International Journal of Information Security (2024) 23:2607–2635
https://doi.org/10.1007/s10207-024-00853-9

REGULAR CONTRIBUTION

Evaluating the merits and constraints of cryptography-steganography fusion: a systematic analysis

Indy Haverkamp[1] · **Dipti K. Sarmah**[1]

Accepted: 12 April 2024 / Published online: 5 May 2024

Abstract
In today's interconnected world, safeguarding digital data's confidentiality and security is crucial. Cryptography and steganography are two primary methods used for information security. While these methods have diverse applications, there is ongoing exploration into the potential benefits of merging them. This review focuses on journal articles from 2010 onwards and conference papers from 2018 onwards that integrate steganography and cryptography in practical applications. The results are gathered through different databases like Scopus, IEEE, and Web of Science. Our approach involves gaining insights into real-world applications explored in the existing literature and categorizing them based on domains and technological areas. Furthermore, we comprehensively analyze the advantages and limitations associated with these implementations, examining them from three evaluation perspectives: security, performance, and user experience. This categorization offers guidance for future research in unexplored areas, while the evaluation perspectives provide essential considerations for analyzing real-world implementations.

Keywords Image steganography · Cryptography · Real-world applications · Evaluation perspectives · Security

1 Introduction

Our daily lives are becoming increasingly linked with the digital realm, encompassing various activities such as messaging, cloud data storage, and financial transactions. Ensuring the security and confidentiality of this data is vital. Cryptography and steganography, two essential sciences of information security [74, 77], offer solutions to render messages unintelligible to eavesdroppers and imperceptible to detection, respectively. These techniques play a crucial role in protecting sensitive information. Both fields serve the purpose of ensuring the confidentiality of data [69], however, in different ways: Cryptography shields the content of a message through the use of encryption keys, ensuring its protection. On the other hand, steganography focuses on concealing the very presence of the message within a "cover" medium [74]. While cryptography finds extensive usage in various everyday applications, both techniques have their respective domains of application and can potentially be combined for enhanced security measures. Steganography encompasses a wide range of techniques and can be applied in different forms, such as images, audio, video, and text, to many applications, for example, IoT communication [7, 21, 39], military [71], cloud storage [2, 18, 46, 67], and more [28, 31, 32, 89, 93]. The growth of interest in steganography was sparked in two ways: the multimedia industry could greatly benefit from possible water-marking techniques, and restrictions on cryptographic schemes by governments triggered interest in alternative ways for communication to stay secretive [8] (Fig. 1).

Figure 2 visually represents the exponential growth of publications focusing on the applications of combining steganography and cryptography, as observed in Scopus.[1] This trend highlights the increasing interest in merging or comparing these two disciplines within the research community. While the combination of multiple security mechanisms may appear advantageous, it is important to note that the suitability of combining cryptography with steganography can vary. Several factors, including bandwidth availability

✉ Dipti K. Sarmah
d.k.sarmah@utwente.nl

Indy Haverkamp
i.haverkamp@student.utwente.nl

[1] SCS/EEMCS, University of Twente, P.O. Box 217, 7500AE Enschede, Overjissel, The Netherlands

[1] https://www.scopus.com/

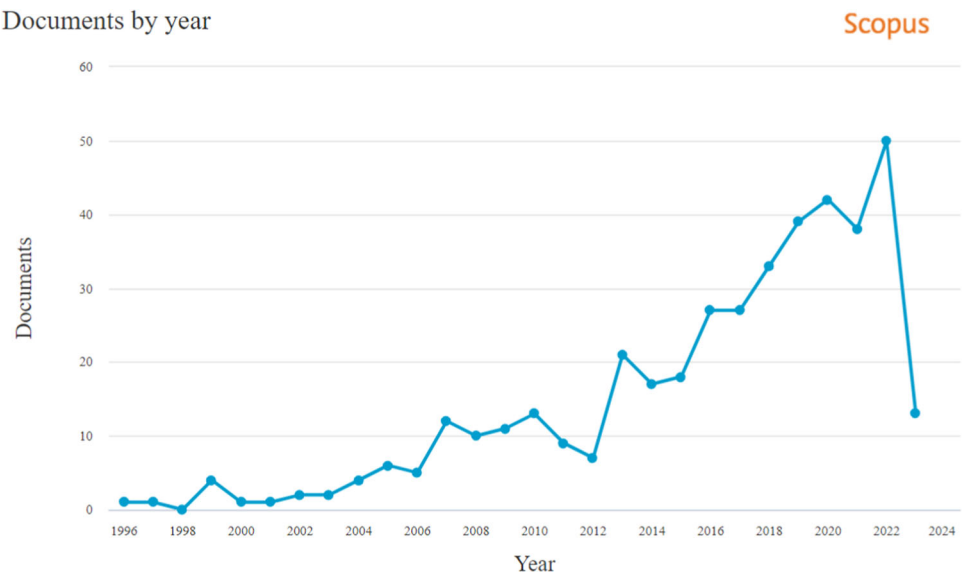


Fig. 1 Graph of published journal articles and conference papers on Scopus (https://www.scopus.com/—with query: ("cryptography" AND "steganography") AND ("application" OR "real-world") AND ("security" OR "cyberattack" OR "cybersecurity")) from 1996 to June 2023

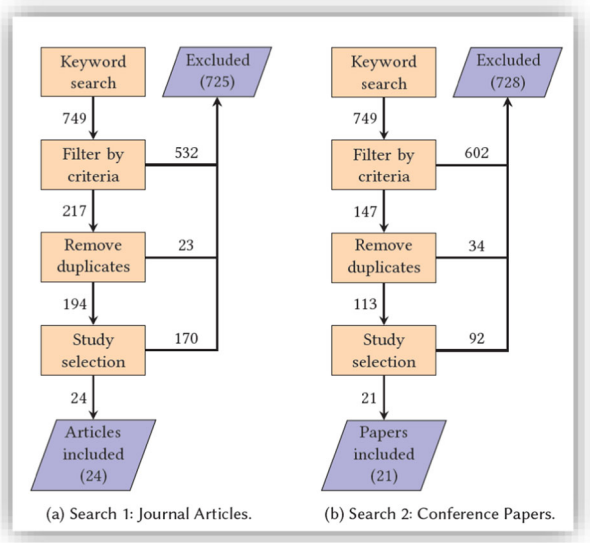


Fig. 2 Data gathering and study selection processes of both literature searches

[37, 81] and latency considerations [88], can influence the feasibility of such integration. For instance, incorporating additional layers of security may result in increased data size, potentially exceeding the available bandwidth and causing slower transmission speeds. Interestingly, the computational complexity of a combined approach does not always exhibit a linear increase. A notable example is presented in [25], where steganography with Diffie-Hellman encryption demonstrated the same time complexity as steganography alone. However, when using RSA [91] encryption, a higher time complexity was observed [25]. Therefore, the choice between these techniques heavily relies on the specific security requirements of the given situation and the particular types of cryptography and steganography employed. In this paper, we refer to **"a combined approach"** to the combined use of steganography and cryptography. Furthermore,**'method' and'scheme' interchangeably** refer to a paper's combined implementation.

As the number of systems requiring protection from cyberattacks continues to rise, the exploration of applications where steganography and cryptography can be combined becomes increasingly intriguing. Nonetheless, to identify potential areas for improvement or future research, it is imperative to gain a comprehensive understanding of the current state of research in this field.

The goal of this research is in threefold steps as mentioned in the following. This also helps to formulate the research questions.

1. The research does a systematic literature review aiming to bring forth a novel perspective by identifying and analyzing papers that delve into the combined application of cryptography and steganography across real-world applications.
2. The research categorizes these applications based on diverse domains and contexts, such as their domain of applications (e.g., Medical or Transportation) and technological domain (e.g., Cloud Computing or Internet of Things).
3. The research also explores several relevant studies to identify the advantages, limitations, and trade-offs discussed in the existing literature and gain insight into how the performance of these combined implementations can be effectively analyzed.

The findings derived from this comprehensive review yield valuable insights into the current research landscape, contributing to advancements in fortifying systems against cyber threats. Consequently, these findings prompt the formulation of the following research questions, which further drive exploration and inquiry in this field. **The primary research question** focuses on exploring the advantages and limitations of utilizing a combined steganography and cryptography approach in diverse real-world applications as a means to enhance security against cyberattacks on a system.

To address this primary question, **three key sub-questions** necessitate analysis:

i. What are the various real-world applications where combined steganography and cryptography approaches can be used? **(RQ1)**
ii. What are the advantages, limitations, and trade-offs of using a combined approach in these applications? **(RQ2)**
iii. How are implementations of a combined approach evaluated across different real-world applications? **(RQ3)**

By addressing these sub-questions, a comprehensive understanding of the benefits, constraints, and evaluation methods surrounding the combined application of steganography and cryptography can be obtained, leading to significant insights for bolstering system security against cyber threats.

This paper is organized into several sections, including the Introduction section as referred to in Sect. 1. Section 2 discusses the background and related work of the steganography and cryptography techniques as well as evaluation methods. Section 3 elaborates on the methodology of the research including the search strategy for conducting a literature review, databases to collect resources, and tools to optimize the efficiency of the review process. The results are presented in Sect. 4 which includes different types of applications and categorization approaches of these applications, exploring limitations and advantages of the applications, and analyzing these methods to provide valuable insights into the combination of cryptography and steganography methods in terms of security, performance, and user perspective. Section 5 gives the concluding remarks and presents the future scope of the research. References are drawn at the end of the paper.

2 Background and related work

There is high interest in organizations, researchers, and end users in the sciences of steganography and cryptography to enhance security for different applications and several domains. In this research, we analyzed several papers that focus on the combination of cryptography and steganography to identify the real gap and pros and cons of combining both sciences. For that, we focused on several relevant applications, and one of the important and interesting applications in the medical domain where Bhardwaj, R. [13] addresses the critical challenge of ensuring patient data privacy and security in telemedicine applications. The author proposes an enhanced reversible data-hiding technique operating in the encrypted domain. The proposed algorithm embeds secret messages in hexadecimal form and utilizes four binary bits of electronic patient information (EPI) in each cover image block, ensuring secure communication. However, this approach mitigates underflow and overflow problems, enabling precise information embedding even in low-intensity pixel areas.

On the other side, the research [22] discusses the growing challenge of securing medical data in healthcare applications due to the expanding presence of the Internet of Things (IoT). They propose a hybrid security model combining cryptography and steganography to protect diagnostic text data within medical images. The encryption process precedes the embedding of encrypted data into cover images, both color and grayscale, to accommodate varying text sizes. Performance evaluation based on six statistical parameters indicates promising results, with PSNR values ranging from 50.59 to 57.44 for color images and from 50.52 to 56.09 for grayscale images. The proposed model demonstrates its effectiveness in securely hiding confidential patient data within cover images while maintaining high imperceptibility and capacity, with minimal degradation in the received stego-image.

Further, the research [34] states that as the elderly population increases and more people suffer from heart problems, hospitals worldwide are expected to use remote electrocardiogram (ECG) patient monitoring systems. These systems will gather a lot of ECG signals from patients at home, along with other health measurements like blood pressure and temperature, for analysis by remote monitoring systems. It's crucial to keep patient information safe when transmitting data over public networks and storing it on hospital servers. This study introduces a technique using wavelets, which are like a special math tool, to hide patient data in ECG signals. It combines encryption, which is like a lock, and scrambling, which is like mixing things up, to protect the data. This technique lets us put patient info into ECG signals without changing how they look or work. Tests show that the technique keeps data safe (with less than 1% change) and doesn't mess up the ECG readings. This means doctors can still read the ECGs even after we take out the hidden patient info, keeping medical data private and accurate.

Furthermore, the paper [41] proposes a novel steganography technique in their work, aiming to enhance the security of data transmission in telemedicine applications. This technique involves concealing patient information within medical

images using a dynamically generated key, determined through graph coloring and the pixel count of the cover image. By combining steganography with cryptography, the patient information is encrypted using the RSA algorithm to strengthen security measures. Notably, this proposed method ensures reversibility, allowing for the lossless restoration of original medical images after data extraction from the stego medical image. Experimental evaluations demonstrate the efficacy of this approach, showcasing its superior security compared to alternative information hiding methods, particularly in terms of key generation complexity and the quality of restored images as measured by Peak Signal-to-Noise Ratio (PSNR) and Mean Square Error (MSE).

The researchers in [45] also worked along similar lines to enhance robust security measures in the handling of medical images, particularly when sensitive patient records are involved. To address this, a 128-bit secret key is generated based on the histogram of the medical image. Initially, the digital imaging and communications in medicine (DICOM) image undergoes a decomposition process to extract its sensitive features. The resulting image is then divided into blocks dependent on the generated key, followed by key-dependent diffusion and substitution processes. Encryption is performed over five rounds to ensure robust security. Subsequently, the secret key is embedded within the encrypted image using steganography, further enhancing the security of the proposed cipher. At the receiver's end, the secret key is extracted from the embedded image and decryption is carried out in reverse.

An innovative approach is presented in this paper [48], proposing an integrated method that combines cryptography and steganography to bolster data security in automotive applications. In this technique, data is first encrypted using a modified RSA cryptographic algorithm, and the encrypted data is then embedded along the edges of an image using the Least Significant Bit (LSB) technique. Edge detection [55] is accomplished using a fuzzy logic approach. This integrated approach is primarily designed for applications such as Diagnostics over Internet Protocol (DoIP) and Software Updates over the Air (SOTA), which involve the exchange of highly sensitive data. Additionally, the authenticity of the source of software updates is verified using a Hash Algorithm in SOTA.

Additionally, this paper [57] introduces a technique for encrypting and decrypting patient medical details, medical images, text, and pictorial forms using unique algorithms, aligning with the literature discussed above in the medical field. However, this research enhances security through the utilization of chaotic signals [59]. Signal generation and analysis are conducted using Matlab 7.10, demonstrating the efficacy of this method. In similar lines, the paper by Parah et al. [61] introduces a novel and reversible data hiding scheme tailored for e-healthcare applications, emphasizing high capacity and security. The Pixel to Block (PTB) conversion technique is employed to generate cover images efficiently, ensuring the reversibility of medical images without the need for interpolation. To enable tamper detection and content authentication at the receiver, a fragile watermark and Block Checksum are embedded in the cover image, computed for each 4×4 block. Intermediate Significant Bit Substitution (ISBS) is utilized to embed Electronic Patient Records (EPR), watermark, and checksum data, preventing LSB removal/replacement attacks. Evaluation of the scheme includes perceptual imperceptibility and tamper detection capability under various image processing and geometric attacks. Experimental results demonstrate the scheme's reversibility, high-quality watermarked images, and effective tamper detection and localization.

