نشریه علمی-تخصصی
پژوهش های نوین علوم مهندسی
ISSN: 2538-3809
سال ششم، شماره ۲ (پیاپی: ۳۴)، تابستان ۱۴۰۰

پنهان‌کاری در انتقال داده‌های پزشکی ایمن برای سیستم‌های مراقبت بهداشتی مبتنی بر IoT

تورج استواری[۱]

تاریخ دریافت: ۱۴۰۰/۰۶/۰۳
تاریخ پذیرش: ۱۴۰۰/۰۶/۲۶
کد مقاله: ۳۵۲۵۰

چکـیده

با توجه به پیشرفت قابل‌توجه IoT در بخش مراقبت‌های بهداشتی، امنیت و یکپارچگی داده‌های پزشکی برای برنامه‌های خدمات بهداشتی درمانی به چالش‌های بزرگی تبدیل شدند. در این مقاله یک مدل امنیتی ترکیبی برای ایمن‌سازی داده‌های متن تشخیصی در تصاویر پزشکی پیشنهاد شده است. مدل پیشنهادی از طریق تلفیق تکنیک پنهان نگاری دوبعدی[۲] با یک طرح رمزگذاری ترکیبی پیشنهاد شده است. طرح پیشنهادی رمزگذاری ترکیبی با استفاده از ترکیبی از الگوریتم‌های رمزگذاری پیشرفته[۳] و Rivest، Shamir و Adleman (RSA) ساخته شده است. مدل پیشنهادی با رمزگذاری داده‌های مخفی آغاز می‌شود. سپس با استفاده از 2D-DWT-2L نتیجه را در یک عکس روی جلد مخفی می‌کند. هر دو عکس رنگی و مقیاس خاکستری به‌عنوان تصاویر پوششی برای پنهان کردن اندازه متن مختلف استفاده می‌شود.

واژگـان کلـیدی: پنهان کاری، رمزنگاری، تصاویر پزشکی، IoT

۱- کارشناسی مهندس نرم افزار دانشگاه فنی و حرفه‌ای شماره یک، تبریز ایران (نویسنده مسئول)
Toraj.ostovari@gmail.com

2 Discrete Wavelet Transform 2 Level (2D-DWT-2L)

3 Advanced Encryption Standard (AES)

۱- مقدمه

IoT با درگیرکردن دنیای فیزیکی با هم یک محیط ارتباطی یکپارچه از دستگاه‌ها و سیستم‌عامل‌های متصل‌به‌هم ایجاد می‌شود [۱]. با ظهور سیستم‌های اینترنت اشیا مبتنی بر مراقبت‌های بهداشتی از راه دور، انتقال داده‌های پزشکی به روال روزمره تبدیل می‌شود؛ بنابراین، تهیه یک مدل کارآمد برای اطمینان از امنیت و یکپارچگی داده‌های تشخیصی بیمار که از محیط IoT انتقال و دریافت می‌شود، ضروری است [۲] – [۸]. این هدف با استفاده از تکنیک‌های پنهان نگاری و الگوریتم‌های رمزگذاری سیستم برای مخفی کردن اطلاعات دیجیتالی در یک تصویر [۹] – [۱۶] انجام شده است. رمزنگاری اصطلاح دیگری برای رمزگذاری داده است [۱۷] رمزنگاری فرایند رمزگذاری پیام‌ها به شکلی است که هکرها نمی‌توانند آن را بخوانند، اما افراد مجاز می‌توانند از آن استفاده کرد. دو الگوریتم اصلی که برای رمزگذاری داده‌ها در این کار استفاده می‌شود، رمزگذاری پیشرفته استاندارد (AES) و الگوریتم Rivest-Shamir-Adleman (RSA) [۱۸] هستند. AES یک رمز رمزگذاری است که در آن دو کلید از همان کلید استفاده می‌شود [۱۹]. پیام دارای پیام ثابت ۱۲۸ بیتی متن (ساده یا رمزنگاری) و کلیدهایی با طول ۱۲۸ ، ۱۹۲ یا ۲۵۶ بیت است. با ارسال پیام‌های طولانی‌تر، آنها به بلوک‌های ۱۲۸ بیتی تقسیم می‌شوند. ظاهراً کلیدهای طولانی‌تر رمزگشایی را دشوارتر می‌کند، همچنین سربار فرایند رمزگذاری و رمزگشایی طولانی‌تری را نیز اعمال می‌کند. برعکس، RSA الگوریتم کلید عمومی است که به طور گسترده در بخش‌های ارتباطات شخصی استفاده می‌شود [۲۰]. این مزیت داشتن یک اندازه کلید متغیر است که از (۲–۲۰۴۸) بیت برخوردار است. تحقیقات اولیه در پنهان کردن داده‌ها با پنهان‌نگاری آغاز شد که به علم و هنر پنهان کردن اشاره دارد. منظور انتقال اطلاعات مبتنی بر سیستم‌های بهداشتی در یک تصویر است. مزیت پنهان نگاری این است که می‌توان از آن برای انتقال پیام‌های طبقه‌بندی‌شده بدون اینکه واقعیت انتقال مشخص شود استفاده کرد. DWT دارای مکان‌یابی فضایی، گسترش فرکانس و ویژگی‌های چند وضوح فوق‌العاده است که با تئوری اشکال در سیستم بینایی انسان مطابقت دارد. این مقاله هر دو مرحله ۱ و ۲ سطح پنهان‌کاری DWT را که در دامنه فرکانس کار می‌کنند، پیاده‌سازی می‌کند. این تصویر را به قسمت‌هایی با تکرار زیاد و کم تقسیم می‌کند. بخش تکرار زیاد شامل اطلاعات لبه است، درحالی‌که قسمت تکرار کم غالباً به قطعات با تکرار زیاد و کم تقسیم می‌شود [۲۱].

