Analyzing Advantages and Limitations of Combining Cryptography and Steganography Across Applications: A Systematic Review

INDY HAVERKAMP, University of Twente, The Netherlands

In the era of growing interconnectivity, ensuring the confidentiality and security of digital data is crucial. Cryptography and steganography are two primary methods for information security. Cryptography protects the contents of messages, while steganography hides the existence. Although both methods are used in different applications, the potential benefits of combining them is being explored. However, the feasibility of combining these techniques depends on various factors, such as bandwidth limits, latency constraints, and the specific security requirements in a given situation, like electronic voting. This review explores journal articles and conference papers implementing the combination of steganography and cryptography in real-world applications. Research so far is mostly limited to medical applications. Similarly, image steganography is widely used across various domains. This review is novel in several ways: 1) gaining insight into real-world applications being explored by existing literature. 2) split categorization of these applications into application domain (such as Medical or Transportation) and technological domain (such as Cloud Computing or Internet of Things). This review also investigates advantages and limitations of these implementations, and discusses three evaluation perspectives (security, performance, and user). Split categorization can guide research into new areas, while the three perspectives provide important aspects to consider when analyzing or evaluating real-world implementations.

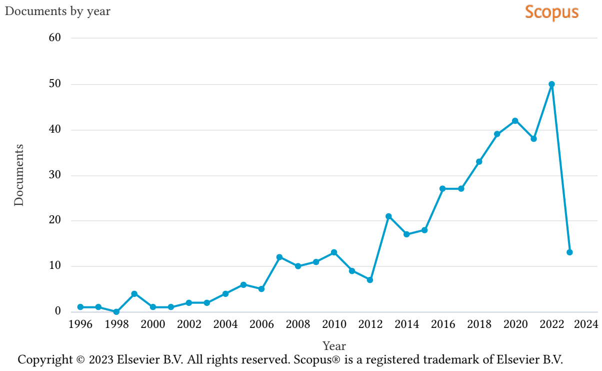
Additional Key Words and Phrases: Steganography, Cryptography, Information Security, Real-world Applications, Application Domains, Evaluation Perspectives

1 INTRODUCTION

An ever-increasing portion of our daily lives is connected to the digital world: we communicate via messaging, store data in the cloud, create payment transactions, and much more. All this data should be handled and stored securely and confidentially. To do this, cryptography and steganography [75, 78], two crucial fields in information security, can be used to make a message unreadable for an eavesdropper and make a message undetectable respectively.

Both fields serve the purpose of ensuring the confidentiality of data [70], but in different ways: while cryptography protects the *contents* of a message using a key, steganography is about *hiding* the message's very existence in a 'cover' medium [75]. Although cryptography is widely used in daily applications, both have their share of applications and could be combined in use. It is important to note that while both techniques greatly reduce the risk of attacks, they are not foolproof [16, 60].

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, 40], military [72], cloud storage [2, 18, 47, 68], and more [28, 31, 32, 38, 90].



Copyright © 2023 Elsevier B.V. All rights reserved. Scopus® is a registered trademark of Elsevier B.V.

Fig. 1. Graph of published journal articles and conference papers on Scopus[1], from 1996 to June 2023.

The growth of interest in steganography was sparked in two ways: the multimedia industry could greatly benefit from possible watermarking techniques, and restrictions on cryptographic schemes by governments triggered interest in alternative ways for communication to stay secretive [8].

Fig. 1 depicts an exponential increase in publications on the applications of combining steganography and cryptography on Scopus[1]. This shows a growing interest in combining or comparing these two disciplines.

Though multiple security mechanisms might seem advantageous, combining cryptography with steganography may not always be suitable. The possibility of combining these two disciplines may be affected by factors such as bandwidth [37, 82] and latency [90]. For instance, the data size can increase due to the additional layers of security, which could exceed available bandwidth, resulting in slower transmission speeds. Interestingly, the computational complexity of a combined approach does not always increase. As an example, [25] implements steganography with Diffie-Hellman encryption. In this case, the time complexity with the addition of encryption was the same as steganography on its own. Yet, using RSA instead, resulted in a higher time complexity [25]. As such, the choice between the two techniques heavily depends on the specific security needs of the situation at hand and the types of cryptography and steganography used.

From here on, "a combined approach" refers to the combined use of steganography and cryptography. Furthermore, 'method' and 'scheme' interchangeably refer to a paper's combined implementation.

TScIT 39, July 7, 2023, Enschede, The Netherlands

© 2023 University of Twente, Faculty of Electrical Engineering, Mathematics and Computer Science.
Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

[1] https://www.scopus.com/ - with query: ("cryptography" AND "steganography") AND ("application" OR "real-world") AND ("security" OR "cyberattack" OR "cybersecurity")

1.1 Problem Statement

With the increase of systems that require protection from cyberattacks, applications where steganography and cryptography can be combined become more interesting. However, to identify possible areas of improvement or future research, understanding the current status of research is crucial.

The novelty of this systematic literature review is the aim to identify and analyze papers that discuss the combined application of cryptography and steganography in various domains and contexts, to identify the advantages, limitations, and trade-offs discussed in the literature, and provide insight into how the performance of these combined implementations can be analyzed. The findings of this review provide valuable insights into the current state of research and contribute to advancements in securing systems against cyber threats. This leads us to the following research questions.

1.2 Research Questions

The main research question is formulated as follows: *What are the advantages and limitations of using a combined steganography and cryptography approach in various real-world applications to enhance security against cyberattacks on a system?* There are three important sub-questions that need to be answered:

(1) What are the various real-world applications where combined steganography and cryptography approaches can be used?
(2) What are the advantages, limitations, and trade-offs of using a combined approach in these applications?
(3) How are implementations of a combined approach evaluated across different real-world applications?

2 METHODOLOGY

To identify relevant literature for this systematic review, a reproducible search strategy was used. The databases that were searched are Scopus[2], the IEEE Digital Library[3], and ISI Web of Science[4]. To streamline the process of reviewing, screening and extracting literature the Parsifal tool[5] was used.

2.1 Data Gathering

The first step of exploring literature is data gathering. Two literature searches were performed, one covering **journal articles** and an additional smaller covering **conference papers**. The results of this additional literature search only provide more insight into the current state of research for RQ1. To explore the aforementioned databases, important keywords and criteria were determined. While both literature searches share the same keywords, their criteria (e.g. year, language) differ slightly to maintain a manageable scope. First, from the research questions in section 1.2 important keywords were derived. Via an iterative process of tuning keywords and exploring the amount of literature on Scopus, the final keywords can be expressed as the following query:

```
("cryptography" AND "steganography")
AND ("application" OR "real-world")
AND ("security" OR "cyberattack" OR "cybersecurity")
```

Based on keywords alone, the three databases returned in total **749 results** (*May 24th, 2023*). Next, inclusion criteria year, language, and type were applied using the filter functionality of these databases. These are described in the following two sections.

2.1.1 *Literature Search 1: Journal Articles.*

An extensive literature search is performed on journal articles. The databases were last accessed on *May 24th, 2023* for this search. The criteria for this search are as follows:

- Only literature from **2010 onwards** is included.
- The literature must be a **journal article**. Review papers, conference papers, books, and other sources are excluded.
- Publications may be from any region, but must be in **English**.

Literature from any country or region is considered. The title, abstract, and keywords were searched. These criteria result in the following additional query options:

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

These search criteria, along with the keywords from section 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.

