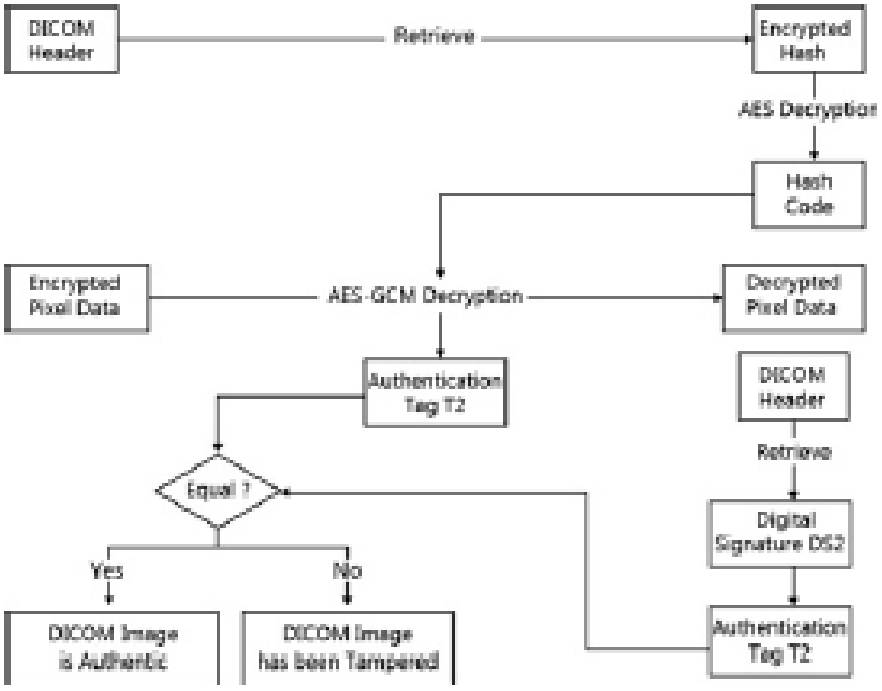
4.1.2 راه کار رمزگشایی و تایید امضا:

این راه کار، داده های سرامد DICOM نیمه رمزگذاری شده و داده های پیکسل رمزگذاری شده را رمزگشایی میکند، اعتبار و یکپارچگی آنها را وارسی میکند همانطور که در شکلهای 3 و 4 نشان داده شده است و زین پس توصیف میشود.

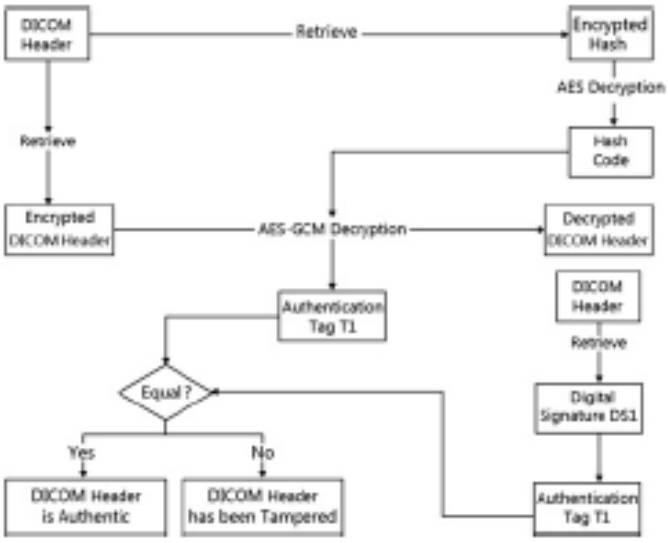
1. **محرمانه بودن داده های پیکسل**: کد درهم رمزگذاری شده صفات خاصه محرمانه سرامد از سرامد DICOM بازیابی کرده و آن با استفاده از استاندارد AES رمزگشایی کنید. خروجی 512 بیتی با AES-GCM به عنوان

یک کلید رمزگذاری و بردار شروع برای رمزگشایی داده های پیکسل مورد استفاده قرار میگیرد. غیر از داده های پیکسل، AES-GCM یک برچسب تایید اعتبار داده های پیکسل را ایجاد میکند.

2. **اعتبار و یکپارچگی داده های پیکسل**: امضای دیجیتالی داده های پیکسل از سرامد و استخراج برچسب تایید اعتبار آن را با استفاده از کلید عمومی موجودیت ارسال بازیابی کنید. برچسب استخراج شده را با برچسب تایید اعتبار ایجاد شده از طریق AES-GCE در مرحله قبلی مقایسه کنید. اگر بین دو برچسب،مطابقت وجود داشته باشد، اعتبار و یکپارچگی داده های پیکسل تایید میشوند.
3. **محرمانه بودن داده های سرامد**: کد درهم رمزگذاری شده داده های پیکسل را بازیابی کرده و آن را با استفاده از استاندارد AES رمزگشایی کنید. خروجی 512 بیتی با AES-GCM به عنوان یک کلید رمزگشایی و بردار شروع برای رمزگشایی صفات خاصه محرمانه سرامد بکار میروند. غیر از صفات خاصه سرامد رمزگشایی شده، AES-GCM یک برچسب تایید اعتبار صفات خاصه را ایجاد مینماید.



