Information Technology Innovations and Applied Communication
Vol. 4, No. 1, Spring, 2026, Serial No. 9,pp.1-15

A Dynamic Approach to Elevating the Security of Industrial Digital Twins Through Innovative Multi-Layer Steganography Leveraging Internet of Things Infrastructure

Mohammadreza Tamimian[1] , Meghdad Aynehband*[2], Mina MoeinPoor[3]

* Assistant Professor in Islamic Azad University, Mahshahr branch, Mahshahr, Iran

(**Received:** 13 March 2026, **Revised:** 14 April 2026, **Accepted:** 06 May 2026, **Published:** 22 May 2026)

ABSTRACT

The Internet of Things (IoT) is an essential network of interconnected physical devices, electronic systems, and software that facilitates seamless, real-time data exchange. The rapid growth and widespread adoption of the Internet have fundamentally transformed personal and organizational lifestyles, revolutionizing how individuals and institutions operate and interact. IoT exemplifies how diverse physical objects and devices can be integrated with the Internet to collaborate and achieve shared goals. Despite the considerable convenience and efficiency offered by IoT devices, security concerns cannot be ignored—they are often grossly underestimated. The lack of robust protection mechanisms puts sensitive personal information at significant risk of breaches and unauthorized access. Ensuring the confidentiality and integrity of data transmitted across IoT networks is a paramount challenge. Without adequate security measures, information exchanged over the Internet remains dangerously vulnerable to interception and hacking by malicious actors. Addressing these security challenges demands a proactive, multifaceted approach. Information security is comprised of three critical dimensions—watermarking, encryption, and digital data steganography—each of which plays a crucial role in mitigating risks. This thesis will assertively focus on the application of digital image steganography, specifically harnessing the Least Significant Bit (LSB) and Most Significant Bit (MSB) techniques, to significantly enhance data security within IoT communications.

Keywords: Digital Twin Security, Security of Internet of things (IOT), Steganography, Cryptography, LSB, MSB

* Corresponding Author E-mail: me.aynehband@iau.ac.ir

«نوآوری‌های فناوری اطلاعات و ارتباطات کاربردی»
سال چهارم، شماره 1، فصل بهار 1405؛ ص 15-1.

علمی- پژوهشی

روشی برای بهبود امنیت همزاد دیجیتال صنعتی با استفاده از پنهان‌نگاری چندلایه مبتنی بر زیرساخت اینترنت اشیا

محمدرضا طمیمیان[1]؛ مقداد آینه‌بند[2]* ؛ مینا معین‌پور[3]

1- استادیار دانشکده برق و کامپیوتر، گروه کامپیوتر، واحد ماهشهر، دانشگاه آزاد اسلامی، ماهشهر، ایران.
2- دانشجوی دکتری، گروه کامپیوتر، واحد دزفول، دانشگاه آزاد اسلامی، دزفول، ایران.
3- دبیر آموزش‌وپرورش، استان تهران، تهران، ایران.

(**دریافت:** 22 اسفند 1404 **بازنگری:** 26 فروردین 1405 **پذیرش:** 16 اردیبهشت 1405 انتشار: 01 خرداد 1405)

چکیده:

نهان‌نگاری[1] با مخفی‌کردن اطلاعات در محتوای معمولی (مانند تصاویر یا متن)، امنیت دوقلوی دیجیتال را افزایش می‌دهد. این روش محرمانگی را حفظ کرده و از دست‌کاری داده‌ها جلوگیری می‌کند، ارتباطات امن بین دستگاه‌های فیزیکی و دیجیتال را ممکن می‌سازد. اینترنت اشیا[2] (IoT) با اتصال دستگاه‌های هوشمند، تحولاتی مانند خودکارسازی و بهبود کارایی ایجاد کرده است، اما چالش‌های امنیتی مانند حملات سایبری و نقض حریم خصوصی را نیز به همراه دارد. دستگاه‌های IoT به دلیل پراکندگی و تنوع، هدف آسانی برای هکرها هستند که می‌توانند داده‌ها را سرقت یا کنترل دستگاه‌ها را به دست بگیرند. برای مقابله با این تهدیدات، روش‌هایی مانند رمزنگاری و نهان‌نگاری پیشنهادشده‌اند. ترکیب این دو روش می‌تواند امنیت اطلاعات را در IoT به طور چشمگیری افزایش دهد. با ادغام رمزنگاری (برای محافظت از محتوای داده) و نهان‌نگاری (برای پنهان‌سازی وجود داده)، سطح امنیتی بالاتری ایجاد می‌شود. این رویکرد نوین، ایمنی دستگاه‌ها و شبکه‌های IoT را بهبود بخشیده و امکان بهره‌مندی از مزایای این فناوری را بدون مواجهه با تهدیدات جدی فراهم می‌کند. با اجرای راهکارهای امنیتی مناسب، می‌توان از خطرات کاست و آینده‌ای امن برای اینترنت اشیا ساخت.

کلیدواژه‌ها: دوقلوی دیجیتال[3]، امنیت دوقلوی دیجیتال، پنهان‌نگاری، رمزنگاری، نهان‌نگاری، فن کم‌اهمیت‌ترین بیت، فن مهم‌ترین بیت.

* رایانامه نویسنده مسئول: E-mail: me.aynehband@iau.ac.ir

[1] Steganography
[2] IOT
[3] Digital twin

1. مقدمه

1-1- همزاد دیجیتال

ایده دوقلوهای دیجیتال نخستین‌بار در آغاز دهه ۱۹۹۰ توسط دیوید گلرنتر [1] در کتابش مطرح شد [1]. در سال ۱۹۹۱، این دانشمند علوم کامپیوتر از دانشگاه ییل[2]، مفهومی به نام "دنیای آینه‌ای[3]" را پیشنهاد داد. این اندیشه دربرگیرنده الگوهای رایانه‌ای از شهرها بود که همه ویژگی‌های یک شهر، به‌صورت تصویری متراکم، پویا، پرجنب‌وجوش و آکنده از جمعیت، بر روی یک صفحه‌نمایش نشان داده می‌شد. ارزش این دنیای آینه‌ای در توانایی آن برای ارائه یک دید کل‌نگر از مناطق شهری نهفته است، درحالی‌که به کاربران توانایی می‌دهد تا به داده‌های دقیق‌تری دسترسی پیدا کنند و درعین‌حال بافت فضایی منطقه را نگهداری کنند[2].

در سال ۲۰۰۲، مایکل گریوز [4]برای نخستین‌بار الگو مفهومی دوقلوهای دیجیتال را به‌منظور مدیریت چرخه عمر محصول در تولید معرفی کرد. هرچند او در ابتدا از نام‌هایی مانند "مدل فضایی آینه‌ای" و "مدل آینه‌ای اطلاعات" استفاده کرد، اما این مفهوم در سال ۲۰۱۷ توسط گریوز با عنوان «دوقلوی دیجیتال» تعریف شد: *دوقلوی دیجیتال مجموعه‌ای از ساختارهای مجازی اطلاعات است که به طور کامل یک محصول فیزیکی بالقوه یا واقعی تولیدشده را از سطح خرد اتمی تا سطح هندسی کلان توصیف می‌کند، در بهترین حالت هر اطلاعاتی که از بازرسی یک محصول تولیدشده فیزیکی به دست می‌آید را می‌توان از دوقلوی دیجیتال آن* به دست آورد [3].

دوقلوی دیجیتال از دیدگاه ریاضیات و محاسبات به‌عنوان یک مدل محاسباتی تعریف می‌شود که در طول زمان تکامل‌یافته و به طور مداوم نمایانگر یک دارایی فیزیکی منحصربه‌فرد است. این دوقلوها با ارائه امکان تحلیل دقیق دارایی و تصمیم‌گیری مبتنی بر داده، زیرساختی برای خودکارسازی هوشمند فراهم می‌کنند. ابتدا، پایه‌ای ریاضی یکپارچه برای دوقلوهای دیجیتال ایجادشده و سپس انتزاعی ریاضی از دوقلو و دارایی فیزیکی مرتبط با آن ارائه می‌شود. این انتزاع در ادامه به یک مدل گرافیکی احتمالی تبدیل می‌شود که تکامل دستگاه‌های جفت شده را توصیف می‌کند.

این مدل تمام جنبه‌های دوقلوی دیجیتال را به‌صورت یکپارچه در برمی‌گیرد و قابلیت پوشش‌دهی کل چرخه عمر دارایی را دارد. درعین‌حال که ازلحاظ ریاضی دقیق است، انعطاف‌پذیری و توسعه‌پذیری بالایی دارد و کاربرد آن را در حوزه‌های مختلف عملی ممکن می‌سازد. دوقلوهای دیجیتال با ترکیب مدل‌های پیشرفته محاسباتی، یادگیری مبتنی بر داده و هوش مصنوعی به‌عنوان یک پارادایم نوظهور برای نظارت، تحلیل و بهینه‌سازی دستگاه‌های پیچیده مطرح‌شده‌اند.

مدل‌سازی ریاضی دوقلوی دیجیتال شامل یک مدل محاسباتی یا مجموعه‌ای از مدل‌های کوپل شده است که در طول زمان تکامل می‌یابد تا ساختار، رفتار و زمینه دارایی فیزیکی منحصربه‌فردی همچون یک جزء سامانه یا فرایند را نمایش دهد. این پارادایم با ارائه مدلی دیجیتال، تطبیقی و جامع برای هر دارایی فیزیکی (که در این زمینه به‌عنوان قُل فیزیکی شناخته می‌شود)، محدودیت‌های شبیه‌سازی سنتی را در ویژگی‌ها برطرف می‌کند[4].