2.1.2 *Literature Search 2: Conference Papers.*

Additionally, a smaller literature search on conference papers is performed. The databases were last accessed on *June 23rd, 2023* for this search. Search criteria and query differ slightly from the previous literature search in the previous section in the ways shown below.

- Only literature from **2018 onwards** is included.
- The literature must be a **conference paper** from **conference proceedings**. Review papers, journal articles, books, and other sources are excluded.
- Publications may again be from any region and must be in **English**.

Which results in 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 section 2.1, resulted in the 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.

[2] https://www.scopus.com/
[3] https://ieeexplore.ieee.org/
[4] https://www.webofscience.com/
[5] https://parsif.al/

2.2 Study Selection

The second step of exploring literature is the selection of relevant studies, which is done in two phases. Below, a list of seven conditions can be seen. These conditions were determined such that only literature addressing the research questions (section 1.2 is considered, and literature of insufficient quality is filtered out. The two literature searches applied these conditions differently.

(1) The paper researches combining the cryptography and steganography disciplines.
(2) The paper researches the application of cryptography and steganography in specific domains (e.g. medical, military, financial) or contexts, and not in a general sense (i.e. to "secure communications").
(3) The paper addresses efforts to improve the security of a system or process, not only to send additional data.
(4) Is the objective clear?
(5) Are related works studied?
(6) Is the methodology clear?
(7) Are the results clear and measured?

2.2.1 *Literature Search 1: Journal Articles.*

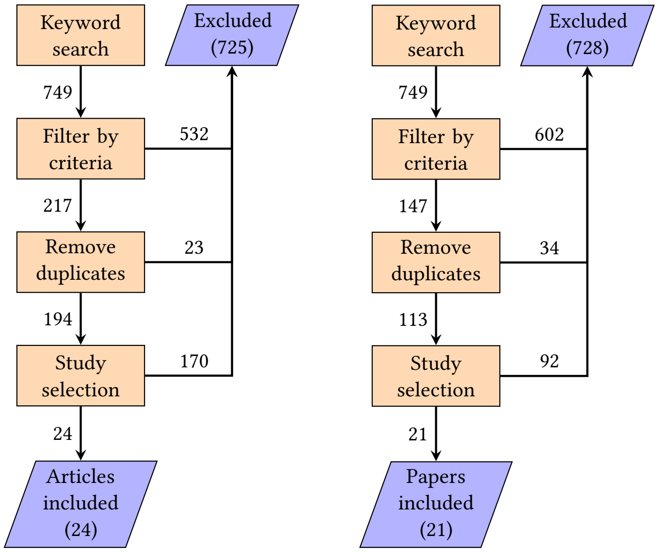
For the first literature search covering journal articles, papers were checked for relevance using **conditions 1-3** (section 2.2) based on title and abstract. Next, papers were **also checked for conditions 4-7** (section 2.2) by scanning the contents. A paper is only included if it meets all seven conditions. This selection process reduced the total results to **24 journal articles**. The flow chart in Fig. 2a shows the process of data gathering and study selection. Papers discussing no particular application (i.e. "secure communications") were not categorized as such, as the search query has already left out a large amount of these papers. Including them would result in an incomplete list.

2.2.2 *Literature Search 2: Conference Papers.*

The literature in the second search, covering conference papers, is **only checked for conditions 1-3** (section 2.2) based on the title and abstract as these are required to determine whether to consider a paper for RQ1. This selection process resulted in **21 conference papers**. Note that two papers appeared to be released before 2018 and were thus filtered out manually. The flow chart in Fig. 2b shows the process of data gathering and study selection.

2.3 Data Extraction

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 (section 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.



(a) Search 1: Journal Articles.

(b) Search 2: Conference Papers.

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

3 RESULTS

This section presents the findings from the systematic review, addressing the research questions outlined in section 1.2. Figures and tables are provided to enhance the visual comprehension of the findings. The arrangement of the following sections aligns with the order of the research questions. Section 3.1 covers the types of applications encountered and how they can be categorized. In section 3.2, the applications, limitations, and advantages are discussed, while in section 3.3 analysis methods.

3.1 RQ1: Exploring Applications

From each study, characteristics related to the context in which it explores the use of steganography with cryptography were extracted. The analysis of the literature suggests the importance of categorizing the application of an article in two ways:

- **The Application Domain**. The domain or industry sector an application operates in. Application domains encountered are: *financial*, *government*, *medical*, *transportation*.
- **The Technological Domain/Technology** [73]. One or more technological topics involved in an application. A technology is considered a tool that can be utilized across various domains to solve different problems or perform various tasks. Technologies encountered are: *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), Voice Operated Systems (Voice).*

By considering these two separate categorizations it enables a more specific identification of commonalities and differences in the applications, which can inform further research and the development of solutions tailored to specific application domains or technologies. This differs from how other reviews ([46]) perform categorization of applications. A study may focus on an application specific to an application domain, such as the *medical* domain, however, other articles ([1, 7, 9, 14, 19, 33, 36, 86, 87, 91] [5, 10]) focus only on applications in a technological domain. A technological domain can apply to a broad number of application domains. As an article may cover both, categorization by application domain is preferred, and in case an application domain or technological domain could not be determined it has not been included. Additionally, independent of the application or technological domain, the specific focus or functionality of an application is also determined:

- **The Functionality**: This refers to the specific features, tasks, or roles an application performs within its domain. Security is considered a common role of the explored literature and is therefore not specified as functionality. For example: *Smart Monitoring, Anonymisation, Healthcare Data Transmission, Vehicle Diagnostics, Malware Detection, Industry 4.0/5.0 Implementation.*

In the following two sections, the results of both literature searches are presented.

3.1.1 Journal Articles.

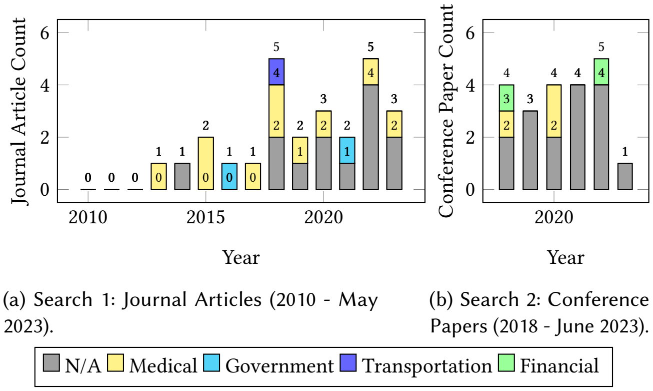
The results from literature search 1 for this question are presented in two tables. Table 1 considers articles and their application domain, while Table 2 the technology, reflecting the split in categorization. For extended tables refer to Appendix A. As some studies only focus on a technological domain, possible application domains, either suggested by the authors or based on similar literature, have been specified in *italics*. A technology can often apply to a broader range of application domains. In these cases, the application domain is specified as '*Cross-Domain*'.

Journal articles published by year from 2010-2023 are shown in Fig. 3a, grouped by the three identified application domains (*Medical*, *Government*, and *Transportation*) or only technological domains (*N/A*). In this figure, a slight rise in articles focussing on only technological domains can be seen, compared to application domains. Given the potential wide range of application domains that can benefit from these technologies (for example IoT [64]), a focus on innovation of technologies in a broader sense should be expected first. Later, optimizing these technologies for specific application domains could yield even greater rewards.