شکل 3



شکل 4

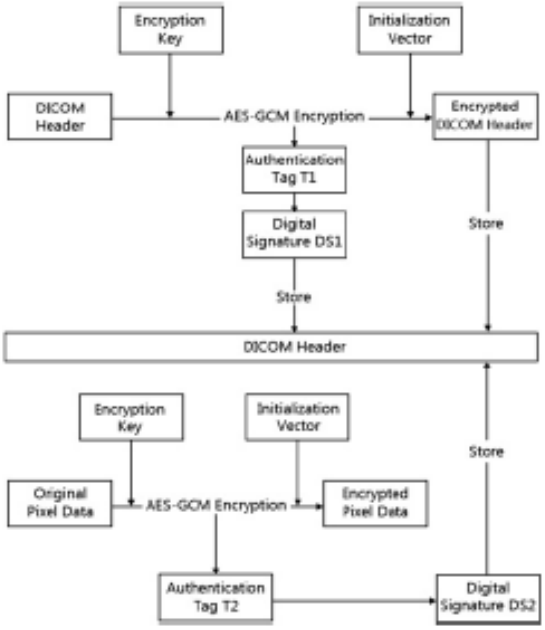
4. **اعتبار و یکپارچگی داده های سرامد**: امضای دیجیتالی داده های سرامد را از سرامد DICOM بازیابی کرده و برچسب تایید اعتبار آن را با استفاده از کلید عمومی موجودیت ارسال استخراج کنید. برچسب استخراج شده را با برچسب تایید اعتبار ایجاد شده از طریق AES-GCE در مرحله قبلی مقایسه کنید. اگر بین این دو برچسب، مطابقت وجود داشته باشد، اعتبار و یکپارچگی صفات خاصه سرامد محرمانه تایید میگردد.

4.2 الگوریتم دوم

در الگوریتم دوم توصیف شده در بالا، کلیدهای رمزگذاری و بردارهای شروع بکار رفته توسط AES-GCM به طور داخلی ، از طریق درهم سازی داده های پیکسل و خواص محرمانه سرامد ایجاد میشوند. این کار سبب ارتقاء امنیت الگوریتم با ایجاد یک پیوند قوی بین داده های سرامد، داده های پیکسل و داده های امنیتی ایجاد شده میشود. با این حال، درهم سازی داده های پیکسل و صفات خاصه محرمانه سرامد برای ایجاد کلیدها و بردارهای شروع ممکن است سبب مخارج کلی محاسباتی شود. بنابراین، الگوریتم دوم توصیف شده در اینجا، چنین مخارج کلی را از بین میبرد، با ارائه کلیدهای رمزگذاری و بردارهای شروع به طور خارجی. این کلیدها میتوانند با استفاده از روشهای مرسوم عرضه شوند همانند مراکز توزیع یا روشهای کلید- عمومی همانند مبادله کلید دیفی- هلمن. گزینه دیگری برای مبادله کلیدهای خارجی و بردارهای شروع، ذخیره آنها به صورت رمزگذاری شده در سرامد DICOM در سمت فرستنده است و آنها را در سمت گیرنده رمزگشایی میکند.

4.2.1 **راه کار رمزگذاری و خلق امضا**: این راه کار، داده های پیکسل و صفات خاصه محرمانه داده های سرامد را به صورت ورودی ها میگیرد و داده های پیکسل کاملا رمز گذاری شده و سرامد DICOM نیمه رمزگذاری شده را ایجاد میکند. مراحل عملیاتی این راه کار در شکل 5 نشان داده شده است و در ذیل به طور دقیق شرح داده میشود.

1. **محرمانه بودن داده های سرامد**: کل صفات خاصه محرمانه سرامد را بخوانید، مقادیر اصلی آنها را با AES-GCE رمزگذاری کنید و صفات خاصه را در "دنباله صفات خاصه اصلاح شده (0550، 0400)" ذخیره نمایید، در حالیکه مقادیر موجود در موقعیتهای اصلی را با موقعیتهای ساختگی جایگزین میکنید. فرایند رمزگذاری AES-GCE از یک کلید رمزگذاری تامین شده خارجی و یک بردار شروع استفاده میکند. غیر از داده های سرامد رمزگذاری شده، AES-GCM یک برچسب تایید اعتبار صفات خاصه محرمانه سرامد را تولید میکند.
2. **اعتبار و یکپارچگی داده های سرامد**: برچسب تایید اعتبار ایجاد شده توسط AES-GCE با کلید خصوصی موجودیت ارسال را با استفاده از ECDSA امضا کنید. این کار با ذخیره سازی امضای دیجیتالی ایجاد شده سرامد در سرامد DICOM طبق خصوصیات امضاهای دیجیتالی توصیف شده در بخش PS 3.15 استاندارد DICOM ایجاد میشود.