شویگرت رکسیک و همکاران ۲۰۲۰ میلادی [5] افزایش کاربرد و پیچیدگی مدل‌های شبیه‌سازی را عامل باز کردن بسیاری از پتانسیل‌های توسعه محصول مجازی بیان کرده‌اند. آن‌ها اشاره کرده‌اند درحالی‌که نرم‌افزارهای شبیه‌سازی قدرتمندتر شده‌اند، داده‌های ورودی موجود بیشتر در کانون تلاش‌ها برای افزایش مزایای بالقوه شبیه‌سازی محصول قرار می‌گیرند. اگر بتوان "داده‌های فاز استفاده[5]" را از برنامه‌های واقعی به مدل‌های شبیه‌سازی وارد کرد، یا از داده‌های فاز استفاده برای اعتبارسنجی نتایج شبیه‌سازی استفاده کرد، می‌توان مدل‌های شبیه‌سازی دقیق‌تری ساخت که درنهایت منجر به محصولات بهتری شود. اصطلاح داده فاز استفاده بر اساس تعریف ویلبرگ و همکاران ۲۰۱۷ میلادی [6] ساخته‌شده است که در آن به داده‌هایی اشاره دارد که در مرحله استفاده توسط خود محصول (به‌عنوان‌مثال، توسط حسگرها یا ریزپردازنده‌ها) یا توسط خدمات مرتبط (مانند برنامه‌ها، گزارش‌های نگهداری و تعمیر یا گزارش تعمیر اساسی) ایجاد می‌شود. شویگرت در ادامه چنین اتصالی بین مدل‌های شبیه‌سازی و داده‌های فاز استفاده را دوقلوی دیجیتال می‌خواند و در طرح موضوع دوقلوی دیجیتال در کاربردهای مهندسی مکانیک همچون صنعت دستگاه‌های گرمایش و سرمایش از تعریف تراثر و همکاران (۲۰۲۰ میلادی) [7] استفاده می‌کند که در آن دوقلوی دیجیتال چنین تعریف‌شده است:

«نمایشی دینامیکی مجازی از یک سامانه فیزیکی که در کل چرخه عمر با تبادل داده‌های دو جهتِ به آن متصل است».



تصویر 1. مدل هوش مصنوعی فیزیک محور[6]

[1] David Gelernter
[2] Yale University
[3] Mirror Worlds
[4] Michael Grieves
[5] Use Phase Data
[6] ISaac Sim Nvidia

پس رابطه بین داده‌ها و شبیه‌سازی‌ها اهمیت می‌یابد و ازآنجاکه این تنها یک مهندسی مبتنی بر داده نیست، بلکه در کنار یادگیری ماشین همچنان از شبیه‌سازی مکانیکی یا شیمیایی بهره می‌برد، پس عبارتی تحت عنوان "یادگیری ماشین مبتنی بر فیزیک ML-Physics"[1] به وجود آمده است.

درواقع یادگیری ماشینی مبتنی بر فیزیک، جریان کاری را در شبیه‌سازی با سامانه‌های پردازش محاسبات با کارایی بالا[2] (HPC) در تمامی رشته‌ها، ازجمله دینامیک سیالات محاسباتی (CFD)، مکانیک ساختاری، شیمی محاسباتی و زیست محاسباتی تغییر می‌دهد. به دلیل کاربردهای گسترده یادگیری ماشین مبتنی بر فیزیک مسئله برای مدل‌سازی دستگاه‌های فیزیکی و استقرار دوقلوهای دیجیتال در صنایع مختلف از صنعت ساخت و تولید تا علوم آب‌وهوا مناسب است.

2-1- اینترنت اشیا زیرساخت حیاتی در همزاد دیجیتال

اینترنت اشیا نقشی حیاتی و زیرساختی در توسعه و عملکرد دوقلوی دیجیتال ایفا می‌کند. دوقلوی دیجیتال به مدل مجازی دقیق و پویا از یک سامانه، محصول، یا فرایند فیزیکی اشاره دارد که داده‌های واقعی آن در زمان واقعی جمع‌آوری، پردازش، و تحلیل می‌شوند. در این میان، اینترنت اشیا به‌عنوان یک پل ارتباطی بین دنیای فیزیکی و مجازی عمل می‌کند. در ادامه نقش زیرساختی اینترنت اشیا (IoT) در دوقلوی دیجیتال توضیح داده می‌شود:

1. جمع‌آوری داده‌ها از دنیای واقعی

دستگاه‌های اینترنت اشیا (IoT) مانند حس‌گرها، ابزارهای هوشمند و دستگاه‌های متصل، داده‌های لازم از دستگاه‌ها، محصولات یا فرایندهای فیزیکی را به‌صورت مستمر و در زمان واقعی جمع‌آوری می‌کنند. این داده‌ها شامل اطلاعاتی نظیر دما، فشار، ارتعاش، مکان، سرعت و دیگر عامل‌های عملکردی است که برای ایجاد و به‌روزرسانی دوقلوی دیجیتال ضروری هستند.

2. انتقال و ارتباطات داده

اینترنت اشیا از پروتکل‌ها و شبکه‌های ارتباطی مانند 5G، Wi-Fi، LoRaWAN و Zigbee استفاده می‌کند تا داده‌های جمع‌آوری‌شده را با سرعت و دقت بالا به پلتفرم‌های پردازش ابریا لبه[3] انتقال دهد. این ارتباط پایدار و سریع یکی از الزامات کلیدی برای عملکرد مؤثر دوقلوی دیجیتال است.

3. ادغام با فناوری‌های تحلیلی

داده‌های اینترنت اشیا (IoT) که از حس‌گرها جمع‌آوری می‌شوند، به کمک زیرساخت‌های تحلیلی پیشرفته مانند هوش مصنوعی[4] و یادگیری ماشین[5] پردازش و تحلیل می‌شوند. این تحلیل‌ها به دوقلوی دیجیتال اجازه می‌دهد که وضعیت فعلی سامانه را بازتاب دهد، پیش‌بینی‌های دقیقی انجام دهد و حتی به تصمیم‌گیری خودکار کمک کند.

4. پشتیبانی از همگام‌سازی زمان واقعی

اینترنت اشیا امکان همگام‌سازی لحظه‌ای داده‌های دنیای واقعی با مدل مجازی دوقلوی دیجیتال را فراهم می‌کند. این ویژگی به سازمان‌ها اجازه می‌دهد تا تغییرات و نوسانات سامانه فیزیکی را به طور دقیق در مدل دیجیتال مشاهده کرده و پاسخ مناسب ارائه دهند.

5. ایجاد بازخورد و کنترل

اینترنت اشیا (IoT) نه‌تنها داده‌ها را از دنیای فیزیکی به مدل دیجیتال منتقل می‌کند، بلکه می‌تواند از طریق دوقلوی دیجیتال دستورات یا اقدامات کنترلی را به دستگاه‌های فیزیکی ارسال کند. این قابلیت در حوزه‌هایی مانند مدیریت انرژی، تعمیرات پیش‌بینانِ، و بهینه‌سازی عملکرد، بسیار مهم است.

6. قابلیت گسترش و مقیاس‌پذیری

زیرساخت اینترنت اشیا (IoT) به دلیل قابلیت مقیاس‌پذیری خود، امکان توسعه و گسترش مدل‌های دوقلوی دیجیتال را فراهم می‌کند. به این معنا که می‌توان دستگاه‌های بیشتری را به شبکه متصل کرد و مدل‌های دیجیتال پیچیده‌تر و دقیق‌تری ایجاد نمود.

ازاین‌رو در دنیای روبه‌رشد اینترنت اشیا، حفاظت از داده‌های حساس در برابر تهدیدات سایبری از اهمیت حیاتی برخوردار است. پنهان‌نگاری، فن برای پنهان‌کردن اطلاعات در یک حامل بی‌ضرر مانند تصویر یا فایل صوتی، ازجمله راه‌حل‌های سنتی برای این چالش بوده است. بااین‌حال، ظهور هوش مصنوعی و پیشرفت‌های چشمگیر در پردازش تصویر، کارایی روش‌های پنهان‌نگاری سنتی را به‌شدت تحت‌الشعاع قرار داده است.

محدودیت‌های پردازشی ذاتی در سخت‌افزارهای اینترنت اشیا، آن‌ها را به استفاده از فن‌های پنهان‌نگاری ضعیف مانند کمترین بیت قابل‌تغییر[6] سوق می‌دهد. این روش‌ها به دلیل سادگی، به‌راحتی توسط مهاجمان شناسایی و مورد سوءاستفاده قرار می‌گیرند. درنتیجه، اطلاعات محرمانه جاسازی‌شده در تصاویر یا فایل‌های پوششی به طور فزاینده‌ای در معرض خطر افشا قرار می‌گیرند.

[1] Physics-Informed Machine Learning (physics-ML)
[2] High-Performance Computing
[3] Cloud or Edge Computing
[4] Artificial Inteligence
[5] Machine Learning
[6] Least Significant Bit (LSB)

این مقاله رویکردی نوین برای غلبه بر چالش‌های امنیتی پنهان‌نگاری در اینترنت اشیا به‌عنوان زیرساخت حیاتی در همزاد دیجیتال را ارائه می‌کند. ما با ادغام رمزنگاری و پنهان‌نگاری، سطح حفاظت از داده‌ها را به طور قابل‌توجهی ارتقا می‌دهیم. این روش ترکیبی، داده‌های حساس را قبل از پنهان‌کردن در یک حامل بی‌ضرر، با استفاده از الگوریتم‌های رمزنگاری قوی رمزگذاری می‌کند.

مزایای این روش عبارت‌اند از:

- امنیت چندلایه: رمزنگاری قبل از پنهان‌نگاری، یک‌لایه حفاظتی اضافی ایجاد می‌کند و حتی در صورت استخراج داده‌های پنهان‌شده توسط مهاجمان، رمزگشایی آن‌ها بدون کلید رمزگذاری غیرممکن می‌شود.
- مقاومت در برابر حملات مبتنی بر هوش مصنوعی: الگوریتم‌های رمزنگاری مدرن در برابر حملات شناخته‌شده مانند حمله حدس و گمان مصون هستند و از داده‌ها در برابر تهدیدات نوظهور مبتنی بر هوش مصنوعی محافظت می‌کنند.
- کارایی: روش‌های پنهان‌نگاری مدرن می‌توانند حجم قابل‌توجهی از داده‌ها را در تصاویر یا فایل‌های پوششی با حداقل اعوجاج پنهان کنند، بدون اینکه بر عملکرد سامانه‌های اینترنت اشیا تأثیر قابل‌توجهی بگذارند.