Fig. 4 visualizes the distribution of application domains (Fig. 4a) and technological domains (Fig. 4c) determined from the data in Table 1. In Fig. 4a, it can be seen that a large part (n=9, [13, 22, 34, 42, 45, 57, 62, 79, 89]) out of 12 focus on the *medical* domain, potentially indicating that the area of research has been rather narrow. Additionally, only few focus on *governmental* applications (n=2, [76, 88]) and *transportation* (n=1, [49]). Similarly, occurrences of a Technological Domain is visualized in Fig. 4c. Note that the technologies with an occurrence of 1 have been grouped as '*Other*'. These are *Big Data, Fog Computing, Web Applications, Personal Computing, Edge computing, and Cyber-Physical Systems*

Table 1. Journal papers focussing on Application Domain (*Government*, *Medical*, *Transportation*) and (optionally) Technological Domain.

Ref.	Technological Domains	Functionalities
Government		
[88]	Internet of Things	Smart monitoring, Anonymisation
[76]	Web Applications	Voting
Medical		
[57]	N/A[6]	Healthcare data transmission
[62]	N/A[6]	Healthcare data transmission
[89]	Cloud Computing	Healthcare data transmission and storage, Privacy protection
[34]	Internet of Things	Remote Patient Monitoring
[22]	Internet of Things	Healthcare data transmission
[42]	N/A[6]	Healthcare data transmission, DICOM
[45]	N/A[6]	Healthcare data transmission, DICOM
[13]	N/A[6]	Healthcare data transmission
[79]	N/A[6]	Healthcare data tampering protection
Transportation		
[49]	Cloud Computing, Edge Computing	Vehicle diagnostics and updates



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

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

Fig. 3. Distribution of literature in Application Domains or only involving Technological Domains (N/A) by year.

After analysis, it appears only one article from 2018 focuses on an application in the Transportation domain. Similarly, 2021 and 2022 lack publications in the medical domain, while the four years prior did. Also notable is the spike in articles focussing on a technology in 2022. The applications discussed in these articles ([7, 36, 87, 91]) appear unrelated, making it difficult to determine if there is an underlying reason.

Additionally, an attempt was made to utilize the VOSviewer tool[10] to find overlap in the authorship of the identified journal articles. None of the articles showed any shared authors, suggesting a scattered distribution of researchers working on the topic. This may indicate the research on the combined approach of steganography and cryptography is relatively new, aligning with the increasing

[6] There is no apparent involvement of a technology in the topic.

[7] Possible domains based on the technology used (incl. but not limited to) [65]

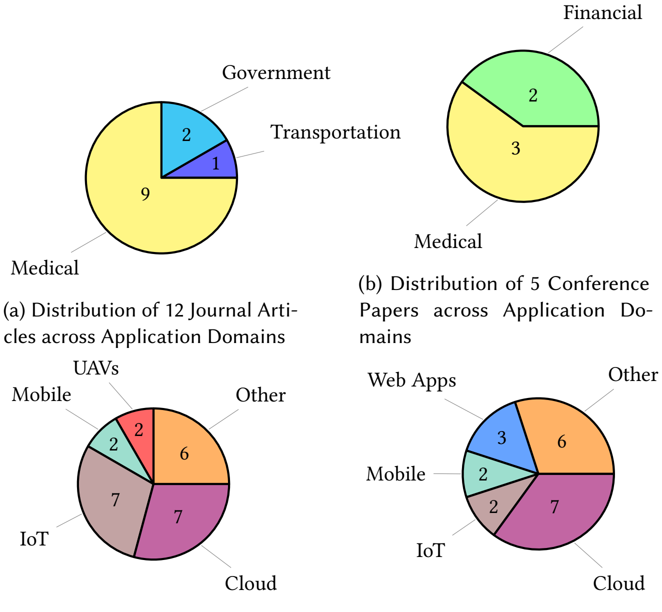
[8] Similar to [36]

[9] Suggested by the authors.

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

Table 2. Journal papers focussing on Technological Domains (Cloud, CPS, etc.) and (optionally) recommended Application Domains.

Ref.	Application Domains	Functionalities
Cloud		
[86]	*Military*[9], *Cross-Domain*	Access Control, Privacy protection
[87]	*Medical*[9]	Access Control
[9]	*Medical, Military*[9]	Privacy Protection
Cloud, Big Data		
[14]	*Energy, Medical, Finance*[7]	Data transmission, *Healthcare data transmissions*[7]
CPS		
[91]	*Cross-Domain*[9]	N/A
IoT		
[7]	*Cross-Domain*	Data transmission
IoT, Fog		
[33]	*Cross-Domain*	Data transmission
IoT, UAVs		
[36]	*Cross-Domain*[9]	Industry 5.0
[1]	*Cross-Domain*[8]	Industry 4.0
Mobile		
[10]	*Cross-Domain*	Malware detection, Malware development
Mobile, Cloud		
[19]	*Entertainment, Finance*[9]	Access control
Personal		
[5]	*Cross-Domain*	Data storage



(a) Distribution of 12 Journal Articles across Application Domains

(b) Distribution of 5 Conference Papers across Application Domains

(c) Occurrences of Technological Domains in 24 Journal Articles

(d) Occurrences of Technological Domains in 21 Conference Papers

Fig. 4. Distributions of Domains of Journal Articles (left) and Conference Papers (right)

trend in the number of articles in the last 13 years in Fig. 3a, but additional factors may be involved. In section 3.2, journal articles focussing on an application domain will be discussed more in-depth.

3.1.2 *Conference Papers.*

Additionally, to provide further insight conference papers are also analyzed. The data collected in this additional literature search is available in Appendix B. Similarly to journal papers, the year in which papers were published is shown in Fig. 3b. Here, a relatively stable number of papers have been published each year, possibly indicating the interest in combining steganography and cryptography has not changed, or this change already having occurred. Unfortunately, due to time constraints, papers published before 2018 were not explored. Surprisingly, from 2018 to 2023, out of 21 papers few (n=5) focused on an application domain (see Fig. 4b). These papers span the *medical* domain (n=3, [23, 29, 48]) and a new *financial* domain (n=2, [53, 63]). *Medical* is again the most popular application domain. Moreover, while of the journal articles 50% of the identified literature explore an application in an application domain, only 24% of conference papers do. This could further emphasize the trend of developing technologies in a more general sense rather than focusing on specific application domains. In a comparable manner, the technological domains are shown in Fig. 4d. Noticeable are journal articles and conference papers sharing three prominent technologies (*Mobile Computing*, *Internet of Things*, and *Cloud Computing*), and again the prevalence of *Cloud Computing*. It should be noted that a direct comparison between both searches is difficult due to the difference in the time period of the literature.

3.2 RQ2: Advantages, limitations and trade-offs

This section discusses observations made on algorithms and methodologies used throughout **journal articles**. First, it presents general observations, after which it will discuss the three **application domains** encountered in journal articles: *Government*, *Medical* and *Transportation* (listed in Table 1). The full data collected for this RQ can be found in Appendix C.

3.2.1 *Government Application Domain.*

This section covers 2 articles which explore an application of both steganography and cryptography in the *government* domain, covering surveillance and voting. Table 3 lists these articles. Their approaches have different strengths and limitations. While the two-tiered video surveillance system provides robustness against cipher-breaking attacks, its quality of recovered data depends on the CS compression rate. The system could also be modified to allow for more than two levels of authorization. On the other hand, the online voting system, despite providing individual verifiability and security, is susceptible to certain security challenges such as collusion among polling officers and network eavesdropping. The system provides receipts, which creates a potential issue in case the user loses their receipt. The performance, such as smaller receipt size, may be improved by exploring other algorithms.

3.2.2 *Medical Application Domain.*

Table 3. Advantages and limitations in the government domain.