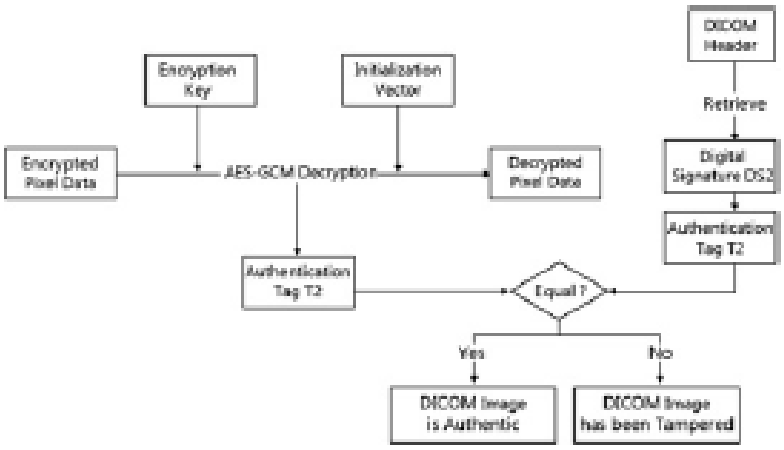
شکل 5

3. **محرمانه بودن داده های پیکسل**: داده های پیکسل را با AES-GCE با استفاده از الگوریتم رمزگذاری مشابه، کلید رمزگذاری و بردار شروع بکار رفته برای رمزگذاری داده های سرامد، رمزگذاری کنید. علاوه بر داده های رمزگذاری شده، AES-GCM یک برچسب تایید اعتبار داده های پیکسل را ایجاد میکند.
4. **اعتبار و یکپارچگی داده های پیکسل**: برچسب تایید اعتبار ایجاد شده توسط AES-GCE را با کلید خصوصی موجودیت ارسال امضا کنید. امضای دیجیتالی ایجاد شده داده های پیکسل در سرامد DICOM طبق خصوصیات امضاهای دیجیتالی توصیف شده در بخش PS 3.15 استاندارد DICOM ذخیره میشود.

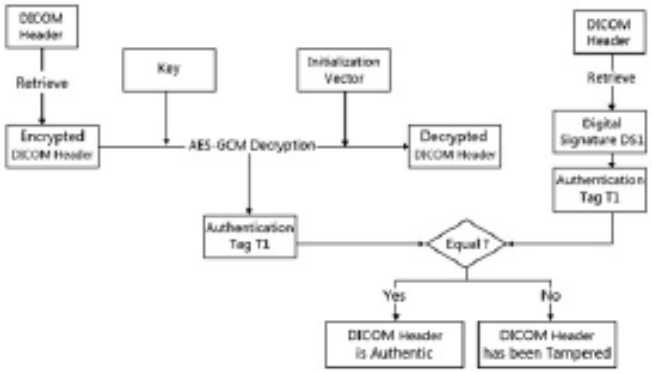
4.2.2 راه کار رمزگشایی و تایید امضا:

این راه کار، سرامد DICOM دریافت شده و داده های پیکسل را رمزگشایی کرده و اعتبار و یکپارچگی آنها را تایید میکند همانطور که در اشکال 6 و 7 نشان داده شده است و در ذیل توصیف شده است.

1. **محرمانه بودن داده های پیکسل**: با استفاده از کلید رمزگشایی و بردار شروع بکار رفته توسط موجودیت ارسال، AES-GCE را برای ایجاد داده های پیکسل و برچسب تایید اعتبار متناظر بکار ببرید.
2. **اعتبار و یکپارچگی داده های پیکسل**: امضای دیجیتالی داده های پیکسل را از سرامد بازیابی کنید و برچسب تایید اعتبار آن را با استفاده از کلید عمومی موجودیت ارسال استخراج نمایید. برچسب استخراج شده را با برچسب تایید اعتبار ایجاد شده از طریق AES-GCE در مرحله قبلی مقایسه نمایید. اگر بین این دو برچسب، یک مطابقت وجود داشته باشد، اعتبار و یکپارچگی داده های پیکسل، تایید میشود.
3. **محرمانه بودن داده های سرامد**: با استفاده از کلید رمزگشایی و بردار شروع بکار رفته از طریق موجودیت ارسال، AES-GCE را برای ایجاد داده های سرامد رمزگشایی شده و برچسب تایید اعتبار مربوطه، بکار ببرید.
4. **اعتبار و یکپارچگی داده های سرامد**: امضای دیجیتالی داده های سرامد را از سرامد DICOM بازیابی کرده و برچسب تایید اعتبار آن را با استفاده از کلید عمومی موجودیت ارسال استخراج نمایید. برچسب استخراج شده را با برچسب تایید اعتبار ایجاد شده توسط AES-GCE در مرحله قبلی مقایسه نمایید. اگر بین این دو برچسب، مطابقت وجود دارد، اعتبار و یکپارچگی صفات خاصه سرامد محرمانه تایید میگردد.