این مقاله با ارائه جزئیات دقیق پیاده‌سازی و ارزیابی تجربی کارایی و امنیت روش پیشنهادی، سهم ارزشمندی در زمینه امنیت اینترنت اشیا ارائه می‌دهد. یافته‌های این مطالعه نشان می‌دهد که ادغام رمزنگاری و پنهان‌نگاری می‌تواند به طور مؤثری امنیت داده‌ها را در اینترنت اشیا ارتقا دهد و از اطلاعات حساس در برابر دسترسی‌های غیرمجاز محافظت نماید.

1-3- چالش‌های پنهان‌نگاری سنتی در اینترنت اشیاء

- ضعف روش‌های پنهان‌نگاری: روش‌های سنتی مانند(LSB) کمترین بیت قابل‌تغییر به دلیل سادگی به‌راحتی قابل‌شناسایی و استخراج توسط مهاجمان هستند.
- محدودیت‌های پردازشی: سخت‌افزارهای اینترنت اشیا به دلیل محدودیت‌های پردازشی، قادر به اجرای الگوریتم‌های پنهان‌نگاری پیچیده نیستند.
- حجم کم داده: روش‌های پنهان‌نگاری سنتی به دلیل ظرفیت کم پنهان‌سازی داده، برای جاسازی حجم زیادی از اطلاعات مناسب نیستند.
- آسیب‌پذیری در برابر حملات مبتنی بر هوش مصنوعی: پیشرفت‌های هوش مصنوعی و پردازش تصویر، شناسایی و استخراج داده‌های پنهان‌شده را برای مهاجمان آسان‌تر می‌کند.

این مقاله رویکردی نوین برای غلبه بر چالش‌های امنیتی پنهان‌نگاری در اینترنت اشیا ارائه می‌کند که شامل مراحل زیر است:

- رمزنگاری: ابتدا داده‌های حساس با استفاده از الگوریتم‌های رمزنگاری قوی مانند استاندارد رمزگذاری پیشرفته[1] یا رمزنگاری کلید عمومی[2] رمزگذاری می‌شوند.
- پنهان‌نگاری: سپس، داده‌های رمزگذاری شده در یک حامل بی‌ضرر مانند تصویر یا فایل صوتی با استفاده از فن‌های پنهان‌نگاری مدرن مانند بنچمارکینگ[3] یا نهان‌نگاری[4] پنهان می‌شوند.
- کاربردها: این روش را می‌توان برای محافظت از انواع مختلف داده‌ها در اینترنت اشیا، ازجمله اطلاعات حسگر، تصاویر، ویدئوها و داده‌های متنی استفاده کرد.

1-4- پنهان‌نگاری: پنهان‌کردن اطلاعات در دنیای دیجیتال

- پنهان‌نگاری: هنر و علم پنهان‌کردن اطلاعات در یک شیء حامل دیگر، به‌گونه‌ای که وجود پیام پنهان غیرقابل‌تشخیص باشد، است. در این فرایند، شیء مخفی کننده که داده در آن پنهان می‌شود، "شیء حامل" نامیده می‌شود و شیء جدید حاصل‌شده "شیء پنهان‌نگاری شده" نامیده می‌شود.
- هدف پنهان‌نگاری: هدف اصلی پنهان‌نگاری، پنهان‌کردن وجود ارتباط یا پیامی است که در یک رسانه حامل جاسازی‌شده است. این امر می‌تواند برای مقاصد مختلفی ازجمله حفاظت از حریم خصوصی، ضد سانسور، احراز هویت و علامت‌گذاری مالکیت معنوی مورداستفاده قرار گیرد.

برخلاف رمزنگاری که فقط محتوای پیام را پنهان می‌کند، پنهان‌نگاری بر وجود پیام تمرکز دارد. به‌عبارت‌دیگر، رمزنگاری پیام را غیر قابل خواندن می‌کند، درحالی‌که پنهان‌نگاری پیام را از دید پنهان می‌کند.

پنهان‌نگاری می‌تواند در انواع مختلف داده‌ها ازجمله متن، تصویر، صوت و ویدئو اعمال شود و می‌تواند برای پنهان‌کردن هر نوع اطلاعات دیجیتالی مانند تصاویر، متن، فایل‌های صوتی و حتی کدهای برنامه‌نویسی استفاده شود. این روش‌ها به‌ویژه در مواردی که احراز هویت کاربر و حریم خصوصی داده‌ها از اهمیت بالایی برخوردار است، بسیار حائز اهمیت هستند.

---

[1] Advanced Encryption Standard (AES)
[2] Rivest–Shamir–Adleman (RSA)
[3] Benchmarking
[4] StegHide

فرایند پنهان‌نگاری دیجیتال

فرایند کلی پنهان‌نگاری دیجیتال شامل سه مرحله اصلی است:

- داده پنهان: داده‌ای که می‌خواهید پنهان کنید، می‌تواند شامل متن، تصاویر، فایل‌های صوتی یا هر نوع اطلاعات دیجیتالی دیگر باشد.
- فایل حامل: فایلی که داده پنهان در آن جاسازی می‌شود. این فایل می‌تواند متن، تصویر، صوت یا ویدئو باشد.
- فایل پنهان‌نگاری: فایل نهایی حاصل از فرایند پنهان‌نگاری که حاوی اطلاعات پنهان‌شده در داخل فایل حامل است.

فایل پوششی می‌تواند هر نوع فایلی باشد که به طور معمول قابل‌حمل و بدون جلب‌توجه باشد. به‌عنوان‌مثال، می‌توان از یک تصویر معمولی به‌عنوان فایل پوششی برای پنهان‌کردن متن یا یک فایل صوتی استفاده کرد.

هدف از فرایند پنهان‌نگاری، جاسازی داده پنهان در داخل فایل حامل به‌گونه‌ای است که وجود آن قابل‌تشخیص نباشد. این امر با استفاده از فن‌های مختلفی مانند تغییر بیت‌های کم‌اهمیت فایل پوششی، یا استفاده از فضای خالی موجود در فایل انجام می‌شود.

تعریف مسئله و سؤالات اصلی تحقیق

تاکنون در زمینه‌ی پنهان‌نگاری روش‌های متفاوتی استفاده‌شده است ازجمله رمزنگاری، نهان‌نگاری و نهان‌نگاری که در فصل‌های پیشین به آن‌ها پرداخته و با رسم شکل و مثال توصیف کرده‌ایم. اگرچه این امر خود نمایانگر پیشرفت روزافزون عرصه فنّاوری در زمینه اینترنت اشیا و تأمین امنیت اطلاعات سری است؛ چراکه با افزایش داده‌های در حال تبادل در اینترنت جلوگیری از دسترسی شخص ثالث به داده‌ها امری چالش‌برانگیز است.

هر یک از روش‌های مرسوم ازجمله مقایسه کمترین بیت قابل‌تغییر (LSB) و بااهمیت‌ترین بیت[1] (MSB) به شیوه‌ای امنیت اطلاعات سری را که در فایل رسانه تعبیه‌شده است را حفظ کرده؛ اما به دلیل ازدیاد خطرات سایبری و هکرها نیاز به روش‌های پیشنهادی نوینی است که بتواند جایگزینی برای روش‌های مرسوم و قدیمی باشد. در روش پیشنهادی باتوجه‌به اینکه هر دو روش پیشین شباهت‌ها و تفاوت‌هایی را دربر داشتند به عبارتی دیگر کمترین بیت قابل‌تغییر (LSB) از کم‌اهمیت‌ترین داده برای تعبیه فایل‌های سری موردنظر استفاده می‌کرد درحالی‌که بااهمیت‌ترین بیت (MSB) از مهم‌ترین داده را برای تعبیه داده موردنظر به کار می‌برد. اگرچه کمترین بیت قابل‌تغییر (LSB) روشی ساده‌تر و سریع‌تر است و بااهمیت‌ترین بیت (MSB) روشی ایمن‌تر و کارآمدتر است.

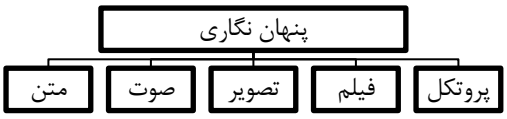
روش پیشنهادی، فن جدید، منحصربه‌فرد و مقرون‌به‌صرفه است که هم ازلحاظ ایمنی و هم ازلحاظ سرعت نسبت به روش قبلی برتری دارد که چالش ما را در این مسئله که چه‌کاری و چگونه آن را انجام دهیم تا در صورت دسترسی شخص ثالث به داده‌ها، وی نتواند متنی که در عکس تزریق کرده‌ایم را پیدا کند، حل کرده است.

در بخش دوم تحقیق به بررسی روش‌های موجود در پنهان‌نگاری و مزایا و معایب آن پرداخت‌شده است. در بخش سوم این تحقیق روش پیشنهادی شرح داده شده است. در چهارمین بخش نتایج پیاده‌سازی و قیاس با سایر روش‌ها مورد بحث واقع‌شده‌اند و نهایتاً بخش پنج نتیجه‌گیری و پیشنهادهای فعالیت‌های آینده بیان‌شده است.

2. روش تحقیق

2-1.انواع پنهان‌نگاری

انواع مختلفی از پنهان‌نگاری وجود دارد که هرکدام بر اساس نوع داده‌ای که در آن پنهان‌سازی انجام می‌شود، دسته‌بندی می‌شوند. برخی از رایج‌ترین انواع پنهان‌نگاری عبارت‌اند از:



شکل 1. انواع پنهان‌نگاری

- پنهان‌نگاری در متن: در این روش، اطلاعات پنهان در داخل یک فایل متنی؛ مانند یک رمان یا مقاله خبری جاسازی می‌شود.
- پنهان‌نگاری در تصویر: در این روش، اطلاعات پنهان در داخل یک تصویر مانند عکس یا نقاشی جاسازی می‌شود.
- پنهان‌نگاری در صوت: در این روش، اطلاعات پنهان در داخل یک فایل صوتی مانند آهنگ یا سخنرانی جاسازی می‌شود.
- پنهان‌نگاری در ویدئو: در این روش، اطلاعات پنهان در داخل یک فایل ویدئویی مانند فیلم یا کلیپ یوتیوب جاسازی می‌شود.