No.	Evaluation
[88]	+ Multi-level auth., No extra channel, Robust against attacks - Face recovery dependent on compression
[76]	+ Verifiability, (k,n) encryption - Collusion, Traffic spoofing, Lost receipts

This section covers 9 articles which explore an application in the *medical* domain. Table 4 lists the articles with encountered advantages and limitations. Three papers ([57, 62, 89]) present the use of chaotic algorithms in their encryption method. While [57] presents a transmission system for generic data that performs chaotic encryption using a 2D-Henon map ([85]), due to limited practical implementation details, future works could draw upon [54] for a deeper implementation analysis. Unfortunately, these three papers lack performance analysis and key measurements like Computation Time (CT) and Throughput (TP) for the chaotic algorithms, hindering assessment of their potential for real-time systems. [62, 89], which use chaotic encryption, can inspire similar approaches. While not all chaotic encryption algorithms, due to complex iterative operations, suit real-time systems, less resource-intensive methods like [61] could be viable. This could be a future scope for research.

Health data in IoT. Two papers ([22, 34]) involve health data transmissions from IoT devices (which generally prefer low power consumption and low computational complexity) in the context of remote patient monitoring. [34] hides data in ECG signals. Conversely, [22] employs image steganography. Both first encrypt data and embed afterward. [34] necessitates the receiver's knowledge of the encryption and embedding keys and transmits no key, while [22] embeds both data and the encryption key. [34] employs XOR cipher for its computational simplicity, while [22] utilizes AES ([30]) and RSA ([92]) encryption. More secure or efficient alternatives like TEA and its variants [51], or hardware-accelerated AES ([55]) could be considered for IoT devices. Both papers use multi-level DWT for steganography. These differences highlight the variety of methodologies applied to protect patient data in IoT transmissions.

Embedding location restrictions. Of the medical papers on healthcare data transmissions, two ([42, 89]) discuss methods that impose restrictions on data embedding locations. [89] uses Distance Regularized Level Set Evolution (DRLSE) [43] to identify Region of Interest (ROI, the lesion area) and Non-Region of Interest (NROI) in a medical image. Data is embedded in the NROI using adaptive PEE for high capacity, while in the ROI, a custom algorithm based on histogram-shifting with contrast enhancement is used for visual clarity. This paper first embeds data and then encrypts the image. [42] also identifies ROI and NROI, specifically in DICOM, and contrastingly it performs encryption first. However, identification of these areas is performed using edge detection instead (Gabor Filter and Canny Edge [56]). Here, patient data is only embedded in the NROI to preserve quality. Moreover, verifiability of integrity, crucial in medical applications, is maintained by embedding an ROI-generated hash in the NROI.

DICOM. While [42, 45] focus on improving DICOM imagery and employ Reversible Data Hiding (RDH), their implementations differ. In both papers, data is first encrypted and then embedded in the image medium. The papers differ in use of algorithms, as [42] uses the RSA algorithm for encryption, while in [45] a XOR cipher is applied with a 128-bit key generated from the cover image's histogram. The length of this key could be increased to 256-bit, as the key generation method appears to support this. However, embedding block selection will be affected, reducing the size of blocks. Both applications apply asymmetric encryption. The main difference in application is where [42] embeds patient data in a DICOM, [45] is about protecting the DICOM image itself and embedding the key used for encryption. In both papers, encryption is performed before embedding. Both papers employ LSB-based steganography, however, in [42] it is combined with a novel graph-coloring approach. Due to the nature of the graph coloring used, brute-forcing is difficult [42].

Hardware. [79] is a complex hardware focused application. Of the identified literature it is the only application that applies to the design of circuits. Reading the paper is highly recommended due to its distinctive approach. However, it is important to note that the paper also focuses on hardware aspects, requiring an understanding of hardware-related concepts.

Table 4. Advantages and limitations in the medical domain.

No.	Evaluation
[57]	+ Improved imperceptibility, Double embedding - Lack of depth
[62]	+ Sensitive to attacks (Integrity), High capacity - File size
[89]	+ Minimal ROI impact, High NROI capacity, Adaptive, Contrast enhancement, No under- and overflow
[34]	+ Visually undetectable, Complete extraction
[22]	+ Higher PSNR, Lower MSE - AES key is shared on channel
[42]	+ Integrity, ROI intact, Dynamic key - Depends on NROI size
[45]	+ Very low computation time, No extra channel
[13]	+ High capacity at same PSNR, Base-16, No under- and overflow - Higher BER
[79]	+ Counterfeit detection, Malicious logic prevention, Low cost design

3.2.3 Transportation Application Domain.

One article covers an application in the transportation domain. Table 5 lists advantages and limitations. [49] more securely delivers diagnostic data to manufacturers and firmware updates. The system, while innovative, could suffer from protracted decryption times and potential inefficiency when dealing with larger OTA files. Future work could explore the use of more efficient cryptographic algorithms and adapt the method to better accommodate larger files (which is common with updates). Future work in the transportation domain could explore vehicle-to-vehicle (V2V) networks, where speed and size of communication should be minimal.

Table 5. Advantages and limitations in the transportation domain.

No.	Evaluation
[49]	+ Data integrity - Processing time

3.2.4 General Observations.

Observations related to all journal articles can be made. First, the steganography methods commonly used in the identified applications primarily involve images, as shown in Table 6. There is a noticeable **underutilization** of the other cover mediums (*audio, signal, hardware, video, text*), indicating a clear gap of research in this area. In the medical domain, 7 out of 9 articles utilize image steganography. The choice of image-based steganography in medical applications, considering the frequent use of imaging, is effective, but exploring other types like video steganography in recorded surgeries or expanding signal steganography beyond ECG signals could diversify data types and enhance usability and robustness in more systems.

Second, in some applications ([22, 45]), the encryption key is **embedded along** with data in the cover medium, removing the need for a separate communication channel (in case of dynamic keys) or pre-established cryptographic key.

Table 6. Journal Articles and their cover medium.

Medium	Journal Articles
Image	[88], [76], [57], [62], [89], [22], [42], [45], [13], [49], [86], [87], [9], [7], [33], [36], [1], [10], [19], [5]
Signal	[34], [91]
Audio	[14]
Hardware	[79]

Third, 42% of the identified articles, across both application domains and technological domain, incorporate a **Reversible Data Hiding** (RDH) technique. Primarily, RDH allows for lossless reconstruction of the original cover media after the hidden data is extracted. This is crucial in sectors like healthcare, where the integrity of original data (e.g., medical imagery) must often be maintained [13, 22, 42, 45, 62, 89].

These findings suggest the need to diversify research on methods and cover mediums. Government application security challenges require attention, and chaotic algorithms' performance in medical domains requires better assessment. A wider range of steganography methods should be explored for healthcare data transmissions, and in transportation, exploration of other cryptographic algorithms is advised for handling larger data files effectively. Research could improve data security across sectors.

3.3 RQ3: Analyzing evaluation methods used

This section discusses the analysis and evaluation methods used in **journal articles**, listed in Appendix D. Analysis of steganography is generally based on four concepts: capacity, robustness, security, and imperceptibility (sometimes split into undetectability and invisibility) [4, 69, 83]. For cryptography, evaluation revolves around security, encryption time, key size, and plain vs cipher size, among others [26, 84]. Due to similarities in these concepts, they are grouped in three perspectives: *Security*, *Performance*, and *User*. These three perspectives are interdependent, as shown in Fig. 5.