شکل 6



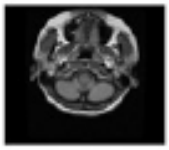
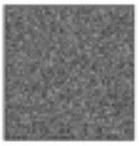
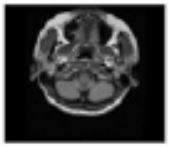
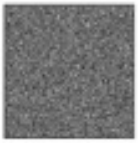
شکل 7

5 تحلیل عملکرد

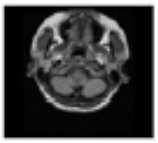
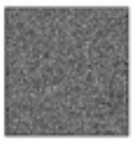
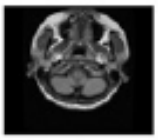
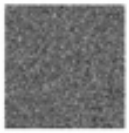
آزمایشگری وسیعی با استفاده از یک مجموعه معیار بیست تصویر مغزی DICOM ام آر آی برای ارزیابی عملکرد الگوریتم های ارائه شده با توجه به دستاوردهای شرایط امنیتی از قبل تنظیم شده صورت گرفته است. اندازه هر تصویر DICOM ، 256× 256 پیکسل با عمق 16 بیت است. آزمایشات در یک رابط گرافیکی کاربر (GUI) مبتنی بر محیط MATLAB اجرا شد که بر روی یک دستگاه Dell N5010 اجرا میشود (Intel Core TM,4.00 GB RAM و M350در 2.27 GHz با سیستم عامل ویندوز اکس پی مایکروسافت).

محرمانه بودن تضمین میشود اگر تصویر رمزگذاری شده، به شدت به تصویر واضح اصلی ناهمبسته باشد. برای سنجش همبستگی بین تصاویر واضح و رمزگذاری شده ایجاد شده توسط این دو الگوریتم ، مجموعه تحلیلهای عملکردی ذیل بکار میروند: تحلیل شباهت، تحلیل آنتروپی و تحلیل پیشینه نما. تحلیل یکپارچگی محض هم

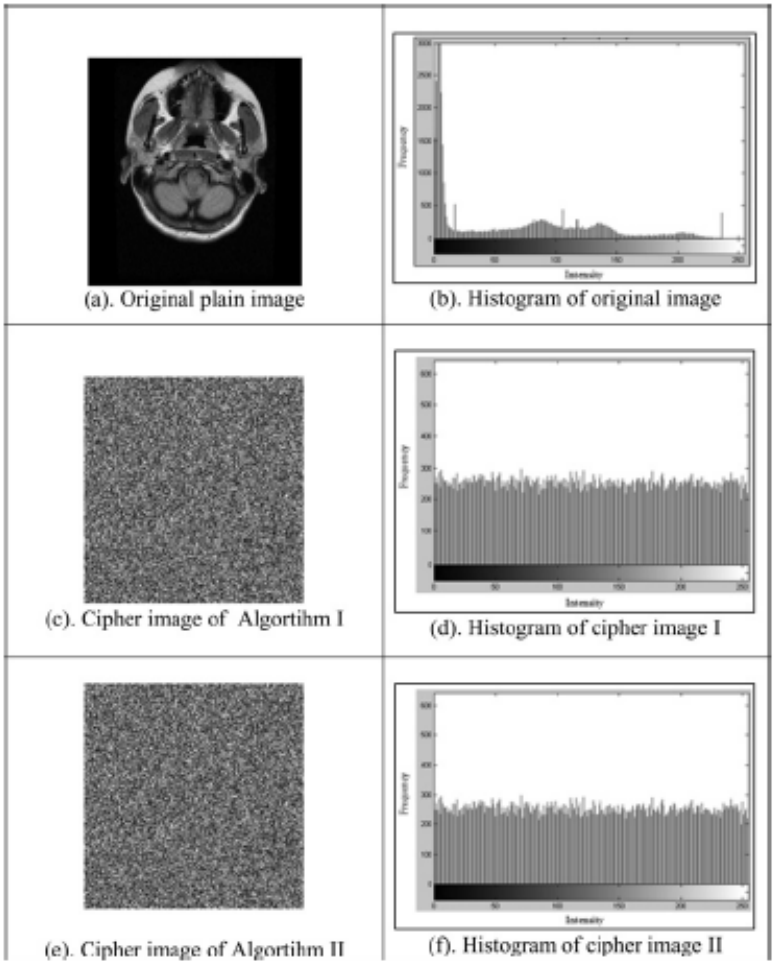
چنین برای نمایش یکپارچگی و اعتبار الگوریتم اجرا شده است. نهایتا، تحلیل زمانی برای ارزیابی شرایط لازم محاسباتی دو الگوریتم اجرا میشود.