In this research [75], the authors propose a new and secure steganography-based End-to-End (E2E) verifiable online voting system to address issues within the voting process. This research introduces a novel approach to online voting by integrating visual cryptography with image steganography to bolster system security while maintaining system usability and performance. The voting system incorporates a password-hashed-based scheme and threshold decryption scheme for added security measures. Further, the research [78] discusses the advantages of combining both steganography and cryptography for having more secure communication. Initially, the Advanced Encryption Standard (AES) algorithm is adapted and employed to encrypt the secret message. Subsequently, the encrypted message is concealed using a steganography method. This hybrid technique ensures dual-layered security, offering both high embedding capacity and quality stego images for enhanced data protection.

Furthermore, the authors in [87] introduce a novel Reversible data hiding in encrypted images (RDHEI) scheme leveraging the median edge detector (MED) and a hierarchical block variable length coding (HBVLC) technique. In this approach, the image owner predicts the pixel values of the carrier image with MED, followed by slicing the prediction error array into bit-planes and encoding them plane by plane. Experimental results demonstrate that the proposed scheme not only restores secret data and the carrier image without loss but also surpasses state-of-the-art methods in embedding rate across images with diverse features.

The previously discussed paper primarily centered around application domains. In contrast, we examined several papers that primarily focused on technological domains. This paper [1] presents the Circle Search Optimization with Deep Learning Enabled Secure UAV Classification (CSODL-SUAVC) model tailored for Industry 4.0 environments. The CSODL-SUAVC model aims to achieve two core objectives: secure

communication via image steganography and image classification. The proposed methodology involves Multi-Level Discrete Wavelet Transformation (ML-DWT), CSO-related Optimal Pixel Selection (CSO-OPS), and signcryption-based encryption. The proposed CSODL-SUAVC model is experimentally validated using benchmark datasets, demonstrating superior performance compared to recent approaches across various evaluation aspects.

In their paper [5], the authors introduce an improved system designed to safeguard sensitive text data on personal computers by combining cryptography and steganography techniques. The system's security is fortified by employing RSA cryptography followed by audio-based steganography. The study includes system modeling and implementation for testing, aimed at exploring the relationship between security, capacity, and data dependency. Experimentation involved securing data within 15 differently sized audio files, yielding insightful results.

Additionally, the research in [7] discusses the promising growth of the Internet of Things (IoT) and the prevalent use of digital images, which has resulted in an increased adoption of image steganography and cryptography. However, current systems encounter challenges related to security, imperceptibility, and capacity. In response, they propose a new Crypt-steganography scheme that integrates three primary elements: hybrid additive cryptography (HAC) for secure message encryption, the bit interchange method (BIGM) to ensure imperceptibility during embedding, and a novel image partitioning method (IPM) for enhanced randomness in pixel selection. Evaluations confirm the scheme's effectiveness in addressing these challenges.

Also, the authors of [9] presented a novel approach to safeguard data on the cloud using Reversible Data Hiding in an Encrypted Image (RDHEI), coupled with homomorphic encryption and a rhombus pattern prediction scheme. With this method, third parties can perform data-hiding operations on encrypted images without knowledge of the original content, ensuring high-level security. The proposed method demonstrates strong protective measures, as evidenced by experimentations. Additionally, the approach enables seamless image recovery and covert extraction.

Further, in this paper, the authors [10], explore how malicious Android applications are evading detection by hiding within images using techniques like Concatenation, Obfuscation, Cryptography, and Steganography. They assess the vulnerability of ten popular Android anti-malware solutions to these methods. Surprisingly, only one solution detected two hiding techniques, while the others remained blind to all eight. This evaluation offers insights into the evolving landscape of Android malware and the effectiveness of current detection systems.

Insufficient security measures in data transmission led to issues like data integrity, confidentiality, and loss, especially with big data. Executing multiple security algorithms reduces throughput and increases security overhead, impacting robustness against data loss. Conversely, compression techniques sacrifice data confidentiality. Existing studies lack comprehensive security policies to address these concerns collectively. Therefore, the authors in their paper [14] propose an integrated approach to enhance confidentiality and provide backup for accidental data loss by combining simplified data encryption standards (SDES) and advanced pattern generation. A novel error control technique maximizes data integrity against transmission errors. A new compression method improves robustness against data loss while maintaining efficiency. Enhanced confidentiality and integrity are achieved through advanced audio steganography. Implementing this integrated technique in a GPU environment accelerates execution speed and reduces complexity. Experiments validate the method's effectiveness in ensuring data confidentiality and integrity, outperforming contemporary approaches.

By covering one more technological aspect, the research [19] introduces a secure Near Field Communication (NFC) smartphone access system using digital keys and Encrypted Steganography Graphical Passwords (ESGP). User perceptions and intentions are evaluated through experiments and surveys, emphasizing security as a key factor in adopting NFC ESGP systems. This offers valuable insights for enhancing security through two-factor authentication on NFC-enabled smartphones.

Further, recognizing Fog computing as an intriguing domain bridging the cloud and Internet of Things (IoT) necessitates a secure communication channel to prevent attacks. In the paper [33], the strengths and weaknesses of hybrid strategies of cryptography and steganography in fog environments, where real-time transmission is crucial, are discussed. This paper presents a novel Fog-Based Security Strategy (FBS2) that integrates cryptography and steganography techniques. The Cryptography Technique (PCT) entails two phases: confusion and diffusion, which scramble and modify pixel values of secret images using innovative methodologies. The Steganography Technique utilizes discrete wavelet packet transform, employing a new matching procedure based on the most significant bits of encrypted secret images and cover image pixels. Experimental results illustrate FBS2's superiority in efficiency, security, and processing time, executing it well-suited for fog environments.

Furthermore, the paper [36] explores Industry 5.0, which merges human and machine capabilities to meet complex manufacturing demands through optimized robotized processes. Industry 5.0 utilizes collaborative robots (cobots) for improved productivity and safety, while unmanned aerial vehicles (UAVs) are expected to have a significant role.

Despite UAVs' advantages like mobility and energy efficiency, challenges such as security and reliability persist. To address this, the article presents AIUAV-SCC, an artificial intelligence-based framework tailored for Industry 5.0. It consists of two main phases: image steganography-based secure communication and deep learning (DL)-based classification. Initially, a new image steganography technique is employed, integrating multilevel discrete wavelet transformation, quantum bacterial colony optimization, and encryption processes.

Another interesting method proposed in the research [85] for encrypting digital images using a special type of mathematical system called a chaotic system. Chaotic systems have properties that make them very difficult to predict and control, which is useful for encryption. The method proposed in this paper uses a specific type of chaotic system called the two-dimensional Hénon-Sine map (2D-HSM), which has been designed to be more effective than other chaotic systems for this purpose. Additionally, the method incorporates a technique inspired by DNA to further enhance the encryption process. This new encryption scheme aims to protect images when they are sent over the Internet. The paper presents experimental tests to show that this scheme performs better than other methods in terms of security and resistance to attacks.

Furthermore, advanced cloud computing is considered one of the prominent technologies offering cost-saving benefits and flexible services. With the increasing volume of multimedia data, many data owners choose to outsource their data to the cloud. However, this trend raises privacy concerns, as users relinquish control over their data. To address these concerns, reversible data hiding schemes for encrypted image data in cloud computing have been proposed by [86]. These schemes aim to ensure data security without relying on the trustworthiness of cloud servers. Theoretical analysis confirms the security and correctness of the proposed encryption model, with acceptable computation costs adjustable based on security needs.

We also focused on Conference papers that explore the combination of cryptography and steganography, covering various applications and technological domains. The work at [23], presents a novel framework that combines a hybrid encryption scheme using chaotic maps and 2D Discrete Wavelet Transform (DWT) Steganography to enhance security by maintaining patient privacy. Additionally, a web-based monitoring platform is deployed for tracking electronic medical records during transmission. Experimental results show that the proposed framework outperforms existing approaches in terms of accuracy, sensitivity, and perceptibility, with high imperceptibility and limited degradation in the stego image.

Along similar lines, the authors [29] present the aim of their study to protect the privacy and confidentiality of data during multimedia exchanges between two IoT hops in uncertain environments. To achieve this, a robust multilevel security approach based on information hiding and cryptography is proposed to deter attackers and ensure data confidentiality. Existing schemes often struggle to strike a balance between medical image quality and security, and directly embedding secret data into images followed by encryption can make it easy for intruders to detect and extract hidden information. This study yields superior results in terms of imperceptibility and security by employing the right method in the right context.

Also, another application aspect Reversible data hiding (RDH) ensures secure digital data transmission, especially vital in telemedicine where medical images and electronic patient records (EPR) are exchanged. This study [47] proposes a novel RDH scheme that embeds EPR data during image encryption. Using a block-wise encryption technique, the scheme hides EPR data bits within the encrypted image. A support vector machine (SVM)-based classification scheme is employed for data extraction and image recovery. Experimental results show superior performance compared to existing schemes in terms of embedding rate and bit error rate.

Further, Network security is crucial in safeguarding against malicious attacks, especially with the rapid growth of e-commerce worldwide. This study [52] proposes a novel approach to enhance online shopping security by minimizing the sharing of sensitive customer data during fund transfers. Combining text-based steganography, visual cryptography, and OTP (One Time Password), the proposed payment system ensures customer data privacy, prevents identity theft, and increases customer confidence. By utilizing steganography and visual cryptography, the method minimizes information sharing between consumers and online merchants, thereby enhancing data security and preventing misuse of information.

Further moving forward with another interesting research [62] that focusses on E-commerce platform transactions. this study proposes a two-layered security mechanism for e-transactions using dynamic QR codes. The first layer involves encapsulating payment information within a dynamic QR code, unique to each order, which includes bank details, user information, and order specifics. The second layer employs encryption through Secure Electronic Transactions (SET) to further secure the payment process. This dual-layer approach enhances security by introducing dynamic QR codes, reducing vulnerability to cyber-attacks and ensuring secure transmission of payment data. On the other side, the authors [3] proposed a lightweight dynamic encryption algorithm using DNA-based stream ciphers. This algorithm generates a one-time dynamic key (DLFSR) based on collected data, encoding both the text and key into a dynamic DNA format. The ciphertext is then produced through an

addition process using a proposed table, with decryption information hidden within for key distribution. Statistical tests and performance evaluations demonstrate the algorithm's effectiveness in providing security for restricted devices, outperforming previous approaches.

To safeguard IPv6 packet identities against Denial-of-Service (DoS) attacks, this paper [6] proposes a combination of cryptography and steganography methods. Ensuring secure communication in IPv6 network applications is crucial due to prevalent issues like DoS attacks and IP spoofing. The proposed approach involves generating unique identities for each node, encrypting them, and embedding them into transmitted packets. Upon reception, packets are verified to authenticate the source before processing. The paper conducts nine experiments to evaluate the proposed scheme, which includes creating IPv6 addresses, applying logistics mapping, RSA encryption, and SHA2 authentication. Network performance is assessed using OPNET modular, demonstrating improved computation power consumption and better overall results, including memory usage, packet loss, and traffic throughput. In a similar line, the paper [11] suggests a hybrid security method using hashing, encryption, and image steganography to better protect user credentials in databases. The aim is to help developers integrate strong password security practices into their software development process to prevent data breaches. Experimental results show the effectiveness of this approach.

Security is crucial across various applications, including cloud storage and messaging. While AES, DES, and RSA are common encryption methods, relying solely on one can lead to vulnerabilities if the encryption key is compromised. To address this, hybrid cryptography is employed in this research [12], combining existing techniques with three new methods. Data is divided into three sections and encrypted with AES, DES, and RSA respectively. Encryption keys are stored using LSB steganography in an image, ensuring additional security. Users must retrieve the keys from the image to access and decrypt the data stored in the cloud, enhancing overall security. Further, Castillo et al. [17] present a new mobile app that secures images using AES encryption and LSB steganography. It employs a 256-bit AES key for robust protection and utilizes the Diffie-Hellman algorithm for secure key exchange. The app development follows the Rapid Application Development Model, ensuring iterative refinement and early testing. Evaluation based on ISO/IEC/IEEE 29119 Testing Standards indicates user satisfaction with an overall mean rating of 4.17.

As mentioned above, one of the interesting areas is Cloud Computing (CC) which has emerged as a popular model for delivering services over the Internet, with Software as a Service (SaaS) being a prominent example. Despite its benefits, security remains a concern. This paper [24] presents an application model for securing SaaS applications hosted on private clouds. The model consists of two micro-services: an Application Layer Firewall to prevent malicious activity, and a secure login application for sensitive data transmission. Additionally, a Hidden Markov Model layer is implemented for intrusion detection. The second micro-service uses Advanced Encryption Standard (AES) for document encryption within the private cloud. Further security is provided through a novel Video Steganography approach using the Least Significant Bit (LSB) technique. Overall, the paper outlines a comprehensive approach to enhance security in SaaS applications.

Further, considering confidentiality and integrity important aspects for sharing confidential information while communication, the research [38] introduces "Stag-chain", a blockchain-based design combining steganography, AES encryption, and InterPlanetary File System (IPFS) Protocol for decentralized cloud storage. The image file is stored on the cloud temporarily, replaced by a normal image afterward. This scheme aims to develop an app ensuring data confidentiality, secure data transmission, and protection against unauthorized access. Furthermore, Madavi et al. [43] introduce a compact steganography technique for robust data hiding while maintaining perfect invisibility. It combines DES, AES, and RC4 encryption methods for enhanced security. The study aims to achieve data security using steganography with the Least Significant Bit (LSB) Algorithm and Hybrid Encryption, encrypting user input and concealing it within image files for maximum security during message transmission.

Additionally, the authors [51] introduce a highly secure web-based authentication system utilizing Image Steganography and the 128-bit Advanced Encryption Standard (AES) algorithm. This system encrypts user passwords using AES. Also, face identification photographs are used as stegoimages to conceal the encrypted passwords, further enhancing security. The proposed work demonstrated resilience against advanced steganalysis attacks, including the chi-squared attack and neighborhood histogram. The authors recommended this secure authentication method for future web applications dealing with sensitive user data.

In [65], the authors investigate using audio signal processing for cybersecurity in voice applications. As voice interfaces become ubiquitous in devices, the research focuses on securely identifying and authenticating users through cryptography and audio steganography, ensuring both security and usability. Also, the paper [66] introduces security strategies aimed at enhancing data protection in the cloud, addressing concerns such as confidentiality, accessibility, and integrity. By leveraging steganography, encryption-decryption techniques, compression, and file splitting, our

proposed approach aims to overcome the limitations of traditional data protection methods, providing clients with an effective and secure means to store and share information.