انتخاب نوع پنهان‌نگاری مناسب به عوامل مختلفی مانند نوع داده‌ای که باید پنهان شود، سطح امنیتی موردنیاز و نوع فایلی که به‌عنوان حامل استفاده می‌شود، بستگی دارد.

[1] Most Significant Bit Differencing (MSB)

2-2. کاربردهای پنهان‌نگاری

پنهان‌نگاری کاربردهای مختلفی در دنیای واقعی دارد، ازجمله:

- حفاظت از حریم خصوصی: می‌توان از پنهان‌نگاری برای پنهان‌کردن اطلاعات حساس مانند ایمیل‌ها، اسناد و تصاویر شخصی در برابر دید دیگران استفاده کرد.
- ضد سانسور: می‌توان از پنهان‌نگاری برای دورزدن سانسور و به‌اشتراک‌گذاری اطلاعات در کشورهایی که آزادی بیان در آن‌ها محدود است استفاده کرد.
- احراز هویت: می‌توان از پنهان‌نگاری برای جاسازی علامت‌های نامرئی در تصاویر یا فایل‌های صوتی برای تأیید صحت یا مالکیت استفاده کرد.
- علامت‌گذاری مالکیت معنوی: می‌توان از پنهان‌نگاری برای جاسازی اطلاعات مربوط به مالکیت معنوی در داخل تصاویر، موسیقی یا و غیره بهره برد.

3-2. چالش‌های پیش روی پنهان‌نگاری

باوجود مزایای متعدد، پنهان‌نگاری با چالش‌هایی نیز روبرو است. یکی از چالش‌های اصلی، یافتن تعادل بین ظرفیت پنهان‌سازی و شفافیت ادراکی است. روش‌های پنهان‌نگاری با ظرفیت پنهان‌سازی بالا ممکن است اعوجاج قابل‌توجهی در فایل حامل ایجاد کنند و به‌راحتی توسط مهاجمان شناسایی شوند. ازسوی‌دیگر، روش‌های با شفافیت ادراکی بالا، ظرفیت پنهان‌سازی محدودی دارند و حجم کمتری از اطلاعات را می‌توانند در خود ذخیره نمایند.

4-2. روش‌های پنهان‌نگاری

1-4-2. کم‌اهمیت‌ترین بیت (LSB)

پنهان‌نگاری مبتنی بر کم‌اهمیت‌ترین بیت (LSB) یکی از ساده‌ترین و رایج‌ترین روش‌هایی است که برای پنهان‌کردن اطلاعات محرمانه در تصاویر دیجیتال استفاده می‌شود. در این روش، بیت‌های کم‌اهمیت (LSB) هر پیکسل در تصویر پوششی بابیت‌های داده پنهان جایگزین می‌شوند.

نحوه عملکرد:

فرایند پنهان‌نگاری LSB به شرح زیر است:

1) **انتخاب بیت‌های LSB**: معمولاً یک بیت از هر کانال رنگی (قرمز، سبز و آبی) در هر پیکسل برای پنهان‌کردن اطلاعات استفاده می‌شود. این به این معنی است که در یک تصویر 24 بیتی، می‌توان تا 3 بیت اطلاعات را در هر پیکسل جاسازی کرد.
2) **جایگزینی بیت‌ها:** بیت‌های LSB تصویر پوششی بابیت‌های داده پنهان جایگزین می‌شوند. این کار به‌گونه‌ای انجام می‌شود که تغییر قابل‌توجهی در ظاهر تصویر ایجاد نکند.
3) **ذخیره تصویر پنهان‌نگاری:** تصویر پنهان‌نگاری نهایی که حاوی اطلاعات پنهان است، ذخیره می‌شود.

مزایا:

- سادگی: روش LSB بسیار ساده و آسان برای پیاده‌سازی است.
- ظرفیت پنهان‌سازی: این روش می‌تواند حجم قابل‌توجهی از اطلاعات را در تصاویر پنهان کند.
- شفافیت ادراکی: تصاویر پنهان‌نگاری شده با استفاده از LSB معمولاً برای چشم انسان غیرقابل‌تشخیص هستند.

معایب:

- امنیت ضعیف: این روش نسبتاً در برابر حملات پنهان‌نگاری آسیب‌پذیر است. مهاجمان ماهر می‌توانند با تجزیه‌وتحلیل آماری تصاویر، اطلاعات پنهان را استخراج کنند.
- ظرفیت محدود: ظرفیت پنهان‌سازی اطلاعات در روش LSB به‌اندازه تصویر پوششی محدود می‌شود.
- اعوجاج: در صورت جاسازی حجم زیادی از اطلاعات، ممکن است اعوجاج جزئی در تصویر پنهان‌نگاری ایجاد شود.

به‌طورکلی، روش LSB یک روش ساده و کارآمد برای پنهان‌کردن اطلاعات در تصاویر است، اما به دلیل امنیت ضعیف، برای کاربردهایی که نیاز به امنیت بالایی دارند، مناسب نیست.

علاوه بر روش LSB، روش‌های پنهان‌نگاری دیگری نیز وجود دارند که از فن‌های پیچیده‌تری برای پنهان‌کردن اطلاعات در تصاویر، صوت، ویدئو و سایر انواع داده‌ها استفاده می‌کنند.

که در ادامه به بررسی برخی از این روش‌ها می‌پردازیم:

2-4-2. پنهان‌نگاری مبتنی بر تبدیل کسینوس گسسته DCT[1]

این روش از تبدیل کسینوس گسسته (DCT) برای پنهان‌کردن اطلاعات در ضرایب DCT تصویر استفاده می‌کند.

3-4-2. پنهان‌نگاری مبتنی بر تبدیل موجک گسسته DWT[2]

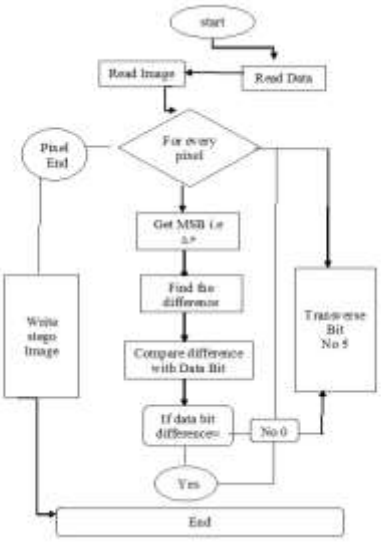
این روش از تبدیل موجک گسسته (DWT) برای پنهان‌کردن اطلاعات در ضرایب DWT تصویر استفاده می‌کند.

4-4-2. پنهان‌نگاری مبتنی بر علامت‌گذاری

این روش از علامت‌گذاری‌های نامرئی برای پنهان‌کردن اطلاعات در تصاویر استفاده می‌کند.

---

[1] Discrete Cosine Transform (DCT)
[2] Discrete wavelet transform (DWT)



شکل 2. رمزگذاری داده‌ها

2-4-5. پنهان‌نگاری مبتنی بر شبکه‌های عصبی

این روش از شبکه‌های عصبی مصنوعی برای پنهان‌کردن اطلاعات در تصاویر و سایر انواع داده‌ها استفاده می‌کند.

انتخاب روش مناسب برای پنهان‌نگاری به عوامل مختلفی مانند نوع داده‌ای که باید پنهان شود، سطح امنیتی موردنیاز، نوع فایلی که به‌عنوان حامل استفاده می‌شود و محدودیت‌های پردازشی بستگی دارد.

2-4-6. پنهان‌نگاری مبتنی بر مهم‌ترین بیت (MSB)

درروش MSB، اطلاعات پنهان در مهم‌ترین بیت (MSB) پیکسل‌های تصویر جاسازی می‌شوند. برخلاف روش LSB که از کم‌اهمیت‌ترین بیت‌ها (LSB) استفاده می‌کند، MSB از مهم‌ترین بیت‌ها برای پنهان‌سازی اطلاعات استفاده می‌کند.

نحوه عملکرد:

فرایند پنهان‌نگاری MSB به شرح زیر است:

- انتخاب بیت‌های :MSB معمولاً یک بیت از هر کانال رنگی (قرمز، سبز و آبی) در هر پیکسل برای پنهان‌کردن اطلاعات استفاده می‌شود. این به این معنی است که در یک تصویر 24 بیتی، می‌توان تا 3 بیت اطلاعات را در هر پیکسل جاسازی کرد.
- تغییر بیت‌های :MSB برای هر پیکسل در تصویر حامل، مراحل زیر را انجام دهید:
  - خواندن بیت‌های 5 و 6: ابتدا بیت‌های 5 و 6 هر پیکسل در تصویر حامل را بخوانید.
  - محاسبه تفاوت: تفاوت بین بیت 5 و 6 را محاسبه کنید. این تفاوت به‌عنوان "تفاوت" شناخته می‌شود.
  - مقایسه بابیت داده: بیت داده را با "تفاوت" محاسبه‌شده مقایسه کنید. اگر بیت داده با "تفاوت" برابر نباشد، بیت 5 پیکسل را تغییر دهید.
  - نوشتن تصویر پنهان‌نگاری: تصویر پنهان‌نگاری نهایی که حاوی اطلاعات پنهان‌شده است را ذخیره کنید.

مزایا:

- ظرفیت پنهان‌سازی: روش MSB می‌تواند حجم قابل‌توجهی از اطلاعات را در تصاویر پنهان کند.
- امنیت: روش MSB به دلیل استفاده از مهم‌ترین بیت‌ها، تا حدی نسبت به حملات پنهان‌نگاری مقاوم‌تر است.