هدف از پنهان‌نگاری نه‌تنها جلوگیری از دانستن اطلاعات پنهان توسط سرپرستان، بلکه رفع سوظن در داشتن اطلاعات پنهان است. پیام یک سند محرمانه است که باید در حامل منتقل شود و از آن استفاده شود، بنابراین تشخیص آن دشوار می‌شود. در هر سیستم پنهان نگاری دو جنبه اصلی وجود دارد که عبارت‌اند از ظرفیت پنهان‌نگاری و عدم محسوس بودن. ازاین‌رو، این دو خاصیت با هم گیج‌کننده هستند زیرا افزایش ظرفیت در عین حفظ نامحسوس بودن پنهان نگاری از سیستم پنهان نگاری سخت است. علاوه بر این، هنوز روش‌های محدودی برای پنهان کردن اطلاعات برای استفاده با پروتکل‌های ارتباطی انتقال داده وجود دارد که می‌تواند غیرمتعارف باشد اما آینده آنها امیدوارکننده نیست. این مقاله با هدف بهبود امنیت انتقال داده‌های پزشکی بر اساس ادغام بین یک روش پنهان نگاری و یک طرح رمزگذاری ترکیبی برای یک سیستم مراقبت بهداشتی با امنیت بالا دریافت کنید. این مقاله در پنج بخش از جمله این بخش سازمان‌یافته است. بخش ۲ کارهای مرتبط را نشان می‌دهد؛ بخش ۳ مدل پیشنهادی و الگوریتم‌های آنها را توضیح می‌دهد؛ بخش ۴ نتایج آزمایشی و بحث‌های آنها را ارائه می‌دهد و بخش ۵ نتیجه‌گیری اصلی را خلاصه می‌کند.