Further, the transmission of satellite images via the Internet has gained considerable attention, especially with the rise of cloud and web-based satellite information services. Ensuring secure and high-quality data transfer to users has become a priority. To address this in the research [70], a combination of steganography and cryptography techniques is employed. Steganography hides data within images, audio, or video, while cryptography ensures data remains unintelligible to cyber attackers. This fusion approach offers a unique method for information protection. The paper proposes combining steganography algorithms such as Least Significant Bit (LSB) and Most Significant Bit (MSB) with cryptography algorithms like Rivest-Shamir-Adleman (RSA) for enhanced security.

This is another interesting research under technology development [73]. The rise of multimedia applications has fueled the use of digital archives, with cloud storage being a common choice for storing, transmitting, and sharing multimedia content. However, the reliance on cloud services poses security risks, compromising data privacy. To mitigate these risks, data access is restricted to authenticated users, and data is encrypted before storage in the cloud. Cipher Text-Policy Attribute-Based Encryption (CP-ABE) is used to encrypt data and control access, but traditional CP-ABE requires substantial computing resources. To address this, an efficient pairing-free CP-ABE scheme using elliptic curve cryptography is proposed, reducing memory and resource requirements. However, even with CP-ABE, plaintext retrieval is easier with cryptanalysis. To enhance data security and ownership, cryptography is combined with steganography, embedding ciphertext into images to thwart cryptanalysis and improve data security and privacy, particularly for multimedia applications.

Further, Modern healthcare relies on secure medical imaging systems for accurate diagnosis. This paper [79] proposes a method to protect the JPEG compression processor used in these systems from threats like counterfeiting and Trojan insertion. By integrating robust structural obfuscation and hardware steganography, the approach ensures double-layered defense with minimal design cost. Also, Online shopping presents risks such as credit card fraud and identity theft. This paper [80] introduces a novel scheme to detect and prevent phishing sites using extended visual cryptography, steganography, and an Android application. The scheme reduces user interaction by automatically uploading shares and QR code details during authentication, enhancing security by minimizing errors from manual intervention.

Ensuring image security and copyright protection, especially post-COVID-19, is challenging. This paper [98] introduces SecDH, a medical data hiding scheme designed to address these challenges specifically for COVID-19 images. The scheme begins by normalizing the cover image to enhance resistance against geometric attack and computes a normalized principal component for embedding. Experimental results show SecDH's imperceptibility and advantages over traditional schemes. In a similar line, this research [100] introduces a robust technique with a high embedding capacity for color images. By fusing multi-focus images using NSCT and computing hash values for authentication, the technique enhances information richness and security. Embedding the fused image and hash value into the cover media using transformed-domain schemes, along with encryption, ensures higher security. Additionally, a hybrid optimization algorithm computes an optimal factor for improved imperceptibility and robustness. Experimental results demonstrate the technique's effectiveness and resistance to common attacks, achieving a 9.5% increase in robustness and an 8.8% enhancement in quality compared to existing works.

Further, the research [99] proposes SIELNet, a robust encryption algorithm for color images. Utilizing a novel chaotic map and custom network, SIELNet ensures secure data transmission and storage. Experimental results validate its superior performance, promising enhanced data integrity in Industry 5.0.

Furthermore, the evaluation of these techniques relies on a diverse set of metrics that assess their performance in terms of security, robustness, capacity, perceptual quality, and statistical characteristics. This research background provides an overview of the key evaluation metrics, tools, and attacks used for steganography, and cryptography, including their definitions and significance in assessing the effectiveness of covert communication methods. With the help of the following information on evaluation criteria, tools, and attacks, numerous research papers spanning both cryptography and steganography domains have been analyzed and are presented in Table 10. This provides readers with in-depth information to facilitate their understanding of the Results section with clarity.

I. **Evaluation criteria**

- *Peak signal to noise ratio* (PSNR) [1, 5, 7, 92, 95, 97] PSNR is a widely used metric in image processing that quantifies the quality of reconstructed signals by measuring the ratio of the peak signal power to the noise power. In steganography, PSNR is employed to evaluate the perceptual quality of stego images by comparing them to their original counterparts, with higher PSNR values indicating better image fidelity. The PSNR of the grey-level image is defined as follows:

$$PSNR = 10 \times log_{10}\left(\frac{255^2}{MSE}\right)$$

- *Mean square error* (MSE) [1, 22, 92, 95, 97] MSE measures the average squared difference between the pixel values of the original and reconstructed signals, providing a quantitative measure of reconstruction accuracy. In steganography, MSE is utilized to assess the distortion introduced by embedding hidden data, with lower MSE values indicating reduced perceptual distortion.

$$MSE = \frac{1}{WH}\sum(S(i,\ j) - C(i,\ j))^2$$

- *Correlation coefficient* (CC) [1, 9, 22, 95] CC serves as a robust metric commonly applied to evaluate message correlation, particularly within image formats through median filtering. While not extensively employed in steganography, its utility is more pronounced when messages adopt image form. In the realm of image watermarking, CC finds wider usage owing to the prevalent image-based nature of watermarks. Notably, CC's modus operandi doesn't hinge on error quantification but centers on computing the correlation between original message image pixels and their counterparts extracted from the message. Consequently, CC values, ranging from −1 to 1, signify correlation strength, with 1 denoting optimal correlation. Its computation can be executed using the following equation:

$$CC = \frac{\sum_x \sum_y (M_{xy} - \overline{M})(M\prime_{xy} - \overline{M\prime})}{\sqrt{(\sum_x \sum_y ((M_{xy} - \overline{M})^2)(\sum_x \sum_y (M_{xy\prime} - \overline{M\prime})^2}}$$

- *Capacity* [5, 92, 95, 97] Capacity refers to the maximum amount of hidden information that can be embedded within a cover signal without causing perceptible distortion. In steganography, capacity metrics assess the payload capacity of steganographic algorithms, guiding the selection of embedding techniques to achieve a balance between data hiding capacity and perceptual quality.
- *Structural similarity index* (SSIM) [7, 22, 33, 96] It's a metric used in image processing to quantify the similarity between two images. SSIM considers luminance, contrast, and structure, mimicking human visual perception. It's widely used in research to evaluate the quality of image compression, denoising, and restoration algorithms.
- *Human visual system* (HVS) *metrics* [7, 95] HVS metrics model the perceptual characteristics of the human visual system to evaluate the visual quality and perceptibility of stego signals. In steganography, HVS metrics such as the Structural Similarity Index (SSIM) and perceptual entropy are utilized to assess the visibility of embedded data and ensure imperceptibility to human observers.
- *Entropy* [33, 88, 96] Entropy measures the randomness or uncertainty of a signal and is used to quantify the information content of cover and stego signals. In steganography, entropy metrics assess the statistical properties of stego signals, with lower entropy values indicating a higher degree of hidden information. The entropy can be calculated for an 8-bit image as follows:

$H(I) = -\sum_{i=1}^{2^8} P(I_i) log_b P(I_i)$, where I denote the Intensity value, and $P(I_i)$ represents the probability of intensity value I_i.

- *Histogram analysis* [9, 45, 92, 95, 97] Histogram analysis examines the distribution of pixel intensities in cover and stego signals to detect statistical anomalies introduced by steganographic embedding. In steganalysis, histogram-based metrics evaluate the statistical differences between cover and stego signals, facilitating the detection of hidden information.
- *Bit error ratio* (BER) [9, 13, 22, 95] BER quantifies the ratio of incorrectly received bits to the total number of transmitted bits and is used to measure the accuracy of data transmission in digital communication systems. In steganography, BER is employed to evaluate the accuracy of data extraction from stego signals, with lower BER values indicating a higher level of data integrity.
- *Bits per pixel* (BPP) [41, 61, 85, 95] BPP measures the average number of embedded bits per pixel in stego images and is used to quantify the embedding efficiency of steganographic algorithms [96]. In steganography, BPP metrics assess the trade-off between embedding capacity and visual quality, guiding the selection of embedding parameters.
- *Signal-to-noise ratio* (SNR) [14, 95] SNR measures the ratio of signal power to noise power and is used to quantify the quality of transmitted signals in communication systems. In steganography, SNR metrics evaluate the robustness of steganographic algorithms to noise interference, with higher SNR values indicating better signal quality.
- *Amplitude difference* (AD) [14] AD measures the difference in amplitude or magnitude between the original plaintext and the corresponding ciphertext resulting from the encryption process. It quantifies the level of distortion introduced during encryption, with lower AD values indicating minimal alteration in amplitude between the plaintext and ciphertext. The assessment of AD aids in evaluating the perceptual quality and robustness of cryptographic algorithms, ensuring that encrypted data retains fidelity and is resistant to unauthorized tampering.
- *Avalanche effect* (AE) [14] AE characterizes the sensitivity of a cryptographic algorithm to small changes in the input,

resulting in significant changes in the output ciphertext. A robust cryptographic algorithm exhibits a pronounced avalanche effect, where even minor modifications in the input plaintext lead to extensive changes in the resulting ciphertext. AE plays a pivotal role in assessing the security and strength of encryption algorithms, as it indicates the extent to which encrypted data conceals underlying patterns and resists cryptanalysis attempts aimed at deciphering the original plaintext.

- *Bits per code* (BPC) [14] BPC refers to the average number of bits used to represent each symbol or code in a given data encoding scheme or communication system. It quantifies the efficiency of data representation and transmission by measuring the ratio of the total number of bits to the total number of codes or symbols transmitted. In data encoding and compression techniques, a lower BPC indicates higher efficiency in representing data using fewer bits, while ensuring minimal information loss or distortion.
- Throughput [14]: Throughput represents the rate at which data is successfully transmitted or processed over a communication channel or system within a specific time. It measures the amount of data transferred per unit time and is typically expressed in bits per second (bps) or a similar unit of data transmission rate. Throughput is influenced by factors such as channel bandwidth, data encoding efficiency, error correction mechanisms, and system latency. Higher throughput values indicate greater data transmission capacity and efficiency, enabling faster and more reliable communication.
- *Uncorrectable error rate* (UER) [14] UER is a metric used in error detection and correction systems to quantify the frequency or probability of errors that cannot be successfully detected or corrected by error correction mechanisms. It represents the rate of errors that remain undetected or uncorrected despite the implementation of error detection and correction techniques. A low Uncorrectable Error Rate is desirable in communication systems, indicating a high level of reliability and effectiveness in error detection and correction processes.
- *Cronbach's alpha* (CA) [19] Cronbach's alpha is a measure of internal consistency and reliability of steganographic or cryptographic algorithms. It ensures that they consistently perform as intended across different datasets or scenarios.
- *Composite reliability* (CR) [19] Composite reliability is another measure of internal consistency reliability, similar to Cronbach's alpha. It evaluates the reliability of a set of items in measuring a latent construct, taking into account the factor loadings of the items.
- *Average variance extracted* (AVE) [19] AVE is a measure of convergent validity in structural equation modeling (SEM). It assesses the amount of variance captured by a latent construct in relation to the variance due to measurement error.
- *Structural equation modeling* (SEM) [19] SEM is a statistical method used to test and validate theoretical models that specify relationships among observed and latent variables. It allows researchers to assess the structural relationships between variables and evaluate the goodness-of-fit of the proposed model.
- *Normalized chi-square* (Normalized $\chi 2$) [19] Normalized chi-square is a goodness-of-fit measure used in SEM, indicating the discrepancy between the observed and expected covariance matrices relative to the degrees of freedom.
- *Goodness-of-fit index* (GFI) [19] GFI is a measure of the overall fit of the structural equation model to the observed data. It assesses the extent to which the model reproduces the observed covariance matrix.
- *Root mean square error* (RMSE) [19] RMSE is a measure of discrepancy between observed and predicted values in SEM. It quantifies the average difference between observed and model-estimated covariance matrices, with lower RMSE values indicating better model fit.
- *Normed fit index* (NFI) [19] NFI is a goodness-of-fit index in SEM that evaluates the relative improvement in the fit of the proposed model compared to a null model. Higher NFI values indicate a better fit.
- *Tucker lewis index* (TLI) 19] TLI, also known as the Non-Normed Fit Index (NNFI), is a measure of incremental fit in SEM. It compares the proposed model to a baseline model with uncorrelated variables, with TLI values close to 1 indicating a good fit.
- *Comparative fit index* (CFI) [19] CFI is another measure of incremental fit in SEM, assessing the improvement in the fit of the proposed model relative to a null model. CFI values close to 1 indicate a good fit.
- *Normalized cross-correlation coefficient* (NCCC) [33] NCCC is employed to measure the similarity between the cover and stego-images. A high NCCC value close to 1 signifies that the steganographic process has been performed effectively, resulting in minimal detectable differences between the original cover image and the stego-image, thereby ensuring the concealment of hidden information within the cover image. This can be evaluated as $\gamma_{p,q} = \frac{cov(p,q)}{\sqrt{D(p)\sqrt{D(q)}}}, withD(p),$ where p and q represent two variables that can denote either the secret and decrypted images in the cryptography process or the cover and stego-images in the steganography process. The correlation coefficient is γ, and each of the $cov(p, q)$, $D(p)$, and $D(q)$, correspond to the covariance and variances [33] of these variables p and q.
- *Number of pixel change rates* (NPCR) [33] The NPCR metric is utilized during the encryption stage to evaluate the disparity between cipher images before and after a single pixel alteration in a plaintext image. Let P represent the total number of pixels, where C1 and C2 denote the

cipher images before and after the pixel change, respectively. Additionally, D is a bipolar array defined such that $D(i, j) = 0\ if C1(i, j) = C2(i, j)$, $and D(i, j) = 1$ otherwise. The NPCR determines the percentage of differing pixel values between the original and encrypted images. This metric gauges the resilience of the encryption method against potential intrusions and attacks, with higher NPCR values indicating a stronger strategy. $N(C1, C2) = \sum_{i,j} \frac{D(i,j)}{P} \times 100\%$.

- *Unified average changing intensity* (UACI) [33] UACI calculates the mean intensity of variances between two images with the following formula: $UACI = \frac{1}{2}[\sum_{pq} \frac{I_1(p,q)\_I_2(p,q)}{255}] \times 100$, where I_1, I_2 represent the two encrypted images derived from the original image by altering a single pixel, with, p and q denoting the coordinates of the pixels being considered I_1, and I_2 respectively.
- *Percentage residual difference* (PRD) [34] This metric assesses the variance between the original ECG host signal and the resulting watermarked ECG signal, calculated as $PRD = \sqrt{\frac{\sum_{i=1}^{N}(x_i - y_i)^2}{\sum_{i=1}^{N} x^2{}_i}}$, where x represents the Original ECG signal, and y is the watermarked signal.
- *Weighted wavelet percentage residual difference* (WWPRD) [34] This metric is used particularly in the context of watermarking techniques. It is employed to evaluate the effectiveness of image watermarking algorithms by quantifying the perceptual differences between the original image and the watermarked version. In WWPRD, the residual difference between the original image and the watermarked image is calculated in the wavelet domain. By analyzing the WWPRD values, researchers can assess the trade-off between watermark invisibility (how imperceptible the watermark is to human observers) and robustness (how resistant the watermark is to various image processing operations and attacks).