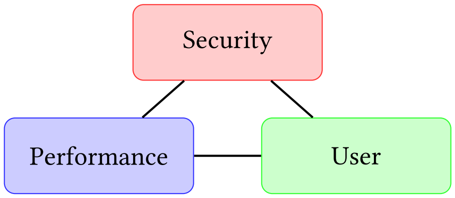


Fig. 5. The three discussed analysis perspectives.

3.3.1 Security Perspective.

Just as cryptography can be vulnerable to various types of attacks, such as ciphertext and plaintext attacks [50], steganography is also subject to similar types of attacks, including known carrier and known message attacks [50]. The importance of protection against these attacks depends on the order of applying steganography and cryptography.

If data is **embedded first** and encrypted afterward, the strength of the encryption is the foremost defense against attacks. [13, 57, 88, 89] (Appendix C) are examples of articles which employ this order. Among these, some consider advanced attacks like histogram equalization ([9, 45, 62, 89]), and only one performs rotation attacks ([62]).

Similarly, if data is **encrypted first**, the strength or imperceptibility of the stego object is the foremost defense against attacks. Most applications utilize this order of operations ([13, 22, 34, 42, 45, 49, 62, 76] a.o.). These implementations focus mostly on stenographic imperceptibility using metrics such as PSNR, SSIM, MSE, and BER, and rely mostly on cryptographic evaluation from previous works. Articles that propose a custom or more complex encryption method ([34, 45, 49, 57, 62, 89]) still analyze cryptographic security.

3.3.2 Performance Perspective.

Performance of systems encountered can be affected by several factors: computation time (CT, related to both steganography and cryptography [27]), capacity (usually in Bits-Per-Pixel, only related to steganography [69]), and key size (in this case only cryptography [27, 84]).

Typically, an increase in **computation time** corresponds to an increase in power consumption, making it an important factor in both **real-time** and **power-sensitive** systems. While [1, 13, 33, 36, 45, 49] employ CT measurements, only the two similar applications [1, 36] appear to operate in an environment where power consumption should specifically be managed. CT measurements are generally discussed in 'total time', or analyzed per component of the system individually [49]. In this case, embedding time, extraction time, encryption time, and more are tested separately. This way, performance improvements can be made more specific. Surprisingly, of seven articles exploring applications in the Internet of Things, three [7, 22, 34] do not utilize a time-based analysis metric. This makes it difficult to accurately assess the performance and efficiency of their proposed applications. A time-based analysis is key in comprehensively understanding application performance, as it not only reveals how quickly processes are carried out, but it also provides insights into how efficiently system resources are being utilized.

Another important metric is **capacity**. The balance between imperceptibility and capacity is important, depending on the application. For (real-time) applications which share relatively small pieces of data, the capacity of a cover medium may not be as important. In this case, imperceptibility could also be less relevant. Capacity is evaluated (either compared to other implementations or to itself with different parameters) in 9 out of 24 articles [5, 7, 9, 13, 42, 62, 76, 86, 87]. Notable is that only one article ([7]) involving IoT analyzed the capacity of the steganographic method employed.

For cryptographic algorithms, the **key size** can greatly affect encryption time as described in [41]. [22] focuses on IoT and performs cryptographic operations using an AES key size of 128 bits. While AES-128 is generally considered secure, larger keys can be used. More efficient encryption algorithms could enable the use of larger keys at similar encryption times. Surprisingly, key sizes for well-known cryptographic algorithms do not appear to be discussed or justified very often.

3.3.3 User Perspective.

The user perspective assesses how seamlessly a system incorporating steganography and cryptography fits into the user's workflow, with a focus on ease of use, comprehension, trust, processing time, and system stability. The impact of the system on the user's workflow is especially critical for applications where the user has direct interaction with the system, though slightly less where the system is operating in the background, potentially impacting the user's experience.

From the surveyed literature, a limited number conduct **usability tests** to analyse user experience. The e-voting system implementation discussed in [76] conducts usability and **user acceptance** testing using Nielsen's quality components [59] and Davis' Technology Acceptance Model (TAM) [20] respectively. These methods are well-established. Similarly, the NFC access control scheme in [19] conducts usability, perceived vulnerability, perceived security, and behavioural intention tests, examining how the proposed security scheme could influence user behaviour. Here, methods were adapted from [15, 35, 77].

Applications such as remote patient monitoring ([34]) are intended to be user-friendly, requiring little to no complex additional setup from the user's end. It mentions **additional complexity** introduced by the implementation of steganography or cryptography should ideally be abstracted away from the user, however, the only user interaction presented in the article is related to Human Visual System (HVS) imperceptibility (doctors inspecting ECGs). Similarly, hiding files in audio files on PCs [5] is an application close to the end user, however, it does not explore this area further and omits such user testing, leaving an evaluation gap in comprehending the actual user experience and possible improvements.

User experience could significantly be impacted by other perspectives (security, performance). If combining steganography and cryptography causes excessively **slow data processing**, or if the system **lacks robustness** against actions such as compression or cropping attacks, the user's ability to manage (share, post-process) stego objects could be more easily compromised, potentially causing data loss or corruption, degrading the user's experience. Hence, robust implementations of steganography and cryptography are crucial for maintaining a high-quality user experience.

3.3.4 General Observations.

In summary, evaluating steganography and cryptography necessitates careful analysis across security, performance, and user perspectives. Despite their importance, many studies miss certain metrics, creating gaps in comprehending computation time, capacity, key size, and user-friendliness. Balancing steganography and cryptography is crucial to ensure user experience, security, and performance. Future works should aim to address these oversights.

4 CONCLUSION

This review has examined the current state of combined steganography and cryptography applications in journal articles and conference papers. Applications were categorized based on their application domain (e.g., *medical*, *finance*) and technological domain (e.g., *Internet of Things*, *Cloud Computing*). The prevalence of *medical* applications suggests a limited range of domains being explored. Of technologies, *Internet of Things* and *Cloud Computing* applications are actively studied. Real-time constraints and privacy protection in data exchange scenarios are prominent focuses within technological domains. Overall, the combined approach offers advantages in data security and privacy protection across various domains, but trade-offs and limitations exist. Further research is needed to address these challenges and improve methodologies. Evaluation metrics and methods vary, emphasizing the importance of domain-specific knowledge in designing secure systems. To address this, a more generic evaluation with three perspectives (security, performance, and user) is discussed, which incorporates robustness, imperceptibility, capacity, and resistance to attacks. Surprisingly, there is a lack of user testing in the literature. These perspectives highlight the importance of considering the end user in system design.

4.1 Limitations & Future Research Directions

As mentioned before, due to time constraints this review only considered conference papers for RQ1. In the fast-paced field of information security, conference papers often contain the most recent findings and innovative practices. This potentially indicates their relevance not just for RQ1, but also for RQ2 and RQ3. Secondly, the search keywords of this review are limited to the use of the words 'cryptography' and 'steganography', while these technologies may not be explicitly named but instead referred to as 'encryption' or 'data-hiding' respectively. Future research could explore applications in more application domains such as transportation and energy. Research could compare combined implementations to only using either steganography or cryptography to understand in what situations using only one may be better. More research could be done into applying steganographic mediums other than images. It could also explore the impact of combining steganography and cryptography on the experience of the end user more extensively, and understanding user acceptance.