۲- کارهای مرتبط

شباهات و همکاران [۲]، یک مطالعه جامع درباره مسائل امنیتی در شبکه‌های اینترنت اشیا را مورد بررسی قرار داد. در این پژوهش نیازهای امنیتی مختلف، احراز هویت، محرمانه بودن موردبحث قرار گرفت. یک مطالعه تطبیقی انواع مختلف حملات، رفتارهای نامناسب و میزان تهدید آنها که در سطح پایین، متوسط ، سطح بالا و بسیار سطح بالا طبقه‌بندی‌شده است حملات و راه‌حل‌های احتمالی برای مواجهه با این حملات ارائه شده است. بایراگیت [۳]، سه روش پنهان‌کاری تصویر رنگی را برای محافظت از اطلاعات در زیرساخت IoT پیشنهاد کرده است. رویکرد اول و سوم از سه کانال (قرمز، سبز و آبی) استفاده می‌کند، درحالی‌که رویکرد دوم از دو کانال (سبز و آبی) برای انتقال اطلاعات استفاده می‌کند. از تکنیک‌های ترکیب‌بندی پویا برای مخفی کردن اطلاعات در لایه عمیق کانال‌های تصویر با کمک کلید مخفی به اشتراک گذاشته شده استفاده شده است. انوارت و همکاران [۴]، تکنیکی را برای ایمن‌سازی هر نوع عکس به‌ویژه تصاویر پزشکی ایجاد کرد. این اهداف برای حفظ یکپارچگی اطلاعات پزشکی الکترونیکی، اطمینان از در دسترس بودن این اطلاعات و تأیید صحت این اطلاعات برای اطمینان از اینکه افراد مجاز فقط می‌توانند اطلاعات را به دست آورند، حفظ می‌شود. ابتدا روش رمزگذاری AES در قسمت اول اعمال شد. تصویر گوش نیز در این اثر تعبیه شده است، جایی که هفت مقدار به‌عنوان بردار ویژگی از تصویر گوش استخراج شده است. این تکنیک پیشنهادی امنیت تصاویر پزشکی را از طریق ارسال آنها از طریق اینترنت بهبود بخشیده و از دسترسی افراد غیرمجاز به این تصاویر اطمینان حاصل

می‌کند. باتوجه‌به استانداردهای عامل خطر، این برنامه‌ها را می‌توان به نظارت از راه دور، پشتیبانی تشخیصی، پشتیبانی درمانی، اطلاعات پزشکی، آموزش و آگاهی و ارتباطات و آموزش برای کارکنان مراقبت‌های بهداشتی دسته‌بندی کرد. هشت آسیب‌پذیری امنیتی و ده عامل خطر توسط سازمان بهداشت جهانی شناسایی شده است (پروژه امنیت تلفن همراه OWASP) در سال ۲۰۱۴ مورد تجزیه‌وتحلیل قرار گرفته است. رزاق و همکاران[۹]، یک روش امنیتی ترکیبی را برای رمزگذاری، پنهان‌کاری و تکنیک‌های علامت‌گذاری کرده است. این به سه مرحله تجزیه شد. (۱) رمزگذاری تصویر با استفاده از عملیات XOR ، (۲) فرایند تعبیه با استفاده از حداقل بیت‌های قابل‌توجه (LSB) برای تولید تصویر پنهان‌کاری، و سپس (۳) علامت‌گذاری عکس پنهان‌کاری در هر دو دامنه فرکانس و مکان. نتایج تجربی ثابت کرد که روش پیشنهادی بسیار کارآمد و ایمن است. جینت و همکاران [۱۱]، با پنهان کردن داده‌ها با استفاده از مفهوم درخت تصمیم، تکنیک جدیدی را برای انتقال اطلاعات پزشکی بیمار به تصویر پوششی پزشکی ارائه دادند. کدگذاری در فرم بلوک‌های مختلفی که به طور مساوی تقسیم می‌شوند. در پنهان‌سازی، بلوک‌های کد مخفی به تصویر روی جلد اختصاص داده می‌شود تا داده‌ها را با استفاده از مکانیسم نقشه‌برداری بر اساس جستجوی اولین و اول قرار دهد. الگوریتم RSA برای رمزگذاری داده‌ها قبل از جاسازی استفاده شده است.