II. **Steganography and steganalysis tools used**

- *Stegdetect* [10] This tool is designed to detect and analyze hidden information within digital media, providing users with powerful steganalysis capabilities. It employs advanced algorithms and techniques to identify subtle modifications or anomalies in digital files that may indicate the presence of hidden information. StegDetect [10] is widely used by digital forensics experts, law enforcement agencies, and cybersecurity professionals to uncover hidden threats and investigate potential security breaches.

III. **Steganalysis attack** [61, 75, 86]

- *Salt and pepper noise* Salt and Pepper Noise, also known as impulse noise, introduces sporadic white and black pixels in an image, resembling grains of salt and pepper scattered throughout the image. This type of noise typically occurs due to errors in data transmission or faults in image acquisition devices.
- *Additive white gaussian noise* (AWGN) AWGN is a type of noise that follows a Gaussian distribution and is characterized by its constant power spectral density across all frequencies. It represents random variations in pixel values added to the original image, often resulting from electronic interference or sensor noise in imaging devices.
- *Median filtering* Median filtering is a spatial domain filtering technique commonly used to remove impulsive noise such as Salt and Pepper Noise. It replaces each pixel value with the median value of its neighboring pixels within a defined window, effectively reducing the impact of outliers caused by noise.
- *Lowpass filtering* Lowpass filtering is a technique used to suppress high-frequency components in an image while preserving low-frequency information. It is commonly employed to mitigate noise by smoothing the image, thereby reducing the effect of high-frequency noise components such as AWGN.
- *Weiner filtering* Weiner filtering is a signal processing technique used to deconvolve images corrupted by additive noise, such as AWGN. It employs a frequency domain approach to estimate and suppress the noise while enhancing the signal-to-noise ratio in the restored image.
- *Sharpening* Sharpening techniques aim to enhance the perceived sharpness and clarity of an image by accentuating edges and details. However, when applied to noisy images, sharpening can exacerbate the visibility of noise, making it a potential target for attacks aimed at degrading image quality.
- *Histogram equalization attack* Histogram equalization is a technique used to adjust the contrast of an image by redistributing pixel values across a wider dynamic range. However, adversaries can exploit this technique to amplify the visibility of noise, especially in regions with low contrast, thereby degrading the overall quality of the image.
- *Rotation attack* Rotation attacks involve rotating an image by a certain angle, which can introduce geometric distortions and potentially exacerbate the visibility of noise. Adversaries may employ rotation attacks to degrade the quality of images, particularly those affected by noise, as part of malicious activities or security breaches.
- *Pitch removal attacks* These involve the removal or alteration of specific pitch frequencies in audio signals. These attacks are often used in scenarios where certain

frequency components need to be suppressed or modified, such as in audio watermarking or enhancement techniques.

- *Bit-plane removal attacks* This type of attack targets the bit-plane decomposition of images. In digital image processing, images are often represented using a bit-plane decomposition, where each bit-plane represents a different level of image detail or intensity. Bit-plane removal attacks aim to remove or modify specific bit-planes, thereby altering the visual appearance or content of the image.
- *Chi-Square attack* [89] This is a prominent technique used to detect the presence of hidden information within digital media, particularly images. This attack leverages statistical analysis to uncover inconsistencies or anomalies in the distribution of pixel values within an image. The rationale behind the Chi-Square Attack lies in the fact that steganographic embedding typically introduces subtle changes to the statistical properties of an image, such as the distribution of pixel values. These changes, while imperceptible to the human eye, can be detected through statistical analysis methods like the chi-square test.
- *Regular singular (RS) analysis* [75] RS analysis involves analyzing the regular and singular components of an image to identify irregularities or inconsistencies introduced by steganographic embedding techniques. This analysis leverages mathematical properties to distinguish between the regular content of an image and any additional hidden data.
- *Binary similarity measures (BSM) analysis* [75] BSM are statistical measures used to assess the similarity between the binary representations of two images. In steganalysis, these measures are employed to compare the binary data of an original image with that of a potentially steganographic image. Deviations or discrepancies in binary similarity may indicate the presence of hidden data.

The next section discusses the methodology employed by this research.

3 Methodology

In this section, we outline a reproducible search strategy employed for conducting a comprehensive literature survey. Initially, data collection was performed utilizing the selected databases, namely[2]Scopus,[3]IEEE Digital Library, and[4]ISI Web of Science, with search queries formulated as detailed in Sect. 3.1. Subsequently, the study selection process was executed, elucidated in Sect. 3.2. Finally, the final data was extracted from the literature, as described in Sect. 3.3. The[5]Parsifal tool was employed to optimize the efficiency of the review process, including the tasks of reviewing, screening, and extracting relevant literature.

3.1 Data gathering (DG)

The initial step in the literature exploration process involves data gathering. Two distinct literature searches were conducted: one encompassing journal articles and a supplementary search focused on conference papers. These papers are also discussed in Sect. 2. The results of the additional literature search contribute primarily to gaining further insights related to RQ1. To effectively explore the selected databases, essential keywords, and criteria were identified. While both literature searches share common keywords, their criteria, such as publication year and language, were slightly adjusted to ensure a manageable scope. These criteria were refined through an iterative process that involved fine-tuning the keywords and assessing the quantity of relevant literature available on Scopus. The final keywords used for the search query can be expressed as follows:

Search Query: *("cryptography" AND "steganography") AND ("application" OR "real-world") AND ("security" OR "cyberattack" OR "cybersecurity").*

Upon utilizing the specified keywords, the three databases collectively yielded a total of 749 results as of May 24th, 2023. Subsequently, inclusion criteria, encompassing year, language, and type, were applied to filter the obtained results. The application of these criteria is detailed in the following two sub-sections.

(a) DG-Literature Search 1: Journal Articles. A comprehensive literature search was conducted specifically for journal articles, with the databases accessed on May 24th, 2023. The criteria applied to this search are as follows:

- Only literature published from 2010 onwards was included.
- The literature must be classified as a journal article, excluding review papers, conference papers, books, and other sources.
- Publications from any region are considered, but they must be in English.

The search encompassed the examination of titles, abstracts, and keywords. These criteria collectively establish the following additional query options:

[2] https://www.scopus.com/

[3] https://ieeexplore.ieee.org/

[4] https://www.webofscience.com/

[5] https://parsif.al/

year > = 2010
AND language = = English
AND type = = Journal Article

These search criteria, along with the keywords from Sect. 2.1, resulted in the total number of 217 journal articles:

- Scopus: 179
- IEEE: 7
- Web of Science: 31

After removing duplicates using the Parsifal tool, 194 journal articles were left for further analysis.

(b) DG-Literature Search 1: Conference Papers. Furthermore, a supplementary literature search focusing on conference papers was conducted, with the databases accessed on June 23rd, 2023. The search criteria and query vary slightly from the previous literature search as outlined below:

- Only conference papers from conference proceedings published from 2018 onwards were considered.
- Review papers, journal articles, books, and other sources were excluded.
- Similar to the previous search, publications from any region were eligible, provided they were in English.

These criteria lead to the following query options:
year >= 2018
AND language == English
AND type == Conference Paper
AND source type == Conference Proceedings

These search criteria, along with the keywords from Sect. 2.1, resulted in a total number of 147 conference papers:

- Scopus: 93
- IEEE: 43
- Web of Science: 11

After removing duplicates using the Parsifal tool, 113 conference papers were left for further analysis.

3.2 Study selection (SS)

The subsequent stage of the literature exploration process involves the selection of pertinent studies, which comprises two distinct phases. The following are seven conditions established to ensure that only literature addressing the research questions outlined in Sect. 1 is considered while filtering out literature of insufficient quality. It is important to note that the two literature searches applied these conditions differently

1. The paper focuses on researching the combination of cryptography and steganography disciplines.
2. The paper investigates the application of cryptography and steganography within specific domains (e.g., medical, military, financial) or contexts rather than a general application for "secure communications."
3. The paper addresses efforts to enhance the security of a system or process rather than solely transmitting additional data.
4. Is the objective of the paper clearly defined?
5. Have related works been adequately studied?
6. Is the methodology employed in the paper clearly described?
7. Are the results presented clearly and measurably?

(a) SS-Literature Search 1: Journal Articles. In the first literature search focused on journal articles, papers were assessed for relevance based on conditions 1–3 (Sect. 3.2), considering the information presented in the title and abstract. Subsequently, papers were further scrutinized to determine if they met conditions 4–7 (Sect. 3.2) by examining their contents. Only papers that fulfilled all seven conditions were included in the selection process. As a result of this rigorous selection process, the initial total of results was reduced to 24 journal articles. The flow chart depicted in Fig. 2a illustrates the sequential steps involved in data gathering and study selection. Papers that discussed no specific application, such as "secure communications," were not categorized as such since a significant number of such papers were already omitted during the search query phase. Including them in the list would have resulted in an incomplete compilation of relevant articles.

(b) SS-Literature Search 2: Conference Papers. In the second literature search, focusing on conference papers, the selection process entailed examining papers for conditions 1–3 (Sect. 3.2) based on the information presented in the title and abstract. These conditions were crucial in determining whether a paper should be considered for RQ1. As a result of this selection process, 21 conference papers met the criteria. It is worth noting that two papers were identified as having been released before 2018 and were subsequently manually filtered out. The flow chart illustrated in Fig. 2b provides a visual representation of the data-gathering process and study selection for this search.

3.3 Data extraction (DE)

The third step of exploring literature is extracting data. Data extraction consists of two parts, both performed using Parsifal. To answer RQ1 features related to a paper's application have been extracted (both literature searches). The list of features evolved during the process of extraction as it was expanded, restructured, and finalized (Sect. 3.1) to encompass all encountered literature. Next, to answer RQ2 and RQ3, information related to the algorithms and metrics,

advantages, limitations, and evaluation methods discussed by the literature were extracted (only literature search 1: journal articles). The results of data gathering, study selection, and data extraction are presented in the subsequent sections.

4 Results

In this section, we present the comprehensive findings derived from the systematic review, addressing the research questions outlined in Sect. 1. To facilitate a better understanding of the findings, figures, and tables are provided. The subsequent sections are organized in alignment with the order of the research questions. Section 4.1 delves into the encountered types of applications and explores potential categorization approaches. Additionally, Sect. 4.2 discusses the applications, their limitations, and advantages identified during the review process. Lastly, Sect. 4.3 focuses on the analysis methods employed in the literature. By following this structured arrangement, we aim to provide a clear and cohesive presentation of the research findings, offering valuable insights into the combined application of steganography and cryptography in various domains and contexts.

4.1 RQ1: exploring applications

For each study, relevant characteristics pertaining to the context in which the combined application of steganography and cryptography is explored were extracted. The analysis of the literature emphasizes the significance of categorizing the application of each article in two distinct ways:

- *The application domain*: This refers to the specific industry sector or domain in which an application operates. The encountered application domains include financial, government, medical, and transportation.
- *The technological domain/technology* [72]: This aspect involves identifying one or more technological topics associated with an application. Technologies are considered tools that can be employed across various domains to solve diverse problems or perform various tasks. The encountered technologies include Big Data, Blockchain, Cyber-Physical Systems (CPS), Cloud Computing (Cloud), Edge Computing (Edge), Fog Computing (Fog), Internet of Things (IoT), IPv6, Machine Learning (ML), Mobile Computing (Mobile), Personal Computing (Personal), Satellite Imaging (Satellite), Unmanned Aerial Vehicles (UAVs), and Voice Operated Systems (Voice).

By employing these two distinct categorizations, namely **Application Domain and Technological Domain**, it becomes possible to identify specific commonalities and differences within the applications. This facilitates informed research and the development of tailored solutions for specific application domains or technologies. Notably, this categorization approach differs from how other reviews, as exemplified by [45], typically categorize applications. While some studies may focus on applications specific to a particular application domain, such as the medical domain, other articles ([1, 7, 9, 14, 19, 33, 36, 85, 86, 90] [5, 10]) may exclusively concentrate on applications within a technological domain. A technological domain can be applicable across numerous application domains. Given these considerations, categorization by application domain is given precedence, and cases, where the application domain or technological domain could not be determined, have been excluded from categorization. Furthermore, irrespective of the application or technological domain, the specific focus or functionality of each application is also determined.

- **Functionality:** This refers to the specific features, tasks, or roles performed by an application within its domain. It is important to note that security is considered a common role across the explored literature and is, therefore, not specified as functionality. Examples of functionalities include *Smart Monitoring, Anonymization, Healthcare Data Transmission, Vehicle Diagnostics, Malware Detection, and Industry 4.0/5.0 Implementation.*

The subsequent sections present the results obtained from both literature searches, providing further insights into the combined application of steganography and cryptography.

4.1.1 Journal articles

The findings from literature search 1, pertaining to RQ1, are presented in two tables. Table 1 provides an overview of articles and their corresponding application domains, while Table 2 focuses on the technologies employed, reflecting the split categorization approach. The core functionality of each paper studied for this review is explicitly mentioned in both tables. In cases where certain studies solely concentrate on a technological domain, potential application domains have been specified in italics (please refer to Table 2). These application domains are either suggested by the authors themselves or inferred based on similar literature. It is worth noting that technology often has applicability across a broader range of application domains. In such instances, the application domain is identified as 'Cross-Domain.' As showcased in Table 1 and Table 2, a total of 12 journal articles from each table were analyzed, with each article focusing on distinct application domains and their corresponding technological domains.