REFERENCES

[1] Khalid A. Alissa, Mohammed Maray, Areej A. Malibari, Sana Alazwari, Hamed Alqahtani, Mohamed K. Nour, Marwa Obbaya, Mohamed A. Shamseldin, and Mesfer Al Duhayyim. 2023. Optimal Deep Learning Model Enabled Secure UAV Classification for Industry 4.0. *Computers, Materials & Continua* 74, 3 (2023), 5349–5367. https://doi.org/10.32604/cmc.2023.033532

[2] Mustafa S. Abbas, Suadad S. Mahdi, and Shahad A. Hussien. 2020. Security Improvement of Cloud Data Using Hybrid Cryptography and Steganography. *Proceedings of the 2020 International Conference on Computer Science and Software Engineering, CSASE 2020* (4 2020), 123–127. https://doi.org/10.1109/CSASE48920.2020.9142072

[3] Amjad Anwer M. Al Abbas and Najla Badie Ibraheem. 2022. Using DNA In Adynamic Lightweight Algorithm For Stream Cipher In An IoT Application. In *2022 International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*. IEEE, 232–240. https://doi.org/10.1109/ISMSIT56059.2022.9932739

[4] Zaidoon Kh. AL-Ani, A. A. Zaidan, B. B. Zaidan, and Hamdan. O. Alanazi. 2010. Overview: Main Fundamentals for Steganography. 2 (3 2010). https://arxiv.org/abs/1003.4086v1

[5] Nouf Al-Juaid and Adnan Gutub. 2019. Combining RSA and audio steganography on personal computers for enhancing security. *SN Applied Sciences* 1, 8 (8 2019), 830. https://doi.org/10.1007/s42452-019-0875-8

[6] Maytham Hakim Ali and Saif Al-Alak. 2022. Node Protection using Hiding Identity for IPv6 Based Network. In *2022 Muthanna International Conference on Engineering Science and Technology (MICEST)*. IEEE, 111–117. https://doi.org/10.1109/MICEST54286.2022.9790135

[7] Suray Alsamaraee and Ali Salem Ali. 2022. A crypto-steganography scheme for IoT applications based on bit interchange and crypto-system. *Bulletin of Electrical Engineering and Informatics* 11, 6 (12 2022), 3539–3550. https://doi.org/10.11591/EEI.V11I6.4194

[8] Ross J. Anderson and Fabien A.P. Petitcolas. 1998. On the limits of steganography. *IEEE Journal on Selected Areas in Communications* 16, 4 (5 1998), 474–481. https://doi.org/10.1109/49.668971

[9] R. Anushiadevi and Rengarajan Amirtharajan. 2023. Design and development of reversible data hiding- homomorphic encryption &amp; rhombus pattern prediction approach. *Multimedia Tools and Applications* (5 2023). https://doi.org/10.1007/s11042-023-15455-1

[10] Shikha Badhani and Sunil K. Muttoo. 2018. Evading android anti-malware by hiding malicious application inside images. *International Journal of System Assurance Engineering and Management* 9, 2 (4 2018), 482–493. https://doi.org/10.1007/s13198-017-0692-7

[11] Parmit Singh Banga, A. Omar Portillo-Dominguez, and Vanessa Ayala-Rivera. 2022. Protecting User Credentials against SQL Injection through Cryptography and Image Steganography. In *2022 10th International Conference in Software Engineering Research and Innovation (CONISOFT)*. IEEE, 121–130. https://doi.org/10.1109/CONISOFT55708.2022.00025

[12] Putta Bharathi, Gayathri Annam, Jaya Bindu Kandi, Vamsi Krishna Duggana, and Anjali T. 2021. Secure File Storage using Hybrid Cryptography. In *2021 6th International Conference on Communication and Electronics Systems (ICCES)*. IEEE, 1–6. https://doi.org/10.1109/ICCES51350.2021.9489026

[13] Rupali Bhardwaj. 2023. An improved reversible data hiding method in encrypted domain for E-healthcare. *Multimedia Tools and Applications* 82, 11 (5 2023), 16151–16171. https://doi.org/10.1007/s11042-022-13905-w

[14] Shiladitya Bhattacharjee, Lukman Bin Ab. Rahim, Junzo Watada, and Arunava Roy. 2020. Unified GPU Technique to Boost Confidentiality, Integrity and Trim Data Loss in Big Data Transmission. *IEEE Access* 8 (2020), 45477–45495. https://doi.org/10.1109/ACCESS.2020.2978297

[15] Moniruzzaman Bhuiyan and Rich Picking. 2011. A Gesture Controlled User Interface for Inclusive Design and Evaluative Study of Its Usability. *Journal of Software Engineering and Applications* 04, 09 (2011), 513–521. https://doi.org/10.4236/JSEA.2011.49059

[16] Mohammad Ubaidullah Bokhari and Qahtan Makki Shallal. 2016. A Review on Symmetric Key Encryption Techniques in Cryptography. *International Journal of Computer Applications* 147, 10 (8 2016), 43–48. https://doi.org/10.5120/IJCA2016911203

[17] Reynaldo E. Castillo, Gerald T. Cayabyab, Paula Jean M. Castro, and Ma. Rachel Aton. 2018. BlockSight. In *Proceedings of the 2018 International Conference on Information Science and System*. ACM, New York, NY, USA, 117–121. https://doi.org/10.1145/3209914.3209922

[18] L. Caviglione, M. Podolski, W. Mazurczyk, and M. Ianigro. 2017. Covert channels in personal cloud storage services: The case of dropbox. *IEEE Transactions on Industrial Informatics* 13, 4 (2017), 1921–1931. https://doi.org/10.1109/TII.2016.2627503

[19] Soon-Nyean Cheong, Huo-Chong Ling, and Pei-Lee Teh. 2014. Secure Encrypted Steganography Graphical Password scheme for Near Field Communication smartphone access control system. *Expert Systems with Applications* 41, 7 (6 2014), 3561–3568. https://doi.org/10.1016/j.eswa.2013.10.060

[20] Fred D. Davis. 1989. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly: Management Information Systems* 13, 3 (1989), 319–339. https://doi.org/10.2307/249008

[21] Sachin Dhawan, Chinmay Chakraborty, Jaroslav Frnda, Rashmi Gupta, Arun Kumar Rana, and Subhendu Kumar Pani. 2021. SSII: Secured and high-quality steganography using intelligent hybrid optimization algorithms for IoT. *IEEE Access* 9 (2021), 87563–87578. https://doi.org/10.1109/ACCESS.2021.3089357

[22] Mohamed Elhoseny, Gustavo Ramirez-Gonzalez, Osama M. Abu-Elnasr, Shihab A. Shawkat, N. Arunkumar, and Ahmed Farouk. 2018. Secure Medical Data Transmission Model for IoT-Based Healthcare Systems. *IEEE Access* 6 (3 2018), 20596–20608. https://doi.org/10.1109/ACCESS.2018.2817615

[23] Soha M Gamal, Sherin M Youssef, and Ayman Abdel-Hamid. 2020. 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)*. IEEE, 9–14. https://doi.org/10.1109/iCCECE49321.2020.9231144

[24] Suyash S. Ghuge, Nishant Kumar, S Savitha, and V Suraj. 2020. Multilayer Technique to Secure Data Transfer in Private Cloud for SaaS Applications. In *2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*. IEEE, 646–651. https://doi.org/10.1109/ICIMIA48430.2020.9074969

[25] Shailender Gupta, Ankur Goyal, and Bharat Bhushan. 2012. Modern Education and Computer Science. *Modern Education and Computer Science* 6 (2012), 27–34. https://doi.org/10.5815/ijmecs.2012.06.04

[26] Gururaja H S, M Seetha, and Anjan K Koundinya. 2013. Design and Performance Analysis of Secure Elliptic Curve Cryptosystem. *International Journal of Advanced Research in Computer and Communication Engineering* 2 (2013). www.ijarcce.com