معایب:

- اعوجاج: در صورت جاسازی حجم زیادی از اطلاعات، ممکن است اعوجاج قابل‌توجهی در تصویر پنهان‌نگاری ایجاد شود.
- شناسایی: روش MSB تا حدی قابل‌شناسایی توسط الگوریتم‌های پنهان‌نگاری است.

جدول 1. مقایسه LSB و MSB

MSB	LSB	ویژگی
مهم‌ترین بیت‌ها	کم‌اهمیت‌ترین بیت‌ها	بیت‌های مورداستفاده
بالا	متوسط	ظرفیت پنهان‌سازی
متوسط	ضعیف	امنیت
زیاد	کم	اعوجاج
تا حدی دشوار	آسان	شناسایی

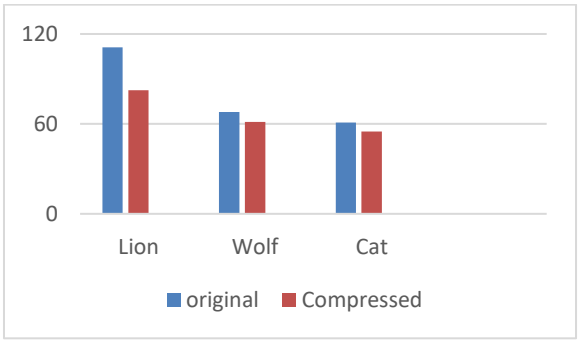
- روش‌های دیگر پنهان‌نگاری: علاوه بر روش‌های LSB و MSB، روش‌های دیگری برای پنهان‌نگاری تصاویر مانند پنهان‌نگاری مبتنی بر DCT و DWT وجود دارد. این روش‌ها از فن‌های پیچیده‌تری برای پنهان‌کردن اطلاعات در تصاویر استفاده می‌کنند و می‌توانند امنیت و ظرفیت پنهان‌سازی بالاتری ارائه دهند.

2-4-7. فن‌های DCT و DWT در پنهان‌نگاری

فن‌های DCT و DWT دو روش مهم در پنهان‌نگاری تصاویر هستند که برای پنهان‌کردن اطلاعات در تصاویر دیجیتال استفاده می‌شوند. این روش‌ها از تبدیل‌های ریاضی برای تجزیه تصویر به فرکانس‌های مختلف و سپس جاسازی اطلاعات در ضرایب تبدیل استفاده می‌کنند.

2-4-8. تبدیل کسینوس گسسته (DCT)

DCT تصاویر را به فرکانس‌های مختلف تبدیل می‌کند. فرکانس‌های پایین نشان‌دهنده اطلاعات کلی تصویر مانند روشنایی و تاریکی هستند، درحالی‌که فرکانس‌های بالا نشان‌دهنده جزئیات دقیق‌تر مانند لبه‌ها و بافت هستند.



شکل 3. تبدیل کسینوس گسسته [21]

2-4-9. نحوه پنهان‌کردن اطلاعات با استفاده از DCT

- تبدیل تصویر به ضرایبDCT: تصویر را به ضرایب DCT تبدیل کنید.
- انتخاب ضرایب: ضرایب DCT با فرکانس پایین را برای جاسازی اطلاعات انتخاب می‌شود. این ضرایب به‌طورکلی کمتر قابل‌توجه هستند و تغییرات در آن‌ها کمتر قابل‌تشخیص است.
- جاسازی اطلاعات: اطلاعات را در ضرایب DCT انتخاب‌شده جاسازی کنید. این کار را می‌توان با فن‌های مختلفی مانند جایگزینی بیت‌ها یا تغییر مقادیر ضرایب انجام داد.
- تبدیل معکوس DCT: ضرایب DCT را به تصویر بازسازی‌شده تبدیل کنید.

مزایای استفاده از DCT

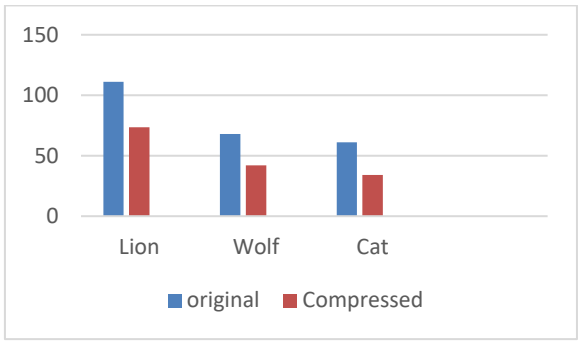
- ظرفیت پنهان‌سازی بالا DCT : می‌تواند حجم قابل‌توجهی از اطلاعات را در تصاویر پنهان کند.
- امنیتDCT: تا حدی در برابر حملات پنهان‌نگاری مقاوم است.

معایب استفاده از DCT

- اعوجاج: در صورت جاسازی حجم زیادی از اطلاعات، ممکن است اعوجاج قابل‌توجهی در تصویر پنهان‌نگاری ایجاد شود.
- پیچیدگیDCT: ازنظر محاسباتی پیچیده‌تر از سایر روش‌های پنهان‌نگاری است.

2-4-10. تبدیل موجک گسسته (DWT)

DWT تصاویر را به سطوح مختلف وضوح تجزیه می‌کند. هر سطح وضوح جزئیات مربوط به یک مقیاس خاص را نشان می‌دهد.



شکل 4. تبدیل موجک گسسته [21]

نحوه پنهان‌کردن اطلاعات با استفاده از DWT

1) **تبدیل تصویر به ضرایب :DWT** تصویر را به ضرایب DWT تبدیل کنید.
2) **انتخاب ضرایب:** ضرایب DWT با سطوح وضوح پایین را برای جاسازی اطلاعات انتخاب می‌شود. این ضرایب به‌طورکلی کمتر قابل‌توجه هستند و تغییرات در آن‌ها کمتر قابل‌تشخیص است.
3) **جاسازی اطلاعات:** اطلاعات را در ضرایب DWT انتخاب‌شده جاسازی کنید. این کار را می‌توان با فن‌های مختلفی مانند جایگزینی بیت‌ها یا تغییر مقادیر ضرایب انجام داد.
4) **بازسازی تصویر:** ضرایب DWT را به تصویر بازسازی‌شده تبدیل کنید.

مزایای استفاده از DWT

- ظرفیت پنهان‌سازی بالاDWT : می‌تواند حجم قابل‌توجهی از اطلاعات را در تصاویر پنهان کند.
- امنیتDWT : تا حدی در برابر حملات پنهان‌نگاری مقاوم است.
- کنترل وضوحDWT : امکان کنترل وضوح اطلاعات پنهان‌شده را فراهم می‌کند.

معایب استفاده از DWT

- اعوجاج: در صورت جاسازی حجم زیادی از اطلاعات، ممکن است اعوجاج قابل‌توجهی در تصویر پنهان‌نگاری ایجاد شود.
- پیچیدگیDWT : ازنظر محاسباتی پیچیده‌تر از سایر روش‌های پنهان‌نگاری است.

جدول 2. مقایسه **DCT** و **DWT**

ویژگی	DWT	DCT
نوع تبدیل	تبدیل موجک گسسته	تبدیل کسینوس گسسته
تجزیه تصویر	به سطوح مختلف وضوح	به فرکانس‌های مختلف
ظرفیت پنهان‌سازی	بالا	بالا
امنیت	تا حدی مقاوم	تا حدی مقاوم
اعوجاج	ممکن است اعوجاج ایجاد کند	ممکن است اعوجاج ایجاد کند
پیچیدگی	پیچیده	پیچیده
کنترل وضوح	دارد	ندارد

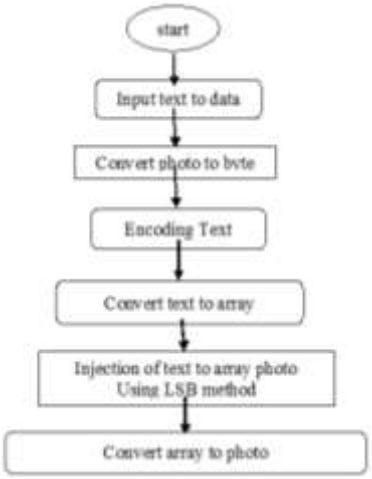
انتخاب روش مناسب

انتخاب روش مناسب برای پنهان‌نگاری تصاویر به عوامل مختلفی مانند نوع داده‌ای که باید پنهان شود، سطح امنیتی موردنیاز، نوع فایلی که به‌عنوان حامل استفاده می‌شود و محدودیت‌های پردازشی بستگی دارد.

3. روش پیشنهادی

ابتدا روش‌های LSB، MSB و روش پیشنهادی را به زبان C++ و در محیط آردوینو برنامه‌نویسی می‌کنیم، سپس بعد از برنامه‌نویسی و اجرای برنامه‌ها معیارهایی همچون سرعت رمزنگاری و رمزگشایی و همچنین تزریق و استخراج داده موردنظر در عکس، حجم عکس قبل و بعد از تزریق و امنیت الگوریتم مورداستفاده را بررسی خواهیم کرد.

لازم به ذکر است به دلیل استفاده از فرمت گرافیکی[1] (BMP) برای عکس‌ها و همچنین کدهای برنامه‌نویسی که به تعداد بایت‌های ورودی عکس، بایت خروجی تولید می‌کنند، همواره حجم عکس قبل و بعد از تزریق برابر است.



شکل 5. روند نمای تبدیل متن به تصویر امن

- در مرحله اول متن محرمانه وارد می¬شود
- سپس تصویر موردنظر را به بایت تبدیل کرده
- متن موردنظر را در فایل مشخص‌شده رمزگذاری می‌کنیم
- متن را به یک آرایی تبدیل کرده
- سپس متن را با استفاده از روش LSB در آرایه تصویر تزریق کرده و در آخر آرایه به‌دست‌آمده را به تصویر تبدیل می‌کنیم.