Table 1 Journal papers focusing on the Application Domain (bold) and (optionally) Technological Domain

Paper details		Domain details		
Ref.	Objective	Application domain	Technological domains	Functionalities
[13]	Securing the transmission of Electronic Patient Information (EPI) using RDH	**Medical**	N/A[a]	Healthcare data transmission, DICOM
[22]	Encrypt and hide diagnostic text data in medical images using RDH		Internet of Things	Remote Patient Monitoring
[34]	Securing the transmission of signals of remote Electrocardiogram (ECG) monitoring systems		Cloud Computing	Healthcare data transmission and storage
[41]	Securing patient details during transmission for remote diagnosis by hiding them inside (Non-Region of Interest) NROI medical images using RDH		Internet of Things	Healthcare data transmission
[45]	Securing the transmission of DICOM images		N/A[a]	Healthcare data transmission, DICOM
[56]	Securing patient details and images during transmission			Healthcare data transmission
[61]	Embedding Electronic Patient Records (EPR), watermarks, and checksums in medical images using RDH			
[78]	Securing a JPEG at the hardware level is used in medical image transmission from counterfeiting, cloning, and Trojan insertion			Healthcare data tampering Protection
[48]	Securing the transmission of vehicle diagnostics (DoIP) and software updates (OTAs)	**Transportation**	Cloud Computing, Edge Computing	Vehicle diagnostics and updates
[75]	Implementation of an E2E verifiable online voting system using voting receipts	**Government**	Web Applications	Voting
[87]	Two-tiered video surveillance: anonymization of sensitive parts with separate decode authorization levels		Internet of Things	Smart monitoring, Anonymization

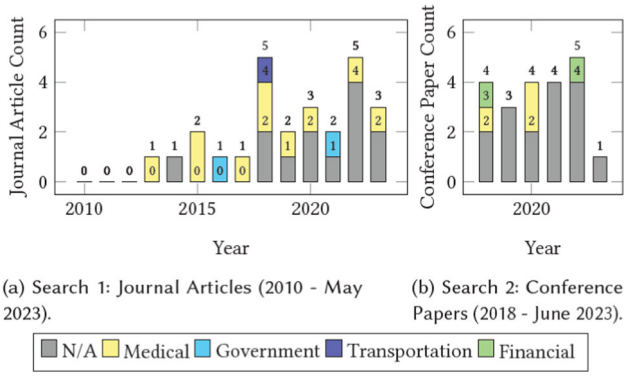
[a]There is no apparent involvement of a technology in the topic
[a]There is no apparent involvement of a technology in the topic
[a]Possible domains based on the technology used (incl. but not limited to) [64]
[a]Suggested by the authors
[a]There is no apparent involvement of a technology in the topic
[a]Reversibility not applicable

Figure 3a displays journal articles published from 2010 to 2023, categorized by application domains *(Medical, Government, and Transportation)* or technological domains *(N/A)*. The figure reveals a modest increase in articles exclusively centered on technological domains, surpassing those focused on application domains. Considering the diverse potential of these technologies across various application domains (e.g., IoT [63]), it is advisable to prioritize innovation in a broader sense. Subsequently, refining these technologies for specific application domains holds the potential for even greater rewards. On the other hand, Fig. 3b presents conference papers published between 2018 and 2023. In addition to the medical domain, as observed in the Journal articles shown in Fig. 3a, there is a notable trend toward the financial domain in conference papers in the realm of combining and applying cryptography and steganography. More information on the Conference papers can be found in subsection 4.1.2.

Figure 4 provides visual representations of the distribution of application domains (Fig. 4a) and technological domains (Fig. 4c) based on the data presented in Table 1. In Fig. 4a, it is

Table 2 Journal papers focusing on Technological Domains (bold) and (optionally) recommended Application Domains

Paper details		Domain details		
Ref.	Objective	Application domain	Technological domains	Functionalities
[1]	Securing UAV image transmissions and classification of images	*Cross-Domain (suggested by authors)*	**Internet of Things, Unmanned Aerial Vehicles**	Industry 4.0
[5]	Hiding encrypted data in available audio files to protect it from unwanted access	*Cross-Domain (suggested by authors)*	**Personal Computing**	Data storage
[7]	Applying combined Improving the capacity of image steganography		**Internet of Things**	Data transmission
[9]	Operating on homomorphically encrypted images to securely handle data in the cloud using RDH	*Medical, Military (suggested by authors),*	**Cloud Computing**	Privacy Protection
[10]	Hiding malicious applications in images to evade detection by Android anti-malware tools	*Cross-Domain (suggested by authors)*	**Mobile Computing**	Malware detection, Malware development
[14]	Improving performance and confidentiality of big data transmissions using GPU	*Energy, Medical, Finance*[a]	**Cloud Computing, Big Data**	Data transmission, Healthcare data transmission
[19]	Customizing the security level of the use of NFC on a phone for authentication: a 2FA system	*Entertainment, Finance*	**Mobile Computing, Cloud Computing**	Access control
[33]	Securing communication between IoT devices and the cloud using fog computing	*Cross-Domain (suggested by authors)*	**Internet of Things, Fog Computing**	Data transmission
[36]	Securing UAV image transmissions over the Internet and hiding the UAV network and classification of images	• *Cross-Domain (suggested by authors)*	**Internet of Things, Unmanned Aerial Vehicles**	Industry 5.0
[85]	Protecting image data in cloud computing using RDH	*Military (suggested by authors), Cross-Domain*	**Cloud Computing**	Access Control, Privacy protection
[86]	A Reversible Data Hiding scheme for securing customer data storage	*Medical*	**Cloud Computing**	Access Control
[90]	Secure communication over a covert channel in the measurements of a dynamic system	*Cross-Domain*[a]	**Cyber-Physical Systems**	N/A



(a) Search 1: Journal Articles (2010 - May 2023).

(b) Search 2: Conference Papers (2018 - June 2023).

Fig. 3 Distribution of literature in application and technological domains (N/A) over time

evident that the majority (n = 9, [13, 22, 34, 41, 45, 56, 61, 78, 88]) out of the total 12 articles focus on the medical domain, suggesting a relatively narrow focus of research in this area. Furthermore, only a small number of articles concentrate on governmental applications (n = 2, [75, 87]) and transportation (n = 1, [48]). Similarly, the occurrences of technological domains are visualized in Fig. 4c. Notably, technologies with an occurrence of 1 are grouped under 'Other,' which includes Big Data, Fog Computing, Web Applications, Personal Computing, Edge Computing, and Cyber-Physical Systems. The visualization in Fig. 4b and d is completed in subsection 3.1.2, where the conference papers are analyzed in depth. After analysis of the journal articles, it becomes evident that only

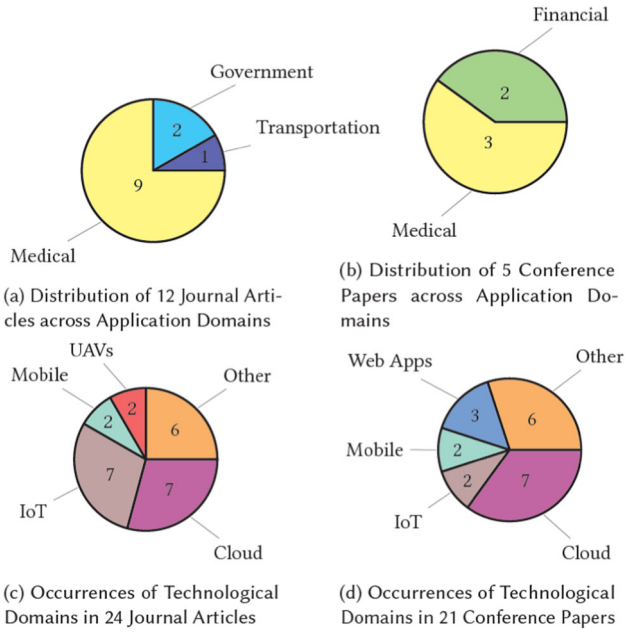


Fig. 4 Distributions of domains of journal articles (left) and conference papers (right)

one article from 2018 focuses on an application in the Transportation domain. Furthermore, in both 2021 and 2022, there is a lack of publications in the medical domain, whereas the four preceding years had such publications. Another notable observation is the surge in articles focusing on a specific technology in 2022. However, the applications discussed in these articles ([7, 36, 86, 90]) seem unrelated, making it challenging to identify any underlying reason behind this trend.

Furthermore, an attempt was made to employ the VOSviewer[6] tool to identify any authorship overlap among the identified journal articles. However, none of the articles displayed any shared authors, indicating a dispersed distribution of researchers working on the topic. This suggests that research on the combined approach of steganography and cryptography is relatively new, aligning with the increasing trend observed in the number of articles over the past 13 years in Fig. 3a. However, it is important to consider that additional factors may contribute to this observation. A more detailed discussion of journal articles focusing on specific application domains is provided in Sect. 3.2.

4.1.2 Conference papers

To gain further insights, conference papers were also subjected to analysis. The results of this additional literature search are presented in Tables 3 and 4, providing additional data for a comprehensive review. Similarly, to journal papers, the publication years of conference papers are depicted in Fig. 3b. Notably, there has been a relatively consistent number of papers published each year, suggesting either a sustained interest in combining steganography and cryptography or a stabilization of the field following a previous period of change. However, due to time constraints, papers published before 2018 were not explored in this study. Surprisingly, from 2018 to 2023, out of the 21 papers analyzed, only a few (n = 5) focused on specific application domains (as seen in Fig. 4b). These papers predominantly spanned the medical domain (n = 3, [23, 29, 47]) and a newly emerging financial domain (n = 2, [52, 62]). Once again, the medical domain emerged as the most popular area of application. Furthermore, while approximately 50% of the identified literature in journal articles explored applications in specific domains, only 24% of conference papers did the same. This disparity may further emphasize the trend of developing technologies in a more generalized sense rather than focusing exclusively on specific application domains. Similarly, Fig. 4d showcases the technological domains, revealing the presence of three prominent technologies shared between journal articles and conference papers: Mobile Computing, the Internet of Things, and Cloud Computing, with Cloud Computing being particularly prevalent. It should be noted that making a direct comparison between the two searches is challenging due to the difference in the time covered by the literature.

4.2 RQ2: advantages, limitations, and trade-offs

In this section, we discuss the observations made regarding the algorithms and methodologies employed in the journal articles. Firstly, we present general observations, and subsequently, we delve into the three application domains encountered in the journal articles, namely Government, Medical, and Transportation The research papers are also sorted out (as listed in Table 1). The research papers are also arranged in ascending order according to these three categories. The full data collected for this RQ2 can be found in Table 5. Further, there are other categories identified from Tables 1 and 2, such as Cross-Domain, Medical-Military, Energy, Medical, Finance, and Military; Cross-domain is also reflected in Table 5. The research papers are discussed in Sect. 2.

- Government application domain

This category focuses on two articles [75, 87] that explore the application of both steganography and cryptography in the government domain, specifically in the areas of surveillance and voting. These articles are listed in Table 6. Each article presents different approaches with their respective strengths and limitations.

[6] https://www.vosviewer.com/

Table 3 Conference papers focusing on the application domain (bold) and (optionally) technological domain

Paper details		Domain details		
Ref.	Objective	Application Domain	Technological domains	Functionalities
[23]	Secure Transmission and Repository Platform for Electronic Medical Images: Case Study of Retinal Fundus in Teleophthalmology	**Medical**	Web Apps	Healthcare data transmission and storage
[29]	Based on IoT Healthcare Application for Medical Data Authentication: Towards A New Secure Framework Using Steganography		Internet of Things	Healthcare data transmission, Privacy Protection
[47]	Reversible Data Hiding Scheme during Encryption Using Machine Learning		Machine Learning	Healthcare data transmission
[52]	Secure Transaction System using Collective Approach of Steganography and Visual Cryptography	**Financial**	N/A[a]	Online payments, Privacy protection
[62]	Two-Layer Secure Mechanism for Electronic Transactions			Online payments

- The first article [75] proposes a two-tiered video surveillance system that offers robustness against cipher-breaking attacks. However, the quality of the recovered data is dependent on the compression rate of the Compressed Sensing (CS) technique used. Additionally, the system could be enhanced to accommodate more than two levels of authorization.
- The second article [87] introduces an online voting system that ensures individual verifiability and security. However, it is susceptible to certain security challenges, such as collusion among polling officers and network eavesdropping. The system provides receipts to voters, but this poses a potential issue in case users lose their receipts. Improvements, such as exploring alternative algorithms, may enhance the system's performance, such as reducing the size of receipts.

Overall, these articles highlight different aspects and considerations in the government domain when implementing steganography and cryptography, emphasizing both the strengths and areas for potential improvement in their respective approaches.

- Medical application domain

This section focuses on nine articles that explore applications in the medical domain. The articles are listed in Table 7, along with their respective advantages and limitations.

Among these articles, three papers ([56, 61, 88]) incorporate the use of chaotic algorithms in their encryption methods. For example, [56] presents a transmission system for generic data that utilizes chaotic encryption based on a 2D-Henon map ([84]). However, limited practical implementation details are provided, and future works could be drawn upon [53] for a more in-depth analysis of the implementation aspects. One drawback is that these three papers lack performance analysis and key measurements such as Computation Time (CT) and Throughput (TP) for the chaotic algorithms. This limitation hampers the assessment of their potential for real-time systems. Nevertheless, [61, 88], which also employs chaotic encryption, can serve as inspiration for similar approaches. It should be noted that not all chaotic encryption algorithms, due to their complex iterative operations, are suitable for real-time systems. However, less resource-intensive methods like [60] could be considered viable alternatives. This aspect could be explored as a future research direction in the field.

- Health data in IoT

Two papers ([22, 34]) focus on health data transmissions from IoT devices, particularly in the context of remote patient monitoring. These devices typically prioritize low power consumption and low computational complexity. In [34], data is concealed within ECG signals, while [22] utilizes image steganography. Both papers employ encryption before embedding the data. In [34], the receiver must possess knowledge of the encryption and embedding keys, and no key is transmitted. On the other hand, [22] embeds both the data and the encryption key. [34] employs XOR cipher for its computational simplicity, while [22] utilizes AES ([30]) and RSA ([90]) encryption methods. It is worth considering more secure or efficient alternatives, such as TEA and

Table 4 Conference papers focusing on technological domains (bold) and (optionally) recommended application domains

Paper details		Domain Details		
Ref.	Objective	Application Domain	Technological domains	Functionalities
[3]	Using DNA In A Dynamic Lightweight Algorithm For Stream Cipher In An IoT Application	*Cross-Domain*	**Internet of Things**	Sensor data transmission
[6]	Node Protection using Hiding Identity for IPv6-Based Network		**IPv6**	Node Protection
[11]	Protecting User Credentials against SQL Injection through Cryptography and Image Steganography		**Web Applications**	Password Protection
[12]	Secure File Storage using Hybrid Cryptography		**Cloud Computing**	Data storage
[17]	Blocksight: A mobile image encryption using advanced encryption standards and the least significant bit algorithm		**Mobile Computing**	Data storage
[24]	Multilayer Technique to Secure Data Transfer in Private Cloud for SaaS Applications		**Cloud Computing**	SaaS
[39]	Stagchain—A Steganography-based Application Working on a Blockchain Environment		**Blockchain, Decentralized Cloud Computing**	Data storage
[43]	Enhanced Cloud Security using Cryptography and Steganography Techniques		**Cloud Computing**	Data storage
[51]	Web authentication security using image steganography and AES encryption		**Web Applications**	Password Protection
[57]	An Efficient Image Encryption Reversible Data Hiding Technique to Improve Payload and High Security in Cloud Platforms		**Cloud Computing**	Privacy Protection
[65]	Enhancing cyber security using audio techniques: A public key infrastructure for sound		**Voice Operated Systems**	Voice Recognition
[66]	Encryption, File Splitting, and File Compression Techniques for Data Security in a virtualized environment		**Cloud Computing**	Data storage
[70]	Secure Fusion of Crypto-Stegano-Based Scheme for Satellite Image Application		**Satellite Imaging**	Data transmission
[73]	Pairing-free CP-ABE-based cryptography combined with steganography for multimedia applications		**Cloud Computing**	Data storage
[79]	Phishing Site Detection and Blacklisting Using EVCS, Steganography Based on Android Application		**Cloud Computing**	Phishing prevention
[80]	Message Security Implementation by Using a Combination of Hill Cipher Method and Pixel Value Differencing Method in Mozilla Thunderbird Email Client		**Personal Computing**	Email

its variants [50] or hardware-accelerated AES ([55]), for IoT devices. Both papers utilize multi-level DWT (Discrete Wavelet Transform) for steganography. These differences highlight the range of methodologies employed to safeguard patient data during IoT transmissions.