Proposed Algorithm	*Original Image*	*Cipher Image*	*Correlation Factor*	*PSNR (dB)*
Algorithm I			*0.0081*	*11.1309*
Algorithm II			*0.0081*	*11.3778*

شکل 8

Proposed Algorithm	*Original Image*	*Entropy of Original Image (bits/pixel)*	*Cipher Image*	*Entropy of Cipher Image (bits/pixel)*
Algorithm I		*5.8739*		*7. 8909*
Algorithm II		*5.8739*		*7.9969*

شکل 9



شکل 10

5.1 تحلیل شباهت

همبستگی استاندارد شده، یک متریک عملکرد بکار رفته برای سنجش درجه شباهت بین دو شی دیجیتالی است. در زمینه الگوریتم های ارائه شده، اگر تصاویر واضح و رمزی، کاملا متفاوت باشند، آنگاه عامل همبستگی استاندارد شده آنها، بسیار پایین یا بسیار نزدیک به صفر خواهد بود. عوامل همبستگی که ما بین تصاویر واضح و رمزدار سنجیدیم، در شکل 8 ارائه میشوند. مقادیر همبستگی پایین بیانگر این است که راه کارهای رمزگذاری که بکار برده ایم، میتوانند کل صفات خاصه تصویر ارسال شده را پنهان سازند، از اینرو، محرمانه بودن لازم را بدست می آورند. نسبت سیگنال به نویز (PSNR) پیک، متریک دیگری است که شباهت بین تصاویر واضح و رمزدار را میسنجد. مقادیر PSNR کسب شده توسط الگوریتمهای ارائه شده در همان شکل داده شده اند. مقادیر پایین اثبات میکنند این دو تصویر، ناهمبسته هستند و از اینرو، محرمانه بودن بدست می آید.

Proposed Algorithm	Noisy Cipher Image	Deciphered Image	Compressed Cipher Image	Deciphered Image
Algorithm I				
Algorithm II				

شکل 11

5.2 تحلیل آنتروپی

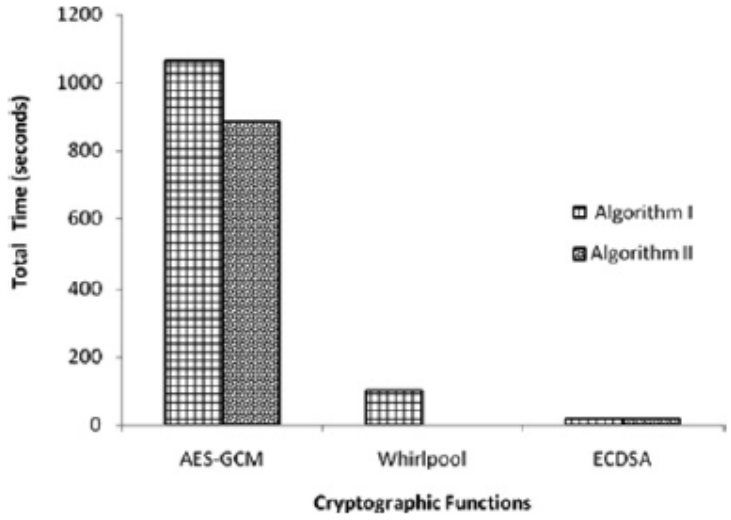
آنتروپی برای سنجش عدم اطمینان موجود در تصویر رمز بکار میرود. هر چه آنتروپی تصویر رمز، بالاتر باشد، درجه تصادفی بودن و محرمانه بودن تصویر بالاتر است. با فرض اینکه بیشینه آنتروپی نمایشی برای یک تصویر مقیاس خاکستری، 8 بیت بر پیکسل باشد، مقادیر آنتروپی بدست آمده برای الگوریتم های ارائه شده در شکل 9 ارائه شده اند. مقادیر آنتروپی بدست آمده تصاویر رمزدار به 8 بیت/پیکسل نزدیک هستند که اثربخشی الگوریتم های ارائه شده در پنهان سازی جزئیات تصاویر اصلی را نشان میدهد. مقدار آنتروپی تصویر واضح اصلی در این شکل برای مقایسه داده شده است.