شرح و پیاده‌سازی روش پیشنهادی

در این آزمون از عکس با فرمت bmp با حجم 374 بایت استفاده می‌کنیم، عکس با نام آزمون در کارت حافظه اس‌دی[2] قرار داده و کارت را درون ماژول[3] sd card که بر روی برد ماژول دوربین ESP32 Cam نصب‌شده است، قرار می‌دهیم.

در ساختار فایل‌های bmp 54 بایت اول مختص به فایل است از 54 بایت اول به بعد را با روش LSB تغییر می‌دهیم.

متغیر از نوع رشته[4] ساخته و داده‌ای که قرار است به‌صورت محرمانه ارسال شود را به‌صورت دستی در آن وارد می‌کنیم. سپس دو متغیر از نوع عدد صحیح[5] ساخته که این دو مسئولیت رمزگذاری و رمزگشایی متن محرمانه رادارند در متغیر اول الگویی از رمزنگاری با مقدار {3،1،3،4،0،2،7،6} قرار داده می‌شود که این متغیر وظیفه‌ی جابه‌جایی نمایه‌های متن محرمانه را دارد.

این متغیر را می‌توان کلید رمزگذاری در این برنامه نامید در بخش بعد متغیر دوم Int وظیفه‌ی رمزگشایی از متن را دارد به این صورت که نمایه‌های جابه‌جاشده توسط متغیر رمزگذاری را به حالت اول که قابل خواندن باشد تبدیل می‌کند.

متن موردنظر را با استفاده از کلیدی که به‌صورت دستی ساخته‌ایم کد کرده و رشته‌های به‌دست‌آمده را به‌وسیله‌ی تابع خواندن بیت (bitread) رشته را خوانده و در کوچک‌ترین بیت در هر بایت شروع جایگزین‌کردن می‌کنیم.

در مرحله‌ی بعد، تصویری را که به‌صورت دستی در SD Card انتقال‌داده‌شده و از جنس تصویر پیکسلی[6] است را می‌خوانیم.

سپس تصویر خوانده‌شده برای عمل پنهان‌نگاری باید تبدیل به بیت شود که با استفاده از الگوریتم‌ها بیت‌ها را تغییر داده بدین صورت که داده‌ی محرمانه که به‌صورت دستی وارد و طبق الگوریتم رمزنگاری تغییر کرده بود باید در تصویر قرار داده شده و ظاهر تصویر به‌هیچ‌وجه تغییر نکند.

متن محرمانه که حاوی پیام (USED STG METHOD) است شامل 15 کاراکتر است که برای تبدیل به آرایه‌ای با b120=8*15 حجم نیاز داریم. متن با استفاده از یک حلقه تبدیل به یک آرایه‌ی b120 می‌شود. حالا آرایه و تصویر آماده‌ی فن پنهان‌نگاری هستند.

[1] Bitmap

[2] sd card
[3] Module
[4] String
[5] integer
[6] Bitmap

در آخر آرایه‌ای که فن پنهان‌نگاری بر روی آن انجام‌شده است. باید تبدیل به تصویر شود؛ بنابراین ابتدا بایت[1] 54 ابتدایی تصویر که شامل هدر فایل[2] می‌شود را کنار گذاشته و عملیات را از بایت 54 فایل تصویر انجام می‌دهد.



شکل 6. برد اینترنت اشیا استفاده‌شده در مدل همزاد دیجیتال Esp32-cam

پس برای تبدیل آرایه به تصویر بایت 54 ابتدایی را در ابتدای فایل جدید قرار داده و در ادامه‌ی آن بایت‌های تغییر پیدا کرده را می‌چینیم که در انتها فایل خروجی را به سمت Sd Card با پسوند Bitmap هدایت می‌کنیم.

سپس نام شبکه بی‌سیم[3] و پسورد[4] یک مودم که متصل به اینترنت است را در دو متغیر وارد کرده و با استفاده از تابع connection ارتباط مابین Esp32-cam را با اینترنت برقرار می‌کنیم.

عکس به‌دست‌آمده را با استفاده از فن کدبندی Base64[5] که در آردوینو با استفاده از کتابخانه Base64.h می‌توان فراخوانی کرد را به کد تبدیل کرده و با روش HTTP POST، به سمت سرور ارسال می‌کنیم سپس سمت سرور عکس را با روش دیکد base64 رمزگشایی کرده و عکس موجود را با روش رمزگشایی LSB رشته‌های متنی را استخراج می‌کنیم (اگر توسط روش LSB قدیمی این روش را انجام داده بودیم به‌راحتی می‌توانستیم داده‌های موجود را مشاهده کنیم) اما باتوجه‌به روش ابداعی استفاده‌شده، رشته‌های به‌دست‌آمده شامل کاراکترهای بی‌معنی است. اطلاعات را به سمت کلیدی که از قبل برای سرور تعریف کرده‌ایم هدایت کرده و رمزگشایی می‌کنیم.

تشریح روش پیشنهادی با استفاده از مثال

جمله‌ی استفاده‌شده جهت ارسال به‌صورت پنهان‌شده (Used Stg Method) است. ابتدا این جمله باید تبدیل به رشته‌ای از کدهای باینری شود که به طور مثال حرف (U) را به باینری تبدیل می‌کنیم که برابر با (01010101) است.

تزریق یک بیت

کد باینری هر حرف را می‌خوانیم اگر برابر با 1 بود مقدار خانه‌ی نمایه شماره‌ی 7 در آرایه‌ی رمزگذاری الگو[6] {5, 1, 3, 4, 0, 2, 7, 6} که برابر با مقدار 5 است نشان از آن می‌دهد که باید در آرایه‌ی جدید خانه‌ی شماره‌ی 5 برابر با 1 شود و همین روش برای مقدار 0 هم انجام می‌شود.

مثال: حرف U

نمایه	7	6	5	4	3	2	1	0
مقدار	0	1	0	1	0	1	0	1

آرایه‌ی جدید:

نمایه	7	6	5	4	3	2	1	0
مقدار			1					

سپس در چرخش بعد حلقه مقدار زیر به دست می‌آید:

نمایه	7	6	5	4	3	2	1	0
مقدار			1				0	

و آرایه‌ی نهایی برابر است با:

نمایه	7	6	5	4	3	2	1	0
مقدار	1	0	1	0	1	0	0	1

پس آرایه‌ی به‌دست‌آمده را با استفاده از روش LSB که قبلاً در فصل 1 توضیح داده شده است در بایت‌های عکس خوانده‌شده تزریق می‌کنیم.

تزریق *u*:

نمایه	7	6	5	4	3	2	1	0
مقدار	1	0	1	0	1	0	0	1

آرایه‌ای فرضی برای بایت 55 عکسی از نوع Byte در نظر می‌گیریم.

نمایه	7	6	5	4	3	2	1	0
مقدار	0	1	1	0	1	1	0	0

پس از اجرای روش LSB بر روی بایت 55 عکس آرایهٔ به‌دست‌آمده به شکل زیر تغییر می‌کند.

نمایه	7	6	5	4	3	2	1	0
مقدار	0	1	1	0	1	1	0	1

سپس با استفاده از تابع Base64 عکس را به رمزگذاری Base64 تبدیل کرده، برد ESP32-Cam به اینترنت متصل شده و عکس را با استفاده از روش HTTP POST بر روی وبگاه به نشانی Stegano.ir ارسال می‌کنیم.

در سمت وبگاه ابتدا عکس به روش Base64 decode رمزگشایی‌شده و عکس به‌دست‌آمده را از بایت 55 به بعد به روش LSB می‌خوانیم.

برای مثال:

بایت 55 برابر با:

نمایه	7	6	5	4	3	2	1	0
مقدار	1	1	1	0	1	1	0	1

[1] Byte
[2] HeaderFile : منظور از هدر فایل 54 بایت اول فایل PNG می‌باشد.
[3] Service Set Identifier (SSID)
[4] Password
[5] Base64 Coding
[6] pattern encode

بیت آخر هر 8 بایت را که خود تشکیل یک بایت می‌دهند را در یک آرایه‌ی 8 بیتی نگهداری می‌کنیم و آرایه‌ی جدید برابر است با:

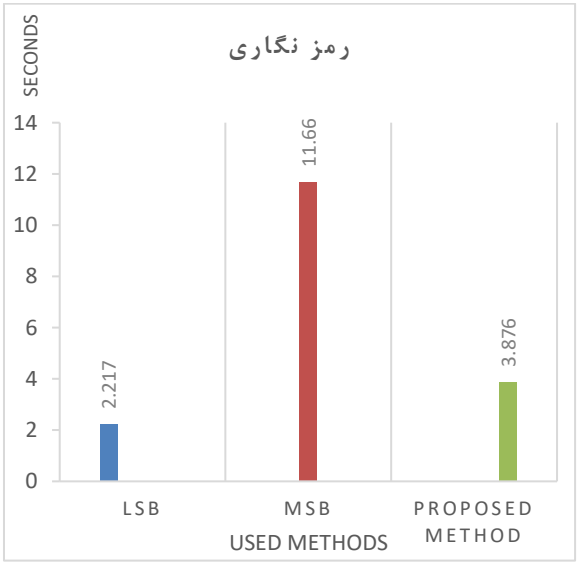
نمایه	7	6	5	4	3	2	1	0
مقدار								1

الگوی معکوس: {4،1،5،2،3،0،7،6} می‌شود، سپس مقادیر به‌دست‌آمده با استفاده از کلیدی که از قبل برای وبگاه تعریف کرده‌ایم رمزگشایی می‌شود.

بایت‌های به‌دست‌آمده با استفاده از قطعه کد دیکد و برابر قرارداد نمایه[1] الگوی معکوس[2] با شمارنده‌ی حلقه رمزگشایی‌شده و درنهایت جمله Used Stg Method نمایش داده می‌شود.