- Embedding location restrictions

Among the medical papers focused on healthcare data transmissions, two ([41, 88]) discuss methods that impose restrictions on data embedding locations. In [88], the Distance Regularized Level Set Evolution (DRLSE) algorithm [42] is utilized to identify the Region of Interest (ROI) and Non-Region of Interest (NROI) in a medical image. Data is embedded in the NROI using adaptive Pixel Expansion

Table 5 Schemes used and characteristics of journal articles

Ref.	Application domains	Steganographic algorithms	Steganography type	Cryptographic algorithms	Operation order	Advantages
[1]	**Cross-Domain**	Multilevel 2D-DWT with CSO pixel selection	Image (not reversible)	Signcryption	encrypt, hide	Lower MSE, higher PSNR, higher CC, lower CT
[5]		3-LSB	Image (not reversible)	RSA	encrypt, hide	RSA asymmetric, less noise with 3-bits
[7]		LSB-based with bit interchange method, and IPM and; HMF for partitioning and pixel selection	Image (reversible)	Custom asymmetric: key generation with EEC and Bézier curve	hide, encrypt	HAC security, IPM randomization, BIGM for high PSNR
[10]		LSB (PNG), DCT (JPEG)	Image (not reversible)	XOR cipher	encrypt, hide	Not detected by antimalware software, encryption/steganography aids circumvention
[19]		LSB	Image (not reversible)	AES-256	encrypt, hide	Two-factor authentication acceptance, user security preference
[33]		DWPT with XOR	Image (not reversible, encrypted domain)	XOR Cipher	encrypt, hide	Superior NPCR, UACI, SSIM, MSE, PSNR, lower processing time, immunity to channel attacks
[36]		Multilevel 2D-DWT with QBCO pixel selection	Image (not reversible)	Signcryption, ElGamal, Kernel Homomorphic	encrypt, hide	Lower computation time, lower MSEs
[90]		LSB in a bit stream	Network	Linear encryption	encrypt, hide	No communication overhead, statistical undetectability, eavesdropping resistance
[9]	**Medical, Military**	Custom using rhombus pattern prediction	Image (reversible, encrypted domain)	Additive homomorphic encryption	encrypt, hide	Low computational complexity, high PSNR, quality decrypted image, capacity balance
[13]	**Medical**	LSB using dynamic key	Image (reversible, encrypted domain)	XOR Cipher	hide, encrypt	High capacity at maintained quality, immunity to under and overflow

Table 5 (continued)

Ref.	Application domains	Steganographic algorithms	Steganography type	Cryptographic algorithms	Operation order	Advantages
[22]		2D-DWT-1L, 2D-DWT-2L	Image (reversible)	AES-128 (odd bits), RSA (even bits)	encrypt, hide	Higher PSNR, lower MSE, Superior performance indication
[34]		LSB-based with DWT	Signal (not reversible)	XOR Ciphering with ASCII coded shared key. This key is used for encryption and scrambling matrix	encrypt, hide	Undetectable distortion, 100% data extraction
[41]		LSB-Based	Image (reversible)	RSA	encrypt, hide	No embedding key storage, robustness via ROI hash
[44]		3-LSB with DWT	Image (reversible, encrypted domain)	XOR Cipher	encrypt, hide	Higher encryption speed
[56]		LSB	Image (not reversible)	PRNG using Chaotic 2D-Henon Map	hide, encrypt	Two patients' data in one signal, high data hiding capacity
[61]		EPR, ISBS	Image (reversible)	Chaotic encryption	encrypt, hide	Fragile nature, tamper verification, high data hiding
[78]		Custom	Hardware[a]	TRIFID Cipher	N/A	Low-cost design
[86]		LSB	Image (reversible)	Stream cipher with XOR	hide, encrypt	Superior embedding rate, entropy, and MAE
[14]	**Energy, Medical, Finance**	LSB-based	Audio (not reversible)	S-DES	encrypt, hide	Confidentiality, robustness, low information loss, GPU speed enhancement
[48]	**Transportation**	LSB using Fuzzy Edge Detection, normal LSB	Image (not reversible)	Modified RSA	encrypt, hide,	Data integrity maintenance
[75]	**Government**	F5 with DCT and Huffman encoding	Image	PBKDF2 with HMAC-SHA1, SHA1PRNG, (k,n)-threshold Scheme	encrypt, hide	Application in user receipt verification
[87]		Custom: obfuscation matrix in "Obfuscated sensitive data"	Image (not reversible)	CS (Compressed Sensing)	encrypt, hide the stego key, encrypt	No need for a secret channel, robust against cipher attacks
[85]	**Military, Cross-Domain**	Custom	Image (reversible, encrypted domain)	ElGamal with homomorphic encryption and re-encryption	encrypt, hide	Re-encryption, errorless image recovery, specific data extraction order

Table 6 Advantages and limitations in the government domain

Ref.	Evaluation
[75]	+ Verifiability, (k,n) encryption – Collusion, Traffic spoofing, Lost receipts
[87]	+ Multi-level authentication, No extra channel, Robust against attacks – Face recovery dependent on the compression

Embedding (PEE) to achieve higher capacity. For the ROI, a custom algorithm based on histogram-shifting with contrast enhancement is employed to ensure visual clarity. In this paper, data embedding is performed before image encryption. In contrast, [41] also identifies ROI and NROI areas, specifically in DICOM images. However, in this case, the encryption process is conducted before the identification of these areas. Edge detection techniques such as the Gabor Filter and Canny Edge [55] are employed for area identification. Patient data is only embedded in the NROI to preserve image quality. Additionally, to maintain the verifiability of integrity, which is crucial in medical applications, an ROI-generated hash is embedded in the NROI. These approaches demonstrate different strategies for data embedding in specific areas of medical images, highlighting the preservation of image quality, visual clarity, and the importance of integrity verification in healthcare applications.

- Transportation Application Domain

An article focuses on an application in the transportation domain, and its advantages and limitations are listed in Table 8. In [48], a system is proposed to securely deliver diagnostic data to manufacturers and handle firmware updates. Although the system is innovative, there could be potential drawbacks, such as extended decryption times and potential inefficiency when dealing with larger software updates. To address these challenges, future work could investigate the utilization of more efficient cryptographic algorithms and adapt the method to better accommodate larger files, which is common when dealing with updates. Moreover, future research in the transportation domain could explore vehicle-to-vehicle (V2V) networks, where minimizing the speed and size of communication is essential.

4.3 General observations

Several observations can be made regarding all the journal articles. Firstly, the steganography methods commonly employed in the identified applications primarily focus on images, as indicated in Table 9.

Table 7 Advantages and limitations in the medical domain

Ref.	Evaluation
[13]	+ High capacity at same PSNR, Base-16, No under- and overflow – Higher BER
[22]	+ Higher PSNR, Lower MSE – AES key is shared on the channel
[34]	+ Visually undetectable, Complete Extraction
[41]	+ Integrity, ROI intact, Dynamic key – Depends on NROI size
[44]	+ Very low computation time, No extra channel
[56]	+ Improved imperceptibility, Double embedding – Lack of depth
[61]	+ Sensitive to attacks (Integrity), High capacity – File size
[78]	+ Counterfeit detection, Malicious logic prevention, Low-cost Design
[88]	+ Minimal ROI impact, High NROI capacity, Adaptive, Contrast enhancement, No under and overflow

Table 8 Advantages and limitations in the transportation domain

Ref.	Evaluation
[48]	+ Data integrity – Processing time

- There is a noticeable underutilization of other cover mediums such as audio, signal, hardware, video, and text. This gap in research highlights the need for further investigation in these areas. Within the medical domain specifically, 7 out of 9 articles utilize image steganography. The choice of image-based steganography in medical applications is effective, considering the frequent use of medical imaging. However, there is potential for diversifying data types by exploring other forms of steganography, such as video steganography in recorded surgeries or expanding signal steganography beyond ECG signals. This diversification would enhance the usability and robustness of steganography in various systems.
- Secondly, in certain applications ([22, 44]), the encryption key is embedded together with the data in the cover medium. This eliminates the requirement for a separate communication channel (in the case of dynamic keys) or pre-established cryptographic keys.
- Thirdly, it is noteworthy that 42% of the identified articles, spanning various application and technological domains, incorporate a Reversible Data Hiding (RDH) technique. RDH techniques enable the lossless reconstruction of the original cover media after the hidden data has been extracted. This capability is particularly crucial in sectors

Table 9 Journal Articles and their cover medium

Medium	Journal Articles
Image	[1, 5, 7, 9, 10, 13, 19, 22, 33, 36, 41, 44, 48, 56, 61, 75, 85–88]
Audio	[14]
Signal	[34, 90]
Hardware	[78]

such as healthcare, where preserving the integrity of the original data, such as medical imagery, is often of utmost importance [13, 22, 41, 44, 61, 88].

Based on these findings, it is evident that there is a need to **diversify research in terms of methods and cover mediums**. Attention should be given to addressing security challenges in government applications, while a more comprehensive assessment of the performance of chaotic algorithms in medical domains is required. Additionally, there is a call for exploring a wider range of steganography methods for healthcare data transmissions. In the transportation domain, it is advisable to explore other cryptographic algorithms to effectively handle larger data files. Overall, research efforts can significantly enhance data security across various sectors by addressing these areas of improvement.

4.4 RQ3: analyzing evaluation methods used

In this section, we discuss the analysis and evaluation methods utilized in the Journal articles, which are listed in Table 10. The analysis of **steganography** typically revolves around four main concepts: **capacity, robustness, security, and imperceptibility** (sometimes divided into undetectability and invisibility) [4, 68, 82]. On the other hand, **cryptography evaluation** focuses on **security, encryption time, key size, plain vs. cipher size**, and other related factors [26, 83]. Considering the similarities between these concepts, they are grouped into three perspectives: Security, Performance, and User. These perspectives are interconnected and interdependent, as demonstrated in Fig. 5.

4.4.1 Security perspective

Similar to cryptography, steganography can also be vulnerable to different types of attacks, such as ciphertext and plaintext attacks [49]. Steganography is susceptible to similar attack types, including known carrier and known message attacks [49]. The significance of safeguarding against these attacks is contingent upon the order in which steganography and cryptography are applied.

When data is embedded first and then encrypted, the primary defense against attacks lies in the strength of the encryption itself. Several articles, such as [13, 57, 87, 88]

Table 10 Analysis/evaluation methods

Ref	Analysis/evaluation methods
[1, 94]	PSNR, MSE, CC, CT with UCM and AID datasets
[5]	Capacity, PSNR
[7]	X^2, HVS, MSE, PSNR, HA, SSIM, capacity in %
[9]	PSNR, SSIM, BER, bpp, histogram, Entropy, Deviation from Ideality, CC, keyspace analysis, key sensitivity,
[10]	PSNR, StegExpose (PNG), Stegdetect (JPEG)
[13]	PSNR, BER, bpp, CT
[14]	SNR, AD, AE, BPC, TP, Il, UER
[19]	Reliability: CA, CR. Validity: AVE. Behavioural Intention: SEM, Normalised X2, GFI, RMSE, NFI, TLI, CFI
[22]	PSNR, MSE, BER, SSIM, SC, CC
[33]	NCCC, entropy, NPCR, UACI, SSIM, MSE, PSNR, CT
[34]	PRD, WWPRD. Doctors inspected ECGs
[36]	MSE, PSNR, CT, CC
[41]	PSNR, MSE, bpp
[44]	Histogram, Entropy, CC (vertical, horizontal, diagonal), Key sensitivity, encryption speed
[48]	DoIP: Encryption time, embedding time, final image time, stego extract time, cipher extract time. SOTA: Same metrics. Slightly different for the receiver side, but it's all time-based
[56]	PSNR, MSE
[61]	Capacity, PSNR, bpp, SSIM. Salt & pepper noise. Additive White Gaussian Noise. Attacks: median filtering, lowpass filtering, Weiner filtering, sharpening, histogram equalization attack, rotation attack
[75]	Steganography: size, RS analysis, BSM analysis. Usability tested: user acceptance
[78]	Steganography: PSNR, MSE
[85]	PSNR, bpp
[86]	MAE, bpp, pitch removal attacks, bit-plane removal attacks
[87]	PSNR, SSIM
[90]	X^2, KLD

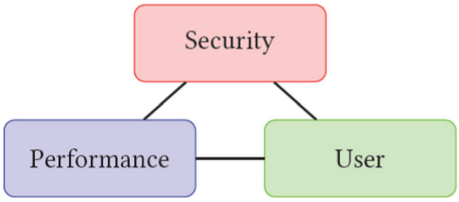


Fig. 5 The three discussed analysis perspectives

(listed in Table 5 in section 3.2), follow this order of operations. Among these articles, some also address advanced attacks, including histogram equalization ([9, 44, 61, 88]), while only one article tackles rotation attacks ([61]). Conversely, when data is encrypted first, the primary defense against attacks lies in the strength or imperceptibility of the stego object. The majority of applications follow this order of operations, as evidenced by articles such as [13, 22, 34, 41, 44, 48, 61, 75], among others. These implementations primarily focus on achieving steganographic imperceptibility, utilizing metrics such as PSNR, SSIM, MSE, and BER. They heavily rely on cryptographic evaluations from previous works. Even articles proposing custom or more complex encryption methods ([34, 44, 48, 56, 61, 88]) still analyze cryptographic security as an integral part of their evaluation.