یحیات و همکاران [۱۲]، برنامه‌های مختلف مراقبت‌های بهداشتی مبتنی بر شبکه حسگر پزشکی بی‌سیم (WMSN) را بررسی کرد که می‌تواند در محیط اینترنت اشیا اجرا شود. همچنین، درباره تکنیک‌های امنیتی که برای رسیدگی به مسائل امنیتی سیستم‌های مراقبت‌های بهداشتی به‌ویژه تکنیک‌های امنیتی ترکیبی استفاده می‌شود، بحث شد. فایو و زاو [۱۳]، الگوریتمی بر اساس تقسیم تصویر اصلی به گروه بلوک‌ها ارائه دادند، جایی که این بلوک‌ها به‌صورت چرخش با استفاده از یک الگوریتم ترانس تشکیل پس از آن، رمزگذاری تصویر تبدیل شده با استفاده از الگوریتم Blowfish صورت پذیرفت. مشخص شد که همبستگی کاهش می‌یابد و با افزایش تعداد بلوک از طریق استفاده از اندازه بلوک‌های کوچک‌تر، آنتروپی افزایش می‌یابد. باریجو و اسکوریتی [۲۱] ، یک سیستم تأیید صحت پزشکی را برای بهبود امنیت تصویر پزشکی پیشنهاد کردند. سیستم پیشنهادی عمدتاً به دو مرحله تجزیه می‌شود: حفاظت و تأیید. از طریق مرحله محافظت، فرم دودویی داده‌های مخفی با استفاده از تکنیک دامنه فرکانس 2D Haar DWT در قسمت با فرکانس بالا (HH) تعبیه شده است. از طریق مرحله هشدار، الگوریتم استخراج برای بازیابی تصویر اصلی و داده‌های مخفی استفاده می‌شود.

۳- مدل پیشنهادی و الگوریتم‌ها

این مقاله یک مدل امنیتی مراقبت‌های بهداشتی را برای تأمین امنیت انتقال داده‌های پزشکی در محیط اینترنت اشیا ارائه می‌دهد. مدل پیشنهادی شامل چهار فرایند ترتیبی است:

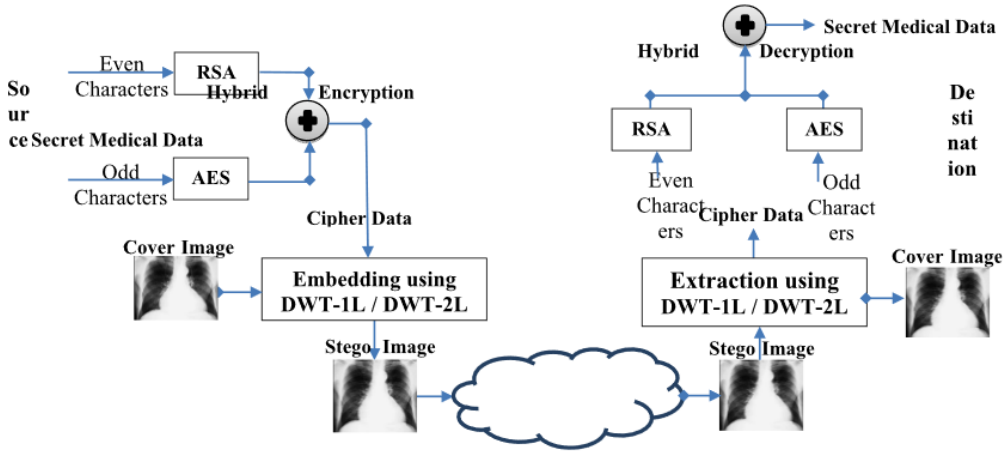
(۱) داده‌های بیمار محرمانه با استفاده از یک طرح رمزگذاری ترکیبی پیش‌فرض رمزگذاری می‌شود که از الگوریتم‌های رمزگذاری هر دو AES و RSA ساخته شده است.

(۲) داده‌های رمزگذاری شده با استفاده از 2D-DWT-1L یا 2D-DWT-2L در یک تصویر روی جلد مخفی می‌شوند و یک تصویر پنهان‌نگاری تولید می‌کنند.

(۳) داده‌های جاسازی شده استخراج می‌شوند.

(۴) داده‌های استخراج شده برای بازیابی داده‌های اصلی رمزگشایی می‌شوند.

شکل زیر چارچوب کلی مدل پیشنهادی ما را برای ایمن‌سازی انتقال مضمون داده در دو طرف منبع و مقصد نشان می‌دهد.