[27] Md Enamul Haque, Sm Zobaed, Muhammad Usama Islam, and Faaiza Mohammad Areef. 2019. Performance Analysis of Cryptographic Algorithms for Selecting Better Utilization on Resource Constraint Devices. *2018 21st International Conference of Computer and Information Technology, ICCIT 2018* (1 2019). https://doi.org/10.1109/ICCITECHN.2018.8631957

[28] P Harsha Sri and K Nagendra Chary. 2022. SECURE FILE STORAGE USING HYBRID CRYPTOGRAPHY. *International Research Journal of Modernization in Engineering Technology and Science* (12 2022). https://doi.org/10.56726/IRJMETS32383

[29] Mohammed Mahdi Hashim, Suhad Hasan Rhaif, Ali A. Abdulrazzaq, Adnan Hussein Ali, and Mustafa Sabah Taha. 2020. Based on IoT Healthcare Application for Medical Data Authentication: Towards A New Secure Framework Using Steganography. *IOP Conference Series: Materials Science and Engineering* 881, 1 (7 2020), 012120. https://doi.org/10.1088/1757-899X/881/1/012120

[30] Simon Heron. 2009. Advanced Encryption Standard (AES). *Network Security* 2009, 12 (12 2009), 8–12. https://doi.org/10.1016/S1353-4858(10)70006-4

[31] Mehdi Hussain, Ainuddin Wahid, Abdul Wahab, Ishrat Batool, and Muhammad Arif. 2015. Secure Password Transmission for Web Applications over Internet using Cryptography and Image Steganography. *International Journal of Security and Its Applications* 9, 2 (2015), 179–188. https://doi.org/10.14257/ijsia.2015.9.2.17

[32] A A Hussein and O Q J Al-Thahab. 2020. Design and simulation a video steganography system by using FFT-Turbo code methods for copyrights application. *Eastern-European Journal of Enterprise Technologies* 2, 9-104 (2020), 43–55. https://doi.org/10.15587/1729-4061.2020.201010

[33] Shaimaa A. Hussein, Ahmed I. Saleh, and Hossam El-Din Mostafa. 2020. A new fog based security strategy (FBS2) for reliable image transmission. *Journal of Ambient Intelligence and Humanized Computing* 11, 8 (8 2020), 3265–3303. https://doi.org/10.1007/s12652-019-01512-x

[34] Ayman Ibaida and Ibrahim Khalil. 2013. Wavelet-Based ECG Steganography for Protecting Patient Confidential Information in Point-of-Care Systems. *IEEE Transactions on Biomedical Engineering* 60, 12 (12 2013), 3322–3330. https://doi.org/10.1109/TBME.2013.2264539

[35] Princely Ifinedo. 2012. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security* 31, 1 (2 2012), 83–95. https://doi.org/10.1016/J.COSE.2011.10.007

[36] Deepak Kumar Jain, Yongfu Li, Meng Joo Er, Qin Xin, Deepak Gupta, and K. Shankar. 2022. Enabling Unmanned Aerial Vehicle Borne Secure Communication With Classification Framework for Industry 5.0. *IEEE Transactions on Industrial Informatics* 18, 8 (8 2022), 5477–5484. https://doi.org/10.1109/TII.2021.3125732

[37] Bartosz Jankowski, Wojciech Mazurczyk, and Krzysztof Szczypiorski. 2013. PadSteg: Introducing inter-protocol steganography. *Telecommunication Systems* 52, 2 (2 2013), 1101–1111. https://doi.org/10.1007/S11235-011-9616-Z/METRICS

[38] Rekha Kashyap* and Manasvini Ganesh. 2019. Securing Information for Commercial File Sharing by Combining Raster Graphic a nd Vector Graphic Stseganographies. *International Journal of Engineering and Advanced Technology* 8, 6 (8 2019), 788–795. https://doi.org/10.35940/ijeat.F8005.088619

[39] V. Kavitha, G S Sruthi, B Thoshinny, and S R Riduvarshini. 2022. Stagchain – A Steganography based Application Working on a Blockchain Environment. In *2022 3rd International Conference on Electronics and Sustainable Communication Systems (ICESC)*. IEEE, 674–681. https://doi.org/10.1109/ICESC54411.2022.9885394

[40] H.A. Khan, R. Abdulla, S.K. Selvaperumal, and A. Bathich. 2021. IoT based on secure personal healthcare using RFID technology and steganography. *International Journal of Electrical and Computer Engineering* 11, 4 (2021), 3300–3309. https://doi.org/10.11591/ijece.v11i4.pp3300-3309

[41] M. Guru Vimal Kumar and U. S. Ragupathy. 2016. A Survey on current key issues and status in cryptography. *Proceedings of the 2016 IEEE International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET 2016* (9 2016), 205–210. https://doi.org/10.1109/WISPNET.2016.7566121

[42] Nawlesh Kumar and V. Kalpana. 2015. A Novel Reversible Steganography Method using Dynamic Key Generation for Medical Images. *Indian Journal of Science and Technology* 8, 16 (7 2015), 1–9. https://doi.org/10.17485/IJST/2015/V8I16/61974

[43] Chunming Li, Chenyang Xu, Changfeng Gui, and Martin D. Fox. 2010. Distance regularized level set evolution and its application to image segmentation. *IEEE Transactions on Image Processing* 19, 12 (12 2010), 3243–3254. https://doi.org/10.1109/TIP.2010.2069690

[44] K P Bindu Madavi and P. Vijaya Karthick. 2021. Enhanced Cloud Security using Cryptography and Steganography Techniques. In *2021 International Conference on Disruptive Technologies for Multi-Disciplinary Research and Applications (CENTCON)*. IEEE, 90–95. https://doi.org/10.1109/CENTCON52345.2021.9687919

[45] L. Mancy and S. Maria Celestin Vigila. 2018. A new diffusion and substitution based cryptosystem for securing medical image applications. *International Journal of Electronic Security and Digital Forensics* 10, 4 (2018), 388–400. https://doi.org/10.1504/IJESDF.2018.095140

[46] Pratap Chandra Mandal, Imon Mukherjee, Goutam Paul, and B. N. Chatterji. 2022. Digital image steganography: A literature survey. *Information Sciences* 609 (9 2022), 1451–1488. https://doi.org/10.1016/J.INS.2022.07.120

[47] S. Mandal and D.A. Khan. 2023. Enhanced-Longest Common Subsequence based novel steganography approach for cloud storage. *Multimedia Tools and Applications* 82, 5 (2023), 7779–7801. https://doi.org/10.1007/s11042-022-13615-3

[48] V.M. Manikandan and V. Masilamani. 2018. Reversible Data Hiding Scheme During Encryption Using Machine Learning. *Procedia Computer Science* 133 (2018), 348–356. https://doi.org/10.1016/j.procs.2018.07.043

[49] Kathiresh Mayilsamy, Neelaveni Ramachandran, and Vismitha Sunder Raj. 2018. An integrated approach for data security in vehicle diagnostics over internet protocol and software update over the air. *Computers & Electrical Engineering* 71 (10 2018), 578–593. https://doi.org/10.1016/j.compeleceng.2018.08.002

[50] Rina Mishra and Praveen Bhanodiya. 2015. A review on steganography and cryptography. *Conference Proceeding - 2015 International Conference on Advances in Computer Engineering and Applications, ICACEA 2015* (7 2015), 119–122. https://doi.org/10.1109/ICACEA.2015.7164679