The following insights are drawn based on the security perspective:

- *Vulnerability to attacks* Similar to cryptography, steganography is prone to various attacks, including ciphertext and plaintext attacks. This underscores the necessity of implementing robust defenses to safeguard against potential security breaches.
- *Order of operations* The sequence in which steganography and cryptography are applied influences the defense mechanisms against attacks. Whether data is embedded first and then encrypted, or vice versa, dictates where the primary defense lies, either in the strength of encryption or the imperceptibility of the stego object.
- *Advanced attack consideration* Some articles address advanced attacks, such as histogram equalization and rotation attacks, highlighting the importance of considering sophisticated attack vectors that may compromise the invisibility of stego objects.
- *Emphasis on imperceptibility* The majority of implementations prioritize achieving steganographic imperceptibility by encrypting data first. This emphasizes the importance of concealing hidden data within digital media while maintaining the appearance and quality of the original content.
- *Integration of cryptographic security* Even articles proposing custom encryption methods analyze cryptographic security comprehensively. This integration underscores the interdependence between cryptographic measures and steganographic techniques in ensuring the overall security of hidden information.

4.4.2 Performance perspective

The performance of encountered systems can be influenced by several factors, including computation time (CT), capacity (related to steganography), and key size (related to cryptography).

Computation time, which encompasses both steganography and cryptography, is particularly important as it correlates with power consumption, making it a crucial consideration in real-time and power-sensitive systems. While some articles like [1, 13, 33, 36, 44, 48] incorporate CT measurements, only two similar applications [1, 36] specifically address the need for managing power consumption in their environments. CT measurements are often discussed as "total time" or analyzed individually for different components of the system, such as embedding time, extraction time, encryption time, and more. This approach allows for more targeted performance improvements. Interestingly, among the seven articles exploring applications in the Internet of Things (IoT), three articles [7, 22, 34] do not utilize time-based analysis metrics. This omission makes it challenging to accurately assess the performance and efficiency of their proposed applications. A time-based analysis is vital for a comprehensive understanding of application performance as it not only reveals the speed of processes but also provides insights into the efficient utilization of system resources.

Another **significant metric to consider is capacity**. The balance between imperceptibility and capacity holds importance depending on the specific application. In certain (real-time) applications where relatively small data fragments are shared, the capacity of the cover medium may not be as critical. In such cases, imperceptibility may also be of lesser relevance. Out of the 24 articles analyzed, capacity is evaluated in 9 articles [5, 7, 9, 13, 41, 61, 75, 85, 86], either in comparison to other implementations or by examining different parameters within the same implementation. It is worth noting that only one article ([7]) focusing on IoT applications specifically analyzed the capacity of the employed steganographic method. The **key size** in cryptographic algorithms can have a significant impact on encryption time, as explained in [40]. In the context of IoT, [22] specifically addresses cryptographic operations using an AES key size of 128 bits. Although AES-128 is generally regarded as secure, larger key sizes can be employed. The utilization of more efficient encryption algorithms could potentially allow for the use of larger keys while maintaining similar encryption times. Surprisingly, the discussion or justification of key sizes for well-known cryptographic algorithms does not appear to be frequently addressed in the analyzed literature.

Upon examining various research papers listed in Table 10, the following insights regarding performance are observed:

- The analysis revealed key considerations related to computation time, capacity, and key size.
- Computation time was emphasized as critical due to its association with power consumption, especially in real-time and power-sensitive systems.
- Capacity, concerning the balance between imperceptibility and capacity in steganography, was noted to vary depending on specific application requirements.
- The analysis underscored the significant impact of key size selection in cryptographic algorithms on encryption time, highlighting the importance of careful consideration in algorithm design.
- Despite the importance of these factors, the analysis revealed areas where certain metrics, such as time-based analysis in IoT applications, were lacking, making it challenging to comprehensively assess performance and efficiency.

4.4.3 User perspective

The user perspective evaluates how effectively a system incorporating steganography and cryptography aligns with the user's workflow, emphasizing factors such as ease of use, comprehension, trust, processing time, and system stability. The impact of the system on the user's workflow is particularly crucial for applications where the user directly interacts with the system. However, even in cases where the system operates in the background, it can still potentially influence the user's experience, albeit to a slightly lesser degree. From the reviewed literature, it is observed that only a limited number of studies include **usability tests** to analyze user experience. For instance, the implementation of an e-voting system discussed in [75] incorporates **usability and user acceptance testing** using Nielsen's quality components [58] and Davis' Technology Acceptance Model (TAM) [20], respectively. These well-established methods assess the usability and acceptance of the system. Similarly, the NFC access control scheme presented in [19] includes usability, perceived vulnerability, perceived security, and behavioral intention tests to examine how the proposed security scheme could influence user behavior. The methods utilized in this study were adapted from previous works [15, 35, 76].

Applications such as remote patient monitoring ([34]) aim to provide a user-friendly experience, requiring minimal complex setup from the user's perspective. It is mentioned that any **additional complexity** introduced by the implementation of steganography or cryptography should ideally be abstracted away from the user. However, the only user interaction highlighted in the article is related to the imperceptibility of the Human Visual System (HVS), where doctors inspect ECGs. Similarly, the application of hiding files in audio files on PCs [5] is closely related to end-users, but the article does not delve further into this aspect and omits user testing in this regard. This omission creates an evaluation gap, as it fails to comprehend the actual user experience and potential areas for improvement. **User experience** can be significantly influenced by other perspectives, such as security and performance. If the combination of steganography and cryptography leads to excessively **slow data processing** or if the system **lacks robustness against attacks** like compression or cropping, it could compromise the user's ability to effectively manage stego objects (e.g., share or post-process them). This vulnerability could potentially result in data loss or corruption, ultimately degrading the overall user experience. Therefore, robust implementations of steganography and cryptography are essential for maintaining a high-quality user experience.

After analyzing the User perspective criteria, we identify the following insights:

- Despite the importance of user experience, there's a noted lack of usability tests in the reviewed literature, with only a few studies incorporating established methods like Nielsen's quality components and Davis' Technology Acceptance Model (TAM).
- Applications aim to provide a user-friendly experience, with additional complexity introduced by steganography or cryptography ideally abstracted away from the user to ensure ease of use.
- User experience can be significantly impacted by factors like security and performance, with slow data processing or lack of robustness against attacks compromising the effective management of stego objects and degrading overall user experience.
- Robust implementations of steganography and cryptography are crucial for maintaining a high-quality user experience, highlighting the importance of considering user-centric factors in system design and evaluation.

4.5 General observations

In summary, the evaluation of steganography and cryptography requires a comprehensive analysis that encompasses security, performance, and user perspectives. Unfortunately, several studies overlook certain metrics, creating gaps in our understanding of computation time, capacity, key size, and user-friendliness. It is crucial to strike a balance between steganography and cryptography to ensure an optimal user experience, robust security, and efficient performance. Future

research should aim to address these oversights and strive for a more comprehensive evaluation framework.

5 Conclusion and future scope

This review examines the state of combined steganography and cryptography applications in journal articles and conference papers, categorized by application and technological domains. While medical applications dominate, IoT and Cloud Computing domains show active research. Real-time constraints and privacy protection are prominent concerns in technological domains. The combined approach provides data security and privacy benefits, but trade-offs and limitations remain. Further research is needed to address these challenges and improve methodologies. The evaluation metrics vary, emphasizing domain-specific knowledge. A comprehensive framework is proposed, incorporating security, performance, and user perspectives. However, there is a notable lack of user testing in the literature, highlighting the need for user-centric system design. This review focused solely on conference papers for RQ1 due to time constraints. Conference papers are valuable sources of the latest findings and innovative practices in the rapidly evolving field of information security, making them relevant not just for RQ1 but also for RQ2 and RQ3. Additionally, the search keywords were limited to "cryptography" and "steganography," but other terms like "encryption" or "data-hiding" may be used. Future research could explore applications in diverse domains such as transportation and energy. Comparative studies could shed light on the advantages of using steganography or cryptography individually in different scenarios. Further investigations into non-image steganographic mediums and the impact of combining steganography and cryptography on end-user experience and acceptance are also warranted.

Author contributions Indy Haverkamp: Conceptualization, Methodology, Validation, Investigation, Formal Analysis, Data Curation, Writing—Original Draft, Visualization, Dipti Kapoor Sarmah: Methodology, Writing—Review & Editing, Visualization, Supervision, Project administration.

Data availability The datasets generated during and/or analyzed during the current study are available from the corresponding author upon reasonable request.

Declarations

Conflict of interest The authors have no competing interests to declare that are relevant to the content of this article.

Human and Animals Participants No

Informed consent All authors agreed with the content and all gave explicit consent to submit.

References

1. Alissa, K.A., Maray, M., Malibari, A.A., Alazwari, S., Alqahtani, H., Nour, M.K., Al Duhayyim, M.: Optimal deep learning model enabled secure UAV classification for industry. Comput. Mater. Contin. **74**(3), 5349–5367 (2023)
2. Abbas, M.S., Mahdi, S.S., Hussien, S.A.: Security improvement of cloud data using hybrid cryptography and steganography. In: 2020 International Conference on Computer Science and Software Engineering (CSASE), pp. 123–127. IEEE (2020)
3. Al Abbas, A.A.M., Ibraheem, N.B.: Using DNA In Adynamic Lightweight Algorithm For Stream Cipher In An IoT Application. In: 2022 International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), pp. 232–240. IEEE (2022)
4. Al-Ani, Z.K., Zaidan, A.A., Zaidan, B.B., Alanazi, H.: Overview: main fundamentals for steganography. arXiv preprint arXiv:1003.4086. (2010)
5. Al-Juaid, N., Gutub, A.: Combining RSA and audio steganography on personal computers for enhancing security. SN Appl. Sci. **1**, 1–11 (2019)
6. Ali, M.H., Al-Alak, S.: Node protection using hiding identity for IPv6 based network. In: 2022 Muthanna International Conference on Engineering Science and Technology (MICEST), pp. 111–117. IEEE (2022)
7. Alsamaraee, S., Ali, A.S.: A crypto-steganography scheme for IoT applications based on bit interchange and crypto-system. Bull. Electr. Eng. Inf. **11**(6), 3539–3550 (2022)
8. Anderson, R.J., Petitcolas, F.A.: On the limits of steganography. IEEE J. Sel. Areas Commun. **16**(4), 474–481 (1998)
9. Anushiadevi, R., Amirtharajan, R.: Design and development of reversible data hiding-homomorphic encryption & rhombus pattern prediction approach. Multimed. Tools Appl. **82**(30), 46269–46292 (2023)
10. Badhani, S., Muttoo, S.K.: Evading android anti-malware by hiding malicious applications inside images. Int. J. Syst. Assur. Eng. Manag. **9**, 482–493 (2018)
11. Banga, P.S., Portillo-Dominguez, A.O., Ayala-Rivera, V.: Protecting user credentials against SQL injection through cryptography and image steganography. In: 2022 10th International Conference in Software Engineering Research and Innovation (CONISOFT), pp. 121–130. IEEE (2022)
12. Bharathi, P., Annam, G., Kandi, J.B., Duggana, V.K., Anjali, T.: Secure file storage using hybrid cryptography. In: 2021 6th International Conference on Communication and Electronics Systems (ICCES), pp. 1–6. IEEE (2021)
13. Bhardwaj, R.: An improved reversible data hiding method in encrypted domain for E-healthcare. Multimed. Tools Appl. **82**(11), 16151–16171 (2023)