شکل ۱: چارچوب پیشنهادی برای اطمینان از انتقال داده‌های پزشکی.

۴ – نتایج آزمایشی

عملکرد سیستم پیشنهادی بر اساس شش پارامتر آماری ارزیابی شد. نسبت اوج سیگنال به نویز در تصاویر[1]، میانگین مربعات خطا[2]، نرخ خطای بیت[3]، شباهت ساختاری[4]، محتوای ساختاری[5] و همبستگی. در مقایسه با روش‌های پیشرفته، مدل پیشنهادی توانایی پنهان کردن اطلاعات بیمار محرمانه را در یک تصویر روی جلد منتقل شده با غیرقابل‌مشاهده بودن بالا، ظرفیت و حداقل خرابی در تصویر پنهان‌کاری دریافت شده، اثبات کرد. شکل‌های ۲ و ۳، خروجی آزمایش‌ها را نشان می‌دهند.

Image	Text Size (byte)	PSNR	MSE	BER	SSIM	SC	Correlation
Image(1)	15	56.60	0.14	0	1	1	1
	30	53.48	0.29	0	1	1	1
	45	51.65	0.44	0	1	1	1
	55	51.91	0.41	0	1	1	1
	100	52.46	0.37	0	1	1	1
	128	50.70	0.55	0	1	1	1
	256	51.66	0.44	0	1	1	1
Image(2)	15	56.60	0.14	0	1	1	1
	30	53.48	0.29	0	1	1	1
	45	51.62	0.45	0	1	1	1
	55	51.88	0.42	0	1	1	1
	100	52.45	0.37	0	1	1	1
	128	50.65	0.56	0	1	1	1
	256	51.60	0.45	0	1	1	1
Image(3)	15	56.24	0.15	0	1	1	1
	30	53.42	0.29	0	1	1	1
	45	51.56	0.45	0	1	1	1
	55	51.82	0.43	0	1	1	1
	100	52.40	0.37	0	1	1	1
	128	50.59	0.57	0	1	1	1
	256	51.49	0.46	0	1	1	1
Image(4)	15	56.39	0.15	0	1	1	1
	30	54.25	0.24	0	1	1	1
	45	52.42	0.37	0	1	1	1
	55	52.37	0.38	0	1	1	1
	100	53.78	0.27	0	1	1	1
	128	51.79	0.48	0	1	1	1
	256	51.27	0.43	0	1	1	1
Image(5)	15	57.44	0.12	0	1	1	1
	30	56.42	0.29	0	1	1	1
	45	53.66	0.37	0	1	1	1
	55	51.69	0.38	0	1	1	1
	100	51.88	0.30	0	1	1	1
	128	52.66	0.49	0	1	1	1
	256	50.58	0.41	0	1	1	1

شکل ۲: نتایج شش پارامتر آماری بدست آمده از عملکرد (D-DWT-2L۲) با طرح ترکیبی (AES و RSA) در تصاویر رنگی با اندازه متن مختلف.

1 Peak Signal to Noise (PSNR)
2 Mean Square Error (MSE)
3 Bit Error Rate (BER)
4 Structural Similarity (SSIM)
5 Structural Content (SC)

Image	Text Size (byte)	PSNR	MSE	BER	SSIM	SC	Correlation
Image(1)	15	56.04	0.16	0	1	1	1
	30	53.43	0.29	0	1	1	1
	45	51.59	0.45	0	1	1	1
	55	51.81	0.42	0	1	1	1
	100	52.44	0.37	0	1	1	1
	128	50.60	0.56	0	1	1	1
	256	51.49	0.46	0	1	1	1
Image(2)	15	56.05	0.16	0	1	1	1
	30	53.43	0.29	0	1	1	1
	45	51.58	0.45	0	1	1	1
	55	51.79	0.43	0	1	1	1
	100	52.46	0.36	0	1	1	1
	128	50.57	0.56	0	1	1	1
	256	51.42	0.46	0	1	1	1
Image(3)	15	56.00	0.16	0	1	1	1
	30	53.42	0.29	0	1	1	1
	45	51.60	0.44	0	1	1	1
	55	51.77	0.43	0	1	1	1
	100	52.50	0.35	0	1	1	1
	128	50.52	0.57	0	1	1	1
	256	51.34	0.47	0	1	1	1
Image(4)	15	56.39	0.14	0	1	1	1
	30	54.01	0.24	0	1	1	1
	45	53.87	0.37	0	1	1	1
	55	52.42	0.37	0	1	1	1
	100	53.78	0.27	0	1	1	1
	128	51.27	0.48	0	1	1	1
	256	51.13	0.42	0	1	1	1
Image(5)	15	56.09	0.15	0	1	1	1
	30	53.56	0.27	0	1	1	1
	45	52.35	0.43	0	1	1	1
	55	52.33	0.42	0	1	1	1
	100	53.23	0.35	0	1	1	1
	128	51.17	0.56	0	1	1	1
	256	51.94	0.46	0	1	1	1