5.3 تحلیل پیشینه نما

تحلیل پیشینه نما یا هیستوگرام تصویر به تجسم همبستگی بین تصاویر واضح و رمزدار با دادن احتمال پیدایش هر سطح خاکستری کمک میکند. شکل 10 هیستوگرامها برای تصاویر واضح و رمزدار را برای این دو الگوریتم نشان میدهد. این تفاوت بزرگ بین هیستوگرامهای تصاویر واضح و رمزدار نشان داده شده در شکل، بیانگر این است که تصاویر به شدت ناهمبسته هستند. به علاوه، هیستوگرامهای تصاویر رمزدار نشان میدهد احتمالا پیدایش سطوح خاکستری، به طور عادلانه توزیع میشود و از اینرو میزان کمی از اطلاعات میتواند از تصاویر رمزدار پیش بینی شود.

5.4 تحلیل یکپارچگی محض

اعتبار و یکپارچگی تصویر دریافت شده، تضمین میشود اگر و تنها اگر، سمت گیرنده بتواند تصویر را به شکل اصلی خود رمزگشایی نماید. هر گونه دستکاری در تصویر رمزدار باید، داده های خروجی بی معنی ایجاد نماید. چندین حمله پردازش سیگنال برای تصاویر رمزدار برای شبیه سازی سناریوهای دستکاری مختلف بکار رفته اند. این حملات شامل نویز گائوسی افزایشی، فشرده سازی JPEG، چرخش، آراستن در بین بقیه موارد است. شکل 11 نتیجه دو حمله بر روی تصاویر رمزدار را نشان میدهد: نویز گائوسی و فشرده سازی JPEG. همانطور که در این شکل نشان داده شده است، فرایند رمزگشایی نمیتواند تصاویر اصلی صحیحی را ایجاد نماید اگر تصاویر رمزدار با یک نویز گائوسی یا یک حمله فشرده سازی JPEG مورد مداخله قرار گیرند. این نتیجه بر خاصیت یکپارچگی محض الگوریتم های ارائه شده تاکید دارد که بیانگر این است که سمت گیرنده میتواند فقط تصویر واضح ارسال شده اصلی را ببیند، اگر و تنها اگر، تصویر دریافت شده بدون هیچ دستکاری، سالم دریافت گردد.



شکل 12

5.5 تحلیل زمانی

کل زمانهای رمزگذاری و رمزگشایی برای هر دو الگوریتم ، اندازه گیری شده اند و در شکل 12 نشان داده شده اند. برای الگوریتم اول، زمانهای رمزگذاری و رمزگشایی، به ترتیب 811.7 و 861.1 ثانیه هستند. الگوریتم دوم به یک مقدار کمتر محاسبه نیاز دارد زیرا کلیدهای رمزگذاری و بردارهای شروع به طور خارجی تامین شدند و به طور داخلی ایجاد نشدند. کل زمانهای رمزگذاری و رمزگشایی برای الگوریتم دوم، به ترتیب 484.8 و 552.7 ثانیه بود.

برای درک بهتر شرایط لازم محاسباتی سه تابع پنهانی، شکل 12، تفکیک زمانهای رمزگذاری و رمزگشایی طی شده توسط هر تابع را نشان میدهد. همانطور که در این شکل نشان داده شده است، دو الگوریتم، بیشترین وقت خود را در اجرای راه کارهای رمزگذاری و رمزگشایی AEC-GCM صرف میکنند. گرداب، تنها در الگوریتم اول برای ایجاد کلیدهای خصوصی و بردارهای اولیه برای AEC-GCM اجرا میشود و ECDSA به حداقل زمان پردازش برای این دو الگوریتم نیاز دارد.

زمانهای رمزگذاری و رمزگشایی AEC-GCM میتوانند به شدت کاهش پیدا کنند اگر و تنها اگر یک زیر مجموعه از صفات خاصه سرامد DICOM محرمانه، رمزگذاری شود، تا اینکه کل صفات خاصه رمزگذاری شود همانطور که توسط استاندارد DICOM پیشنهاد شده است. کاهش بیشتر در زمانهای رمزگذاری و رمزگشایی میتواند با استفاده از سخت افزار ویژه بدست آید همانند پردازشگرهای گرافیکی علاوه بر روشهای برنامه نویسی موازی.