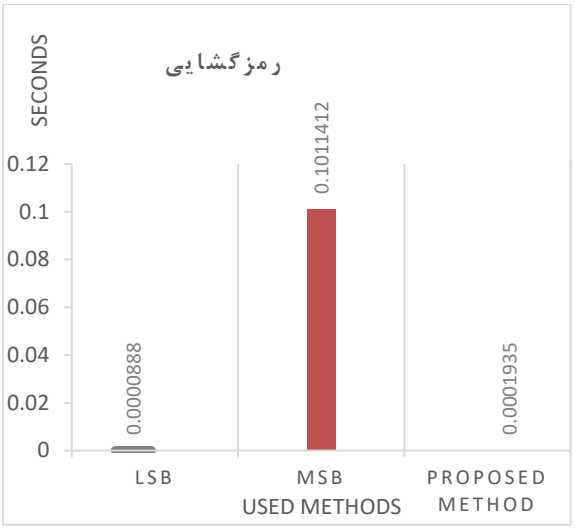
4. نتایج و بحث

همان‌طور که در شکل 7 مشاهده می‌شود، روش LSB به دلیل استفاده از ساده‌ترین فن (جایگزینی بیت کم‌اهمیت هر بایت) سریع‌ترین روش برای رمزگذاری متن در تصویر است. روش MSB Bit Differencing به دلیل انجام عملیات XOR و مقایسه بیت‌ها، زمان بیشتری را برای رمزگذاری صرف می‌کند. روش پیشنهادی که شامل رمزگذاری متن قبل از پنهان‌سازی در تصویر است، به دلیل انجام دو مرحله رمزگذاری، بیشترین زمان را برای رمزگذاری متن در تصویر می‌برد.



شکل 7. مقایسه زمان رمزگذاری در هر سه روش

همان‌طور که در شکل 8 مشاهده می‌شود، روش LSB به دلیل سادگی و عدم نیاز به انجام عملیات پیچیده، سریع‌ترین روش برای رمزگشایی متن از تصویر است. روش MSB Bit Differencing به دلیل نیاز به انجام عملیات XOR و مقایسه بیت‌ها، زمان بیشتری را برای رمزگشایی متن از تصویر صرف می‌کند. روش پیشنهادی که شامل رمزگذاری متن قبل از پنهان‌سازی در تصویر است، به دلیل انجام دو مرحله رمزگشایی (رمزگشایی متن رمزگذاری شده و سپس رمزگشایی متن پنهان‌شده در تصویر)، بیشترین زمان را برای رمزگشایی متن از تصویر می‌برد.



شکل 8. مقایسه زمان رمزگشایی در هر سه روش

➢ امنیت:

روش LSB به دلیل سادگی و قابل‌پیش‌بینی بودن الگوی پنهان‌سازی، ازنظر امنیتی ضعیف‌ترین روش است. روش MSB Bit Differencing به دلیل استفاده از عملیات XOR و مقایسه بیت‌ها، امنیت را تا حدودی افزایش می‌دهد. روش پیشنهادی که شامل رمزگذاری متن قبل از پنهان‌سازی در تصویر است، به دلیل انجام دو مرحله رمزگذاری و استفاده از الگوریتم جای‌گشت برای پنهان‌سازی متن، ازنظر امنیتی قوی‌ترین روش است.

➢ کیفیت تصوی

هر سه روش پنهان‌سازی متن در تصویر، تا حدی بر کیفیت تصویر تأثیر می‌گذارند. این تأثیر درروش LSB به دلیل جایگزینی بیت‌های کم‌اهمیت تصویر، کمتر قابل‌مشاهده است. درروش MSB Bit Differencing، به دلیل تغییر بیت‌های بااهمیت بیشتر، ممکن است افت جزئی کیفیت تصویر مشاهده شود. درروش پیشنهادی، به دلیل انجام دو مرحله پنهان‌سازی، احتمال افت کیفیت تصویر بیشتر است.

➢ توضیحات روش

- **معیارهای ارزیابی:**
  - زمان رمزگذاری/رمزگشایی: سنجش زمان صرف شده برای پنهان‌سازی و استخراج متن از تصویر؛

[1] Index
[2] Pattern reverse

- امنیت: بررسی مقاومت الگوریتم در برابر حملات ضد پنهان‌نگاری و افشای اطلاعات پنهان؛
- کیفیت تصویر: ارزیابی میزان افت کیفیت تصویر پس از پنهان‌سازی متن؛
- پیچیدگی کد: سنجش تعداد خطوط کد و دشواری پیاده‌سازی الگوریتم؛
- ساختار کد: بررسی سازمان‌دهی و خوانایی کد هر الگوریتم.

- **ابزارهای مورداستفاده:**
  - نمودارها برای نمایش نتایج به‌صورت بصری
  - وبگاه lizard.ws برای محاسبه پیچیدگی کد و شمارش خطوط
  - تحلیل دستی کد برای بررسی ساختار و جزئیات

مقایسه جزئیات:

- **زمان رمزگذاری/ رمزگشایی:**
  - LSB سریع‌ترین روش به دلیل سادگی پنهان‌سازی در بیت‌های کم‌اهمیت؛
  - MSB Bit Differencing کندتر از LSB به دلیل انجام عملیات XOR و مقایسه؛
  - روش پیشنهادی: کندترین به دلیل رمزگذاری دومرحله‌ای (متن و تصویر) ؛

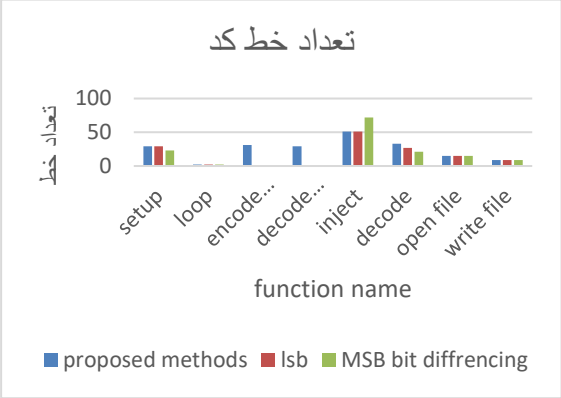
امنیت:

- LSB : ضعیف‌ترین ازنظر امنیتی به دلیل الگوی پنهان‌سازی قابل‌پیش‌بینی؛
- MSB Bit Differencing امنیت متوسط به دلیل استفاده از XOR و مقایسه؛
- روش پیشنهادی: قوی‌ترین ازنظر امنیتی به دلیل رمزگذاری پیش از پنهان‌سازی و الگوریتم جای‌گشت.

- **کیفیت تصویر:**
  - LSB کمترین افت کیفیت به دلیل پنهان‌سازی در بیت‌های کم‌اهمیت؛
  - MSB Bit Differencing افت جزئی کیفیت به دلیل تغییر بیت‌های بااهمیت بیشتر؛
  - روش پیشنهادی: احتمال افت بیشتر کیفیت به دلیل پنهان‌سازی دومرحله‌ای.

- **پیچیدگی کد:**
  - LSB ساده‌ترین ازنظر تعداد خطوط و ساختار به دلیل الگوریتم ساده؛
  - MSB Bit Differencing پیچیدگی متوسط به دلیل توابع XOR و مقایسه؛
  - روش پیشنهادی: پیچیده‌ترین به دلیل توابع رمزگذاری و پنهان‌سازی مجزا.

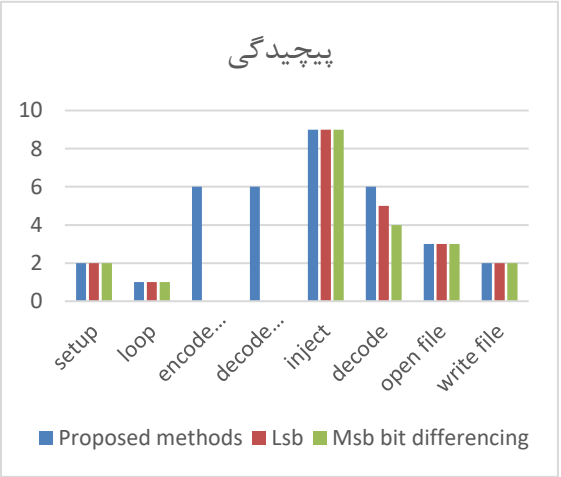
- **ساختار کد:**
  - LSB ساختار ساده و خوانا به دلیل الگوریتم مستقیم؛
  - MSB Bit Differencing ساختار نسبتاً پیچیده به دلیل توابع XOR و مقایسه؛
  - روش پیشنهادی: ساختار پیچیده‌تر به دلیل توابع و مراحل بیشتر.



شکل 9. نمودار تعداد خطوط کدنویسی

همان‌طور که نمایان است تعداد خطوط به‌کاررفته در ساخت روش پیشنهادی در قسمت رمزگذاری و رمزگشایی مقداری بیشتر از دو روش دیگر است و علت هم همان بالابردن بیشتر امنیت به‌واسطه‌ی عملیات رمزنگاری پیش از نهان‌نگاری است.

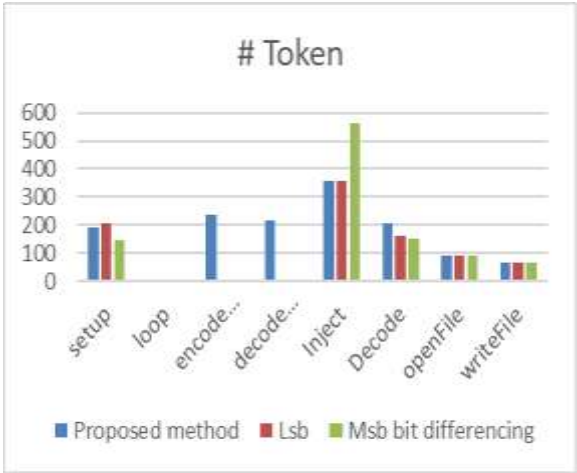
اما بااین‌وجود زمان مورداستفاده برای پردازش روش پیشنهادی تفاوت چندانی با LSB ندارد. ولی ازنظر امنیت روش پیشنهادی به‌غیراز دارابودن فن نهان‌نگاری دارای یک فن رمزنگاری هم است.