شکل ۳: نتایج شش پارامتر آماری بدست آمده از عملکرد (D-DWT-2L۲) با طرح ترکیبی (AES و RSA) در تصاویر خاکستری با اندازه متن مختلف.

۵- نتیجه‌گیری

انتقال داده‌ها از طریق هر کانال ارتباطی به تکنیک‌های رمزگذاری قوی به‌منظور امنیت داده‌ها نیاز دارد. اینترنت اشیا[1] با درگیرکردن هر دودنیای مجازی و فیزیکی با یکدیگر، یک فضای ارتباطی یکپارچه از دستگاه‌ها و سیستم‌عامل‌های به‌هم‌پیوسته را ایجاد می‌کند. عملکرد مدل ما با تکنیک دیگری که توسط انوارت و همکاران توسعه داده شد مقایسه شد [۴]. در ۲۵۶ × ۲۵۶ پیکسل تصویر رنگی پزشکی با استفاده از اندازه متن ۱۸ بایت، دو روش با هم مقایسه شدند. شکل ۲ و ۳ نشان می‌دهد که مقادیر PSNR و MSE را با استفاده از مدل‌های ما در مقایسه با نتایج حاصل از [۴] به دست آورده است. نتایج به‌دست‌آمده پس از استفاده از مدل‌ها روی تصاویر پزشکی ۲۵۶ ۲۵۶ ۲۵۶ رنگی با اندازه متن ۱۸ بایت است. مشخص شد که مدل پیشنهادی ما دارای ارزش PSNR بالاتر و مقدار MSE کوچک‌تر است که عملکرد بالاتر مدل پیشنهادی ما را نشان می‌دهد.

1 Internet of things (IoT)

منابع

[1] A. Darwish, A. E. Hassanien, M. Elhoseny, A. K. Sangaiah, andK. Muhammad, ‘‘The impact of the hybrid platform of Internet of Thingsand cloud computing on healthcare systems: Opportunities, challenges,and open problems,’’J. Ambient Intell. Humanized Comput., to be pub-lished, doi:https://doi.org/10.1007/s12652-017-0659-1

[2] A. Shehabet al., ‘‘Secure and robust fragile watermarking schemefor medical images,’’IEEE Access, vol. 6, pp. 10269–10278, 2018,doi: 10.1109/ACCESS.2018.2799240.

[3] A. K. Bairagi, R. Khondoker, and R. Islam, ‘‘An efficient stegano-graphic approach for protecting communication in the Internet of Things(IoT) critical infrastructures,’’Inf. Secur. J., Global Perspect., vol. 25,nos. 4–6, pp. 197–212, 2016.

[4] A. S. Anwar, K. K. A. Ghany, and H. El Mahdy, ‘‘Improving the securityof images transmission,’’Int. J. Bio-Med. Inform. e-Health, vol. 3, no. 4,pp. 7–13, 2015.

[5] A. Abdelaziz, M. Elhoseny, A. S. Salama, and A. M. Riad, ‘‘A machinelearning model for improving healthcare services on cloud computingenvironment,’’Measurement, vol. 119, pp. 117–128, Apr. 2018. [Online].Available: https://doi.org/10.1016/j.measurement.2018.01.022

[6] M. Paschou, E. Sakkopoulos, E. Sourla, and A. Tsakalidis, ‘‘Health Inter-net of Things: Metrics and methods for efficient data transfer,’’Simul.Model. Pract. Theory, vol. 34, pp. 186–199, May 2013.