6.مقایسه عملکرد

رمزگذاری تایید شده، توسط الگوریتم های ارائه شده ما برای ارائه محرمانه بودن، اعتبار و یکپارچگی بکار رفته است، در عین حال، توسط کوبایاشی و دیگران فقط برای تامین اعتبار و یکپارچگی بکار رفته است. به منظور تکمیل، در جدول 2، عملکرد دو الگوریتم ارائه شده را با عملکرد طرح کوبایاشی مقایسه میکنیم. مقایسه با توجه به همبستگی استاندارد شده، PSNR، آنتروپی و زمانهای پردازش انجام میگیرد. همانطور که در جدول نشان داده شده، الگوریتم های ارائه شده ما، عملکرد رمزگذاری بهتری را بدست آورده و به زمانهای رمزگذاری و رمزگشایی کمتری نیاز دارند.

Algorithm	Normalised correlation	PSNR, dB	Entropy, bits/pixel	Encryption time, s	Decryption time, s
algorithm I	0.0081	11.1309	7.8909	811.7	861.1
algorithm II	0.0081	11.3778	7.9969	484.8	552.7
Kobayashi [24]	0.0242	11.4760	7.4764	876.2	904.2

جدول 2

Algorithm	Confidentiality	Authenticity	Integrity
the DICOM standard	header data only	pixel data only	pixel data only
Kobayashi scheme [24]	pixel data only	pixel data only	pixel data only
algorithm [42]	—	header and pixel data	header and pixel data
algorithm I	header and pixel data	header and pixel data	header and pixel data
algorithm II	header and pixel data	header and pixel data	header and pixel data

جدول 3

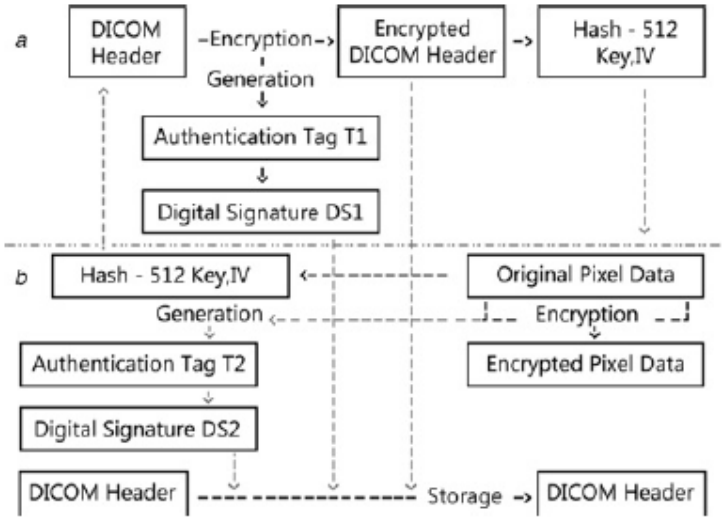
6 بحث و نتیجه گیری ها

الگوریتم های ارائه شده، همانطور که در کل مقاله شرح داده شده است، محرمانه بودن، اعتبار و یکپارچگی را هم برای داده های سرامد و هم پیکسل تصاویر DICOM ارائه میدهند. این امر، یک بهبود مهم محسوب میشود که میتواند به خصوصیات امنیتی استاندارد DICOM گسترش یابد. یعنی، این استاندارد، محرمانه بودن را برای یک زیر مجموعه منتخب از صفات خاصه سرامد از طریق مکانیسمهای مشخص شده در خصوصیت محرمانه بودن سطح برنامه کاربردی اصلی PS 3.15 فراهم می آورد. با این حال، هیچ مکانیسمی را برای کسب محرمانه بودن داده های پیکسل، ارائه نمیدهد. به طورمشابه، این استاندارد، اعتبار و یکپارچگی را برای داده های پیکسل از طریق خصوصیات امضای دیجیتالی مبنای خود ارائه میدهد، با این حال، هیچ گونه مکانیسم اعتبار و یکپارچگی را برای داده های سرامد ارائه نمیدهد.

از سوی دیگر، الگوریتم مبتنی بر DICOM ارائه شده توسط کوبایاشی و دیگران [24]، اعتبار و یکپارچگی را برای داده های پیکسل ارائه میدهد اما برای داده های سرامد ارائه نمیدهد. با توجه به محرمانه بودن، رمزگذاری داده های پیکسل، محرمانه بودن را تامین میکند، در عین حال، چون کلید متقارن در سرامد واضح حفاظت نشده ذخیره میشود، اگر کلید متقارن از طریق مزاحمین مورد بازیابی قرار گیرد، حریم شخصی داده های پیکسل مورد تخطی قرار خواهد گرفت. به علاوه، این الگوریتم، محرمانه بودن را برای داده های سرامد ارائه نمیدهد.با وجود این محدودیتها، یک همبخشی مهم این الگوریتم ارائه شده توسط کوبایاشی و دیگران [24]، پیوند قوی ایجاد شده بین داده های پیکسل و داده های امنیتی خودش است. خلاصه ای از این مقایسه که در بالا ذکر شده است،

در جدول 3 نشان داده شده است. این دو الگوریتم ارائه شده بر حسب کسب سرویسهای امنیتی لازم، رفتار میکنند.