شکل 10: نمودار پیچیدگی

اندازه‌گیری پیچیدگی کد که بهترین وسیله برای پیش‌بینی ضعف و نقص‌های احتمالی است. پیچیدگی کد به طرز فراوانی به کارآمدی نرم‌افزار اثر می‌گذارد. گاهی کد آن‌قدر پیچیده می‌شود که جای پیشرفت ندارد و تنها راه برون‌رفت از این مسیر و بهبودبخشیدن به نرم‌افزار کاهش کدهای آن است.

در شکل 15 همان‌طور که مشاهده می‌کنید بیانگر پیچیدگی بیشتر روش پیشنهادی تنها به دلیل استفاده هم‌زمان از فن رمزنگاری و نهان‌نگاری است. شایان‌ذکر است که در نمودار قبل گفته شد که تعداد خطوط به‌کاررفته در ساخت روش پیشنهادی بیشتر از دو روش دیگر است؛ لذا همین مسئله می‌تواند پیچیدگی کد را افزایش دهد.



شکل 11.تعداد عملگر

یکی دیگر از فن‌های مقایسه‌ای که سه روش را با یکدیگر قیاس کردیم تعداد حروف یا عملگرهایی است که در کد به‌کاررفته است همان‌طور که نمایان است فن MSB در تابع تزریق بالاترین میزان حروف یا عملگر را به دلیل پیچیدگی فن نامبرده به خود اختصاص داده است، اما در کل روش پیشنهادی به دلیل استفاده از رمزنگاری و بالاتر بردن امنیت از حروف یا عملگرهای بیشتری استفاده کرده است. همچنین در روش‌های LSB و پیشنهادی زمان آن‌ها بسیار ناچیز است که علت آن درروش پیشنهادی به نسبت LSB استفاده از دو بار رمز شدن داده به نسبت LSB که فقط یک‌بار انجام می‌شود است. درروش پیشنهادی ازلحاظ میزان زمان رمزگذاری و رمزگشایی بین دو روش قبلی قرار گرفته است. نکته جالب و در حقیقت مهم‌ترین قسمت مقایسه این سه روش این است که اندازه فایل ورودی و خروجی در هر سه روش کاملاً ثابت است و هیچ تغییری نکرده است.

جدول 3. زمان و اندازه فایل به‌دست‌آمده در هر سه روش

روش	LSB	MSB Bit Diffrencing	Proposed method
زمان رمزگشایی (ms)	2.217	11.660	3.876
زمان رمزنگاری (ms)	0.0000888	0.1011412	0.0001935
تعداد خط کد	133	142	199
پیچیدگی	22	21	35
Token	893	1028	1370
Size file before	374B	374B	374B
Size file after	374B	374B	374B

5. نتیجه‌گیری

در این پژوهش مسئله حفظ و تأمین امنیت اطلاعات محرمانه داده‌های مشخص در اینترنت اشیا جهت استفاده در دوقلوی دیجیتال با رویکردی جدید با استفاده از ابزار و مبتنی بر به‌روزترین منابع موجود در این زمینه منجر به شکل‌گیری روشی نوین و ایده‌ای منحصربه‌فرد گردیده است.

در یک محیط آردوینو، با استفاده از برنامه‌نویسی و مقایسه دو روش LSB و MSB Bit Differncing و مقایسه نتایج هر دو روش با نتایج به‌دست‌آمده با روش پیشنهادی به این نتیجه رسیدیم که باتوجه‌به داده حاصل از رمزگشایی پس از رمزگذاری توسط هر سه روش ذکرشده، حجم فایل خروجی کاملاً ثابت مانده و تفاوت در زمان فرایند رمزگذاری و رمزگشایی هر سه روش تأثیری بر اندازه فایل نداشته؛ یعنی حجم فایل به‌دست‌آمده با فایل اصلی برابر است و این فاکتور مناسبی است که نشان می‌دهد شخص ثالث به‌سادگی به اطلاعات نهفته شده در عکس پی نمی‌برد؛ بنابراین انتخاب بهترین روش پنهان‌سازی متن در تصویر به نیازها و اولویت‌های کاربر بستگی دارد. اگر سرعت رمزگذاری و رمزگشایی و همچنین کیفیت تصویر از اهمیت بالایی برخوردار باشد، روش LSB می‌تواند گزینه مناسبی باشد. اگر امنیت از اهمیت بالایی برخوردار باشد، روش پیشنهادی بهترین انتخاب است. روش MSB Bit Differencing می‌تواند به‌عنوان راه‌حلی بینابینی برای تعادل بین سرعت، امنیت و کیفیت تصویر در معماری همزاد دیجیتال صنعتی مورداستفاده قرار گیرد.

6. مراجع

[1] D. Gelernter, Mirror worlds: Or the day software puts the universe in a shoebox... How it will happen and what it will mean. Oxford University Press, 1993.

[2] O. Dawkins, A. Dennett, and A. Hudson-Smith, "Living with a digital twin: Operational management and engagement using IoT and Mixed Realities at

UCL's Here East Campus on the Queen Elizabeth Olympic Park," in Giscience and remote sensing, 2018: GIS Research UK (GISRUK).

[3] M. Grieves and J. Vickers, "Digital twin: Mitigating unpredictable, undesirable emergent behavior in complex systems," Transdisciplinary perspectives on complex systems: New findings and approaches, pp. 85-113, 2017.

[4] M. G. Kapteyn, "Mathematical and Computational Foundations to Enable Predictive Digital Twins at Scale," Massachusetts Institute of Technology, 2021.

[5] S. Schweigert-Recksiek, J. Trauer, C. Engel, K. Spreitzer, and M. Zimmermann, "Conception of a digital twin in mechanical engineering–a case study in technical product development," in Proceedings of the design society: DESIGN conference, 2020, vol. 1: Cambridge University Press, pp. 383-392.

[6] J. Wilberg, I. Triep, C. Hollauer, and M. Omer, "Big Data in product development: Need for a data strategy," in 2017 Portland International Conference on Management of Engineering and Technology (PICMET), 2017: IEEE, pp. 1-10.

[7] J. Trauer, S. Schweigert-Recksiek, C. Engel, K. Spreitzer, and M. Zimmermann, "What is a digital twin?–definitions and insights from an industrial case study in technical product development," in Proceedings of the design society: DESIGN conference, 2020, vol. 1: Cambridge University Press, pp. 757-766.

[8] M. Wazid, A. K. Das, S. Shetty, and M. Jo, “A Tutorial and Future Research for Building a Blockchain-Based Secure Communication Scheme for Internet of Intelligent Things,” IEEE Access, vol. 8, pp. 88700–88716, 2020.

[9] T. Alam, “A reliable framework for communication in internet of smart devices using IEEE 802.15.4,” ARPN J. Eng. Appl. Sci., vol. 13, no. 10, pp. 3378–3387, 2018.

[10] Somnath B. ThigaleRahul PandeyVirendrakumar A. Dhotre, “Robust Routing For Secure Communication in IOT Enabled Network,” Tchno-Societal, pp. 79–86, 2018.

[11] N. Proros and P. Honeyman, “Hide and seek: An Introduction to Steganography,” Secur. Priv., vol. 10, pp. 32–34, 2003.

[12] B. Chitradevi, N. Thinaharan, and M. Vasanthi, “Data Hiding Using Least Significant Bit Steganography in Digital Images,” Stat. Approaches Multidiscip. Res., vol. I, pp. 144–150, 2017.

[13] D. R. I. M. Setiadi, “Payload enhancement on least significant bit image steganography using edge area dilation,” Int. J. Electron. Telecommun., vol. 65, no. 2, pp. 287–292, 2019.

[14] Kaur, M., Alzubi, A.A., Walia, T.S., Yadav, V., Kumar, N., Singh, D., & Lee, H. EGCrypto: A Low-Complexity Elliptic Galois Cryptography Model for Secure Data Transmission in IoT. IEEE Access, 11, 90739-90748., 2023.

[15] X. Liu, Y. Liu, S. Yang, and L. Wang, "A Survey on Deep Learning for IoT Security: Challenges and Solutions," IEEE Access, vol. 10, pp. 50310-50324, 2022.

[16] M. A. Lashgari, A. A. A. Bakar, and H. Abd Rahman, "Steganographic Techniques for Securing IoT Data: A Review," Sensors, vol. 22, no. 8, p. 3022, 2022.

[17] W. Zhang, Z. Li, Y. Zhang, and X. Luo, "A Novel Deep Learning Approach for Image Steganalysis," IEEE Transactions on Information Forensics and Security, vol. 17, no. 8, pp. 2358-23

[18] Kosuru, S.N., Pradhan, A., Basith, A., Sonar, R., & Swain, A.G. Digital Image Steganography With Error Correction on Extracted Data. IEEE Access, 11, 80945-80957, 2023.

[19] and Communication Networks, S. (2024). Retracted: IOT and Blockchain-Based Cloud Model for Secure Data Transmission for Smart City. Security and Communication Networks.

[20] Retracted: IOT and Blockchain-Based Cloud Model for Secure Data Transmission for Smart City. Security and Communication Networks. S, (2024).

[21] Kurniawan, Andri & Purboyo, Tito & Prasasti, Anggunmeka. Implementation of Image Compression Using Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). International Journal of Applied Engineering Research. 12. 13951-13958, (2017).

[22] H. H. O. Nasereddin, “New Method for Image Inside Image Steganography By Ahmed Faleh Supervisor the Master Degree in Computer Science,” no. May 2014, 2015.

[23] Gabriel Macharia Kamau, “An Enhanced Least Significant Bit Steganographic Method For Information Hiding,” Jomo Kenyatta University, 2013.

[24] A. U. Islam et al., “An improved image steganography technique based on MSB using bit differencing,” 2016 6th Int. Conf. Innov. Comput. Technol. INTECH 2016, no. August, pp. 265–269, 2017.

[25] J. M. D. & S. Polymnia, “Herodotus, The Hisories,” in Terpsichore, 1992. https://core-electronics.com.au/guides/esp32-cam-set-up/

[26] https://www.nutsvolts.com/magazine/article/build-a-video-camera-using-the-esp32-cam-board