14. Bhattacharjee, S., Rahim, L.B.A., Watada, J., Roy, A.: Unified GPU technique to boost confidentiality, integrity and trim data loss in big data transmission. IEEE Access **8**, 45477–45495 (2020)
15. Bhuiyan, M., Picking, R.: A gesture controlled user interface for inclusive design and evaluative study of its usability. J. Softw. Eng. Appl. **4**(09), 513 (2011)
16. Bokhari, M.U., Shallal, Q.M.: A review on symmetric key encryption techniques in cryptography. Int. J. Comput. Appl. **147**(10), 43 (2016)
17. Castillo, R.E., Cayabyab, G.T., Castro, P.J.M., Aton, M.R.: Blocksight: a mobile image encryption using advanced encryption standard and least significant bit algorithm. In: Proceedings of the 1st International Conference on Information Science and Systems, pp. 117–121 (2018)
18. Caviglione, L., Podolski, M., Mazurczyk, W., Ianigro, M.: Covert channels in personal cloud storage services: the case of dropbox. IEEE Trans. Ind. Inf. **13**(4), 1921–1931 (2016)
19. Cheong, S.N., Ling, H.C., Teh, P.L.: Secure encrypted steganography graphical password scheme for near field communication smartphone access control system. Expert Syst. Appl. **41**(7), 3561–3568 (2014)
20. Davis, F.D.: Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Q. **13**, 319–340 (1989)
21. Dhawan, S., Chakraborty, C., Frnda, J., Gupta, R., Rana, A.K., Pani, S.K.: SSII: secured and high-quality steganography using intelligent hybrid optimization algorithms for IoT. IEEE Access **9**, 87563–87578 (2021)
22. Elhoseny, M., Ramírez-González, G., Abu-Elnasr, O.M., Shawkat, S.A., Arunkumar, N., Farouk, A.: Secure medical data transmission model for IoT-based healthcare systems. IEEE Access **6**, 20596–20608 (2018)
23. Gamal, S.M., Youssef, S.M., Abdel-Hamid, A.: Secure transmission and repository platform for electronic medical images: case study of retinal fundus in teleophthalmology. In: 2020 International Conference on Computing, Electronics & Communications Engineering (iCCECE), pp. 9–14. IEEE (2020)
24. Ghuge, S.S., Kumar, N., Savitha, S., & Suraj, V.: Multilayer technique to secure data transfer in private cloud for saas applications. In: 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), pp. 646–651. IEEE (2020)
25. Gupta, S., Goyal, A., Bhushan, B.: Information hiding using least significant bit steganography and cryptography. Int. J. Modern Educ. Comput. Sci. **4**(6), 27 (2012)
26. Gururaja, H.S., Seetha, M., Koundinya, A.K.: Design and performance analysis of secure elliptic curve cryptosystem. Int. J. Adv. Res. Comput. Commun. Eng. **2**(8), 1 (2013)
27. Haque, M.E., Zobaed, S.M., Islam, M.U., Areef, F.M.: Performance analysis of cryptographic algorithms for selecting better utilization on resource constraint devices. In: 2018 21st International Conference of Computer and Information Technology (ICCIT), pp. 1–6. IEEE (2018)
28. Sri, P.H., Chary, K.N.: Secure file storage using hybrid cryptography. Int. Res. J. Mod. Eng. Technol. Sci. (2022). https://doi.org/10.56726/IRJMETS32383
29. Hashim, M.M., Rhaif, S.H., Abdulrazzaq, A.A., Ali, A.H., Taha, M.S.: Based on IoT healthcare application for medical data authentication: Towards a new secure framework using steganography. In: IOP Conference Series: Materials Science and Engineering, vol. 881, no. 1, p. 012120. IOP Publishing (2020)
30. Heron, S.: Advanced encryption standard (AES). Netw. Secur. **2009**(12), 8–12 (2009)
31. Hussain, M., Wahab, A.W.A., Batool, I., Arif, M.: Secure password transmission for web applications over internet using cryptography and image steganography. Int. J. Secur. Appl. **9**(2), 179–188 (2015)
32. Hussein, A.A., Jumah Al-Thahab, O.Q.: Design and simulation a video steganography system by using FFTturbo code methods for copyrights application. Eastern-Euro. J. Enterp. Technol. **2**(9), 104 (2020)
33. Hussein, S.A., Saleh, A.I., Mostafa, H.E.D.: A new fog based security strategy (FBS 2) for reliable image transmission. J. Ambient Intell. Humaniz. Comput. **11**, 3265–3303 (2020)
34. Ibaida, A., Khalil, I.: Wavelet-based ECG steganography for protecting patient confidential information in point-of-care systems. IEEE Trans. Biomed. Eng. **60**(12), 3322–3330 (2013)
35. Ifinedo, P.: Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. Comput. Secur. **31**(1), 83–95 (2012)
36. Jain, D.K., Li, Y., Er, M.J., Xin, Q., Gupta, D., Shankar, K.: Enabling unmanned aerial vehicle borne secure communication with classification framework for industry 5.0. IEEE Trans. Ind. Inf. **18**(8), 5477–5484 (2021)
37. Jankowski, B., Mazurczyk, W., Szczypiorski, K.: PadSteg: introducing inter-protocol steganography. Telecommun. Syst. **52**, 1101–1111 (2013)
38. Kavitha, V., Sruthi, G.S., Thoshinny, B., Riduvarshini, S.R.: Stagchain–a steganography based application working on a blockchain environment. In: 2022 3rd International Conference on Electronics and Sustainable Communication Systems (ICESC), pp. 674–681. IEEE (2022)
39. Khan, H.A., Abdulla, R., Selvaperumal, S.K., Bathich, A.: IoT based on secure personal healthcare using RFID technology and steganography. Int. J. Electr. Comput. Eng. **11**(4), 3300 (2021)
40. Kumar, M.G.V., Ragupathy, U.S.: A survey on current key issues and status in cryptography. In: 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), pp. 205–210. IEEE (2016)
41. Kumar, N., Kalpana, V.: A novel reversible steganography method using dynamic key generation for medical images. Indian J. Sci. Technol. **8**(16), 1 (2015)
42. Li, C., Xu, C., Gui, C., Fox, M.D.: Distance regularized level set evolution and its application to image segmentation. IEEE Trans. Image Process. **19**(12), 3243–3254 (2010)
43. Madavi, K.B., Karthick, P.V.: Enhanced cloud security using cryptography and steganography techniques. In: 2021 International Conference on Disruptive Technologies for Multi-Disciplinary Research and Applications (CENTCON), vol. 1, pp. 90–95. IEEE (2021)
44. Mancy, L., Vigila, S.M.C.: A new diffusion and substitution-based cryptosystem for securing medical image applications. Int. J. Electron. Secur. Digit. Forens. **10**(4), 388–400 (2018)
45. Mandal, P.C., Mukherjee, I., Paul, G., Chatterji, B.N.: Digital image steganography: a literature survey. Inf. Sci. **609**, 1451–1488 (2022)
46. Mandal, S., Khan, D.A.: Enhanced-longest common subsequence based novel steganography approach for cloud storage. Multimed. Tools Appl. **82**(5), 7779–7801 (2023)
47. Manikandan, V.M., Masilamani, V.: Reversible data hiding scheme during encryption using machine learning. Proc. Comput. Sci. **133**, 348–356 (2018)
48. Mayilsamy, K., Ramachandran, N., Raj, V.S.: An integrated approach for data security in vehicle diagnostics over internet protocol and software update over the air. Comput. Electr. Eng. **71**, 578–593 (2018)
49. Mishra, R., Bhanodiya, P.: A review on steganography and cryptography. In: 2015 International Conference on Advances in Computer Engineering and Applications, pp. 119–122. IEEE (2015)
50. Mishra, Z., Acharya, B.: High throughput novel architectures of TEA family for high speed IoT and RFID applications. J. Inf. Secur. Appl. **61**, 102906 (2021)
51. Mogale, H., Esiefarienrhe, M., Letlonkane, L. Web authentication security using image steganography and AES encryption. In: 2018

International Conference on Intelligent and Innovative Computing Applications (ICONIC), pp. 1–7. IEEE (2018)
52. More, S.S., Mudrale, A., Raut, S.: Secure transaction system using collective approach of steganography and visual cryptography. In: 2018 International Conference on Smart City and Emerging Technology (ICSCET), pp. 1–6. IEEE (2018)
53. Mostaghim, M., Boostani, R.: CVC: chaotic visual cryptography to enhance steganography. In: 2014 11th International ISC Conference on Information Security and Cryptology, pp. 44–48. IEEE (2014)
54. Munoz, P.S., Tran, N., Craig, B., Dezfouli, B., Liu, Y.: Analyzing the resource utilization of AES encryption on IoT devices. In: 2018 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC), pp. 1200–1207. IEEE (2018)
55. Nadernejad, E., Sharifzadeh, S., Hassanpour, H.: Edge detection techniques: evaluations and comparisons. Appl. Math. Sci. **2**(31), 1507–1520 (2008)
56. Bremnavas, I., Mohamed, I.R., Shenbagavadivu, N.: Secured medical image transmission through the two dimensional chaotic system. Int. J. Appl. Eng. Res. **10**(17), 38391–38396 (2015)
57. Neetha, S.S., Bhuvana, J., Suchithra, R.: An efficient image encryption reversible data hiding technique to improve payload and high security in cloud platforms. In: 2023 6th International Conference on Information Systems and Computer Networks (ISCON), pp. 1–6. IEEE (2023)
58. Nielsen, J., Molich, R.: Heuristic evaluation of user interfaces. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 249–256 (1990)
59. Nissar, A., Mir, A.H.: Classification of steganalysis techniques: a study. Digit. Signal Process. **20**(6), 1758–1770 (2010)
60. Pande, A., Zambreno, J.: A chaotic encryption scheme for real-time embedded systems: design and implementation. Telecommun. Syst. **52**, 551–561 (2013)
61. Parah, S.A., Ahad, F., Sheikh, J.A., Bhat, G.M.: Hiding clinical information in medical images: a new high capacity and reversible data hiding technique. J. Biomed. Inform. **66**, 214–230 (2017)
62. Patil, N., Kondabala, R.: Two-layer secure mechanism for electronic transactions. In: 2022 International Conference on Recent Trends in Microelectronics, Automation, Computing and Communications Systems (ICMACC), pp. 174–181. IEEE (2022)
63. Perwej, Y., Haq, K., Parwej, F., Mumdouh, M., Hassan, M.: The internet of things (IoT) and its application domains. Int. J. Comput. Appl. **975**(8887), 182 (2019)
64. Chen, C.P., Zhang, C.Y.: Data-intensive applications, challenges, techniques and technologies: a survey on big data. Inf. Sci. **275**, 314–347 (2014)
65. Phipps, A., Ouazzane, K., Vassilev, V.: Enhancing cyber security using audio techniques: a public key infrastructure for sound. In: 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 1428–1436. IEEE (2020)
66. Pokharana, A., Sharma, S.: Encryption, file splitting and file compression techniques for data security in virtualized environment. In: 2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA), pp. 480–485. IEEE (2021)
67. Prabu, S., Ganapathy, G.: Steganographic approach to enhance the data security in public cloud. Int. J. Comput. Aided Eng. Technol. **13**(3), 388–408 (2020)
68. Pradhan, A., Sahu, A.K., Swain, G., Sekhar, K.R.: Performance evaluation parameters of image steganography techniques. In: 2016 International Conference on Research Advances in Integrated Navigation Systems (RAINS), pp. 1–8. IEEE (2016)
69. Kumar, P., Sharma, V.K.: Information security based on steganography & cryptography techniques: a review. Int. J. **4**(10), 246–250 (2014)
70. Preethi, P., Prakash, G.: Secure fusion of crypto-stegano based scheme for satellite image application. In: 2021 Asian Conference on Innovation in Technology (ASIANCON), pp. 1–6. IEEE (2021)
71. Ramamoorthy, U., Loganathan, A.: Analysis of video steganography in military applications on cloud. Int. Arab J. Inf. Technol. **19**(6), 897–903 (2022)
72. Angel, N.A., Ravindran, D., Vincent, P.D.R., Srinivasan, K., Hu, Y.C.: Recent advances in evolving computing paradigms: cloud, edge, and fog technologies. Sensors **22**(1), 196 (2021)
73. Reshma, V., Gladwin, S.J., Thiruvenkatesan, C.: Pairing-free CP-ABE based cryptography combined with steganography for multimedia applications. In: 2019 International Conference on Communication and Signal Processing (ICCSP), pp. 0501–0505. IEEE (2019)
74. Rout, H., Mishra, B.K.: Pros and cons of cryptography, steganography and perturbation techniques. IOSR J. Electron. Commun. Eng. **76**, 81 (2014)
75. Issac, B., Rura, L., Haldar, M.K.: Implementation and evaluation of steganography based online voting system. Int. J. Electr. Gov. Res. **12**(3), 71–93 (2016)
76. Ryu, Y.S., Koh, D.H., Ryu, D., Um, D.: Usability evaluation of touchless mouse based on infrared proximity sensing. J. Usability Stud. **7**(1), 31–39 (2011)
77. Saleh, M.E., Aly, A.A., Omara, F.A.: Data security using cryptography and steganography techniques. Int. J. Adv. Comput. Sci. Appl. **7**(6), 390 (2016)
78. Sengupta, A., Rathor, M.: Structural obfuscation and crypto-steganography-based secured JPEG compression hardware for medical imaging systems. IEEE Access **8**, 6543–6565 (2020)
79. Shaji, A., Stephen, M., Sadanandan, S., Sreelakshmi, S., Fasila, K.A.: Phishing site detection and blacklisting using EVCS, steganography based on android application. In: International Conference on Intelligent Data Communication Technologies and Internet of Things (ICICI) 2018, pp. 1384–1390. Springer International Publishing (2019)
80. Siregar, B., Gunawan, H., Budiman, M.A.: Message security implementation by using a combination of hill cipher method and pixel value differencing method in mozilla thunderbird email client. In: Journal of Physics: Conference Series, vol. 1255, no. 1, p. 012034. IOP Publishing (2019)
81. Stanescu, D., Stratulat, M., Ciubotaru, B., Chiciudean, D., Cioarga, R., Micea, M.: Embedding data in video stream using steganography. In: 2007 4th International Symposium on Applied Computational Intelligence and Informatics, pp. 241–244. IEEE (2007)
82. Subhedar, M.S., Mankar, V.H.: Current status and key issues in image steganography: a survey. Comput. Sci. Rev. **13**, 95–113 (2014)
83. Wang, X., Zhang, J., Schooler, E.M., Ion, M.: Performance evaluation of attribute-based encryption: toward data privacy in the IoT. In: 2014 IEEE International Conference on Communications (ICC), pp. 725–730. IEEE (2014)
84. Wu, J., Liao, X., Yang, B.: Image encryption using 2D Hénon-Sine map and DNA approach. Signal Process. **153**, 11–23 (2018)
85. Xiong, L., Shi, Y.: On the privacy-preserving outsourcing scheme of reversible data hiding over encrypted image data in cloud computing. Comput. Mater. Contin. **55**(3), 523 (2018)
86. Xu, S., Horng, J.H., Chang, C.C., Chang, C.C.: Reversible data hiding with hierarchical block variable length coding for cloud security. IEEE Trans. Dependable Secure Comput. (2022). https://doi.org/10.1109/TDSC.2022.3219843
87. Yang, Y., Xiao, X., Cai, X., Zhang, W.: A secure and high visual-quality framework for medical images by contrast-enhancement reversible data hiding and homomorphic encryption. IEEE Access **7**, 96900–96911 (2019)

88. Zhang, L., Hu, X., Rasheed, W., Huang, T., Zhao, C.: An enhanced steganographic code and its application in voice-over-IP steganography. IEEE Access **7**, 97187–97195 (2019)
89. Zhang, X.G., Yang, G.H., Ren, X.X.: Network steganography based security framework for cyber-physical systems. Inf. Sci. **609**, 963–983 (2022)
90. Zhou, X., Tang, X.: Research and implementation of RSA algorithm for encryption and decryption. In: Proceedings of 2011 6th International Forum on Strategic Technology, vol. 2, pp. 1118–1121. IEEE (2011)
91. Sarmah, D.K., Kulkarni, A.J.: JPEG based steganography methods using cohort intelligence with cognitive computing and modified multi random start local search optimization algorithms. Inf. Sci. **430**, 378–396 (2018)
92. Yang, Y., Newsam, S.: Bag-of-visual-words and spatial extensions for land-use classification. In: Proceedings of the 18th SIGSPATIAL International Conference on Advances in Geographic Information Systems, pp. 270–279 (2010)
93. AID: A scene classification dataset, https://www.kaggle.com/datasets/jiayuanchengala/aid-scene-classification-datasets. Accessed 29 Feb 2024
94. Elshoush, H.T., Mahmoud, M.M.: Ameliorating LSB using piecewise linear chaotic map and one-time pad for superlative capacity, imperceptibility and secure audio steganography. IEEE Access **11**, 33354–33380 (2023)
95. Michaylov, K.D., Sarmah, D.K.: Steganography and steganalysis for digital image enhanced forensic analysis and recommendations. J. Cyber Secur. Technol. (2024). https://doi.org/10.1080/23742917.2024.2304441
96. Sarmah, D.K., Kulkarni, A.J.: Improved cohort intelligence—a high capacity, swift and secure approach on JPEG image steganography. J. Inf. Secur. Appl. **45**, 90–106 (2019)
97. Singh, O.P., Singh, A.K., Agrawal, A.K., Zhou, H.: SecDH: security of COVID-19 images based on data hiding with PCA. Comput. Commun. **191**, 368–377 (2022)
98. Singh, K.N., Baranwal, N., Singh, O.P., Singh, A.K.: SIELNet: 3D chaotic-map-based secure image encryption using customized residual dense spatial network. IEEE Trans. Consumer Electron. (2022). https://doi.org/10.1109/TCE.2022.3227401
99. Mahto, D.K., Singh, A.K., Singh, K.N., Singh, O.P., Agrawal, A.K.: Robust copyright protection technique with high-embedding capacity for color images. ACM Trans. Multimed. Comput. Commun. Appl. (2023). https://doi.org/10.1145/3580502