نهایتا، لازم به ذکر است، تلاش برای کسب سه سرویس امنیتی برای تصاویر DICOM، توسط یکی از مولفین در یک الگوریتم مبتنی بر رمز در [42] گزارش شده است. این الگوریتم بر سه تابع پنهانی متکی است که در دو الگوریتم ارائه شده بکار رفته اند. یک نمودار بلوکی رمزگذاری الگوریتم و راه کار خلق امضا در شکل 13 نشان داده شده است. این راه کار یک رویکرد حلقه بسته را میپذیرد تا داده های امنیتی را ایجاد نماید. این حلقه با داده های پیکسل واضح شروع میشود و



شکل 13

با داده های پیکسل رمزگذاری شده تمام میشود. همانطور که در شکل نشان داده شده است، این راه کار با درهم سازی داده های پیکسل برای ایجاد کلید رمزگذاری و بردار شروع برای تابع AES-GCM برای رمزگذاری صفات خاصه محرمانه سرامد آغاز میشود. این حلقه با درهم سازی سرامد رمزگذاری شده ادامه می یابد تا کلید رمزگذاری و بردار شروع را برای تابع AES-GCM ایجاد نماید. این حلقه با رمزگذاری داده های پیکسل و ایجاد برچسب تایید اعتبار متناظر بسته میشود. کدهای درهم رمزگذاری شده در سرامد DICOM ذخیره نمیشود.

در مقایسه با الگوریتم های ارائه شده در این مقاله، الگوریتم [42] یک پیوند قوی بین موجودیتهای مختلف این الگوریتم را نشان میدهد و به فضای ذخیره سازی کمتری در سرامد DICOM نیاز دارد. با این حال، یک تحلیل کامل از این الگوریتم، یک نقص امنیتی جدی را آشکار ساخت که به از دست دادن کامل محرمانه بودن، هم برای داده های سرامد و هم پیکسل منجر میگردد. دلیل این نقص این است که کلیدهای ایجاد شده به طور داخلی و بردارهای شروع، در سرامد DICOM به طور واضح ارسال شدند (رمزگذاری نشدند). بنابراین در مقایسه با الگوریتم های ارائه شده در این مقاله، الگوریتم گزارش شده در [42] تایید اعتبار و یکپارچگی داده های سرامد و پیکسل تصاویر DICOM را کسب میکند، در حالیکه محرمانه بودن، بدست نمی آید. این الگوریتم با استاندارد DICOM و طرح کوبایاشی در جدول 3 مقایسه میشود.

برای نتیجه گیری، دو الگوریتم مبتنی بر رمز ارائه شده، برای ارائه محرمانه بودن، اعتبار و یکپارچگی برای فایلهای DICOM بین موجودیتهای پزشکی توسعه یافته است. برخلاف استاندارد DICOM و سایر الگوریتم های پنهانی مبتنی بر DICOM، الگوریتم های ارائه شده، سرویسهای امنیتی لازم برای داده های پیکسل هم چنین برای داده های سرامد را ارائه میدهند. ارائه سرویسهای امنیتی برای سرامد، مهم است زیرا شامل داده های محرمانه میشود که باید در طول ارسال حفاظت شوند و در پایانه دریافت کننده پیش از اینکه مورد استفاده اهداف تشخیصی قرار گیرند، تایید شوند. الگوریتم ها با استفاده از مقدمات پنهانی قوی اجرا شدند: AES-GCM، تابع درهمسازی گردابی و ECDSA. عملکرد موثر الگوریتم ها، به صورت منعکس شده از طریق نتایج حاصله برای همبستگی، آنتروپی، PSNR، تحلیل هیستوگرام و نیرومندی در برابر حملات پردازش سیگنال کسب شده است.

به عنوان یک تحقیق در حال پیشروی، اخیرا بر روی توسعه الگوریتم های ارائه شده برای رسیدگی به تصاویر پزشکی DICOM چند تکه ای و چند قابی کار میکنیم. برای آینده، یک طرح مکان یابی مداخله را ادغام میکنیم تا یکپارچگی مبتنی بر محتوا را به جای عاملیت یکپارچگی محض مد نظر قرار دهیم که با الگوریتم های کنونی اجرا شده است. مکان یابی مداخله یک عاملیت مفید محسوب میشود زیرا کنترل یکپارچگی بر مبنای حفاظت دقیق کل بخشهای تصویر ممکن است به طور غیر ضروری محض باشد زیرا اعواجها بر روی تصویر همچنین ممکن است به خاطر نویزی باشد که از فرایند ارسال نشات میگیرد.