[7] M. Sajjadet al., ‘‘Raspberry Pi assisted face recognition frameworkfor enhanced law-enforcement services in smart cities,’’Future Gen-erat. Comput. Syst., to be published, doi:https://doi.org/10.1016/j.future.2017.11.013

[8] P. Kumar and H.-J. Lee, ‘‘Security issues in healthcare applications usingwireless medical sensor networks: A survey,’’Sensors, vol. 12, no. 1,pp. 55–91, 2012.

[9] M. A. Razzaq, R. A. Shaikh, M. A. Baig, and A. A. Memon, ‘‘Digitalimage security: Fusion of encryption, steganography and watermarking,’’Int. J. Adv. Comput. Sci. Appl., vol. 8, no. 5, pp. 224–228, 2017.

[10] N. Dey and V. Santhi,Intelligent Techniques in Signal Processing for Mul-timedia Security. New York, NY, USA: Springer, 2017, doi:10.1007/978-3-319-44790-2.

[11] M. Jain, R. C. Choudhary, and A. Kumar, ‘‘Secure medical image steganog-raphy with RSA cryptography using decision tree,’’ inProc. 2nd Int. Conf.Contemp. Comput. Inform. (IC3I), Dec. 2016, pp. 291–295.

[12] L. Yehia, A. Khedr, and A. Darwish, ‘‘Hybrid security techniques forInternet of Things healthcare applications,’’Adv. Internet Things, vol. 5,pp. 21–25, Jul. 2015.

[13] Z. M. Zaw and S. W. Phyo, ‘‘Security enhancement system based on theintegration of cryptography and steganography,’’Int. J. Comput., vol. 19,no. 1, pp. 26–39, 2015.

[14] R. K. Gupta and P. Singh, ‘‘A new way to design and implementation ofhybrid crypto system for security of the information in public network,’’Int. J. Emerg. Technol. Adv. Eng., vol. 3, no. 8, pp. 108–115, 2013.

[15] S. A. Laskar and K. Hemachandran, ‘‘High capacity data hiding using LSBsteganography and encryption,’’Int. J. Database Manage. Syst., vol. 4,no. 6, p. 57, 2012.

[16] L. Yu, Z. Wang, and W. Wang, ‘‘The application of hybrid encryptionalgorithm in software security,’’ inProc. 4th Int. Conf. Comput. Intell.Commun. Netw. (CICN), Nov. 2012, pp. 762–765.

[17] S. F. Mare, M. Vladutiu, and L. Prodan, ‘‘Secret data communicationsystem using steganography, AES and RSA,’’ inProc. IEEE 17th Int. Symp.Design Technol. Electron. Packag. (SIITME), Oct. 2011, pp. 339–344.

[18] A. K. Mandal, C. Parakash, and A. Tiwari, ‘‘Performance evaluation ofcryptographic algorithms: DES and AES,’’ inProc. IEEE Students’ Conf.Elect., Electron. Comput. Sci. (SCEECS), Mar. 2012, pp. 1–5.

[19] S. F. Mjolsnes, Ed.,A Multidisciplinary Introduction to Information Secu-rity. Boca Raton, FL, USA: CRC Press, 2011.

[20] R. L. Rivest, A. Shamir, and L. Adleman, ‘‘A method for obtaining digitalsignatures and public-key cryptosystems,’’Commun. ACM, vol. 21, no. 2,pp. 120–126, 1978.

[21] M. S. Sreekutty and P. S. Baiju, ‘‘Security enhancement in image steganog-raphy for medical integrity verification system,’’ inProc. Int. Conf. Circuit,Power Comput. Technol. (ICCPCT), Apr. 2017, pp. 1–5.

پیوست:

لینک دریافت پروژه:

https://mega.nz/file/JO5WDQqA#6Aa-gV1_7IE67KIpVnkPX4cOXKK1Tk2xF64-T5j_iyU