[51] Zeesha Mishra and Bibhudendra Acharya. 2021. High throughput novel architectures of TEA family for high speed IoT and RFID applications. *Journal of Information Security and Applications* 61 (9 2021), 102906. https://doi.org/10.1016/J.JISA.2021.102906

[52] Hope Mogale, Michael Esiefarienrhe, and Lucia Letlonkane. 2018. Web Authentication Security Using Image Steganography and AES Encryption. In *2018 International Conference on Intelligent and Innovative Computing Applications (ICONIC)*. IEEE, 1–7. https://doi.org/10.1109/ICONIC.2018.8601208

[53] Shraddha S. More, Anagha Mudrale, and Sukhada Raut. 2018. Secure Transaction System using Collective Approach of Steganography and Visual Cryptography. In *2018 International Conference on Smart City and Emerging Technology (ICSCET)*. IEEE, 1–6. https://doi.org/10.1109/ICSCET.2018.8537262

[54] Melika Mostaghim and Reza Boostani. 2014. CVC: Chaotic visual cryptography to enhance steganography. *2014 11th International ISC Conference on Information Security and Cryptology, ISCISC 2014* (12 2014), 44–48. https://doi.org/10.1109/ISCISC.2014.6994020

[55] Pedro Sanchez Munoz, Nam Tran, Brandon Craig, Behnam Dezfouli, and Yuhong Liu. 2019. Analyzing the Resource Utilization of AES Encryption on IoT Devices. *2018 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference, APSIPA ASC 2018 - Proceedings* (3 2019), 1200–1207. https://doi.org/10.23919/APSIPA.2018.8659779

[56] Ehsan Nadernejad, Sara Sharifzadeh, and Hamid Hassanpour. 2008. Edge Detection Techniques: Evaluations and Comparisons. *Applied Mathematical Sciences* 2, 31 (2008), 1507–1520.

[57] Brem Navas, I Mohamed, and N Shenbagavadivu. 2015. Secured medical image transmission through the two dimensional chaotic system. *International Journal of Applied Engineering Research* 10 (5 2015), 38391–38396.

[58] S.S Neetha, J Bhuvana, and R Suchithra. 2023. 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)*. IEEE, 1–6. https://doi.org/10.1109/ISCON57294.2023.10112201

[59] Jakob Nielsen and Rolf Molich. 1990. Heuristic evaluation of user interfaces. *Conference on Human Factors in Computing Systems - Proceedings* (3 1990), 249–256. https://doi.org/10.1145/97243.97281

[60] Arooj Nissar and A. H. Mir. 2010. Classification of steganalysis techniques: A study. *Digital Signal Processing* 20, 6 (12 2010), 1758–1770. https://doi.org/10.1016/J.DSP.2010.02.003

[61] Amit Pande and Joseph Zambreno. 2011. A chaotic encryption scheme for real-time embedded systems: design and implementation. *Telecommunication Systems* 52, 2 (6 2011), 551–561. https://doi.org/10.1007/s11235-011-9460-1

[62] Shabir A. Parah, Farhana Ahad, Javaid A. Sheikh, and G.M. Bhat. 2017. Hiding clinical information in medical images: A new high capacity and reversible data hiding technique. *Journal of Biomedical Informatics* 66 (2 2017), 214–230. https://doi.org/10.1016/j.jbi.2017.01.006

[63] Nileema Patil and Renuka Kondabala. 2022. Two-Layer Secure Mechanism for Electronic Transactions. In *2022 International Conference on Recent Trends in Microelectronics, Automation, Computing and Communications Systems (ICMACC)*. IEEE, 174–181. https://doi.org/10.1109/ICMACC54824.2022.10093478

[64] Yusuf Perwej, Kashiful Haq, Firoj Parwej, and Mumdouh M. 2019. The Internet of Things (IoT) and its Application Domains. *International Journal of Computer Applications* 182, 49 (4 2019), 36–49. https://doi.org/10.5120/IJCA2019918763

[65] C. L. Philip Chen and Chun Yang Zhang. 2014. Data-intensive applications, challenges, techniques and technologies: A survey on Big Data. *Information Sciences* 275 (8 2014), 314–347. https://doi.org/10.1016/J.INS.2014.01.015

[66] Anthony Phipps, Karim Ouazzane, and Vassil Vassilev. 2020. 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)*. IEEE, 1428–1436. https://doi.org/10.1109/TrustCom50675.2020.00192

[67] Anchal Pokharana and Samiksha Sharma. 2021. 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)*. IEEE, 480–485. https://doi.org/10.1109/ICIRCA51532.2021.9544599

[68] S. Prabu and G. Ganapathy. 2020. Steganographic approach to enhance the data security in public cloud. *International Journal of Computer Aided Engineering and Technology* 13, 3 (2020), 388–408. https://doi.org/10.1504/IJCAET.2020.109522

[69] Anita Pradhan, Aditya Kumar Sahu, Gandharba Swain, and K. Raja Sekhar. 2016. Performance evaluation parameters of image steganography techniques. *International Conference on Research Advances in Integrated Navigation Systems, RAINS 2016* (12 2016). https://doi.org/10.1109/RAINS.2016.7764399

[70] Pramendra Prajapati, Pramendra Kumar MTech Scholar, and Vijay Kumar Sharma Asst. 2014. Information Security Based on Steganography & Cryptography Techniques: A Review. *International Journal of Advanced Research in Computer Science and Software Engineering* 4, 10 (10 2014), 2277. https://www.researchgate.net/publication/268388237

[71] Podamekala Preethi and G. Prakash. 2021. Secure Fusion of Crypto-Stegano Based Scheme for Satellite Image Application. In *2021 Asian Conference on Innovation in Technology (ASIANCON)*. IEEE, 1–6. https://doi.org/10.1109/ASIANCON51346.2021.9544752

[72] U. Ramamoorthy and A. Loganathan. 2022. Analysis of Video Steganography in Military Applications on Cloud. *International Arab Journal of Information Technology* 19, 6 (2022), 897–903. https://doi.org/10.34028/iajit/19/6/7

[73] D A ; ; Ravindran, R ; Vincent, K ; Srinivasan, Robertas Damaševičius, M Poongodi, Hafiz Tayyab Rauf, Hasan Ali Khattak, Nancy A Angel, Dakshanamoorthy Ravindran, P M Durai, Raj Vincent, Kathiravan Srinivasan, and Yuh-Chung Hu. 2021. Recent Advances in Evolving Computing Paradigms: Cloud, Edge, and Fog Technologies. *Sensors 2022, Vol. 22, Page 196* 22, 1 (12 2021), 196. https://doi.org/10.3390/S22010196

[74] V. Reshma, S. Joseph Gladwin, and C. Thiruvenkatesan. 2019. Pairing-Free CP-ABE based Cryptography Combined with Steganography for Multimedia Applications. In *2019 International Conference on Communication and Signal Processing (ICCSP)*. IEEE, 0501–0505. https://doi.org/10.1109/ICCSP.2019.8698053

[75] Haripriya Rout and Brojo Kishore Mishra. 2015. Pros and Cons of Cryptography, Steganography and Perturbation techniques. *IOSR Journal of Electronics and Communication Engineering* (2015), 2278–8735. www.iosrjournals.org

[76] Lauretha Rura, Biju Issac, and Manas Kumar Haldar. 2016. Implementation and Evaluation of Steganography Based Online Voting System. *International Journal of Electronic Government Research* 12, 3 (7 2016), 71–93. https://doi.org/10.4018/IJEGR.2016070105

[77] Young Sam Ryu, Do Hyong, Koh Graduate Student, and Dugan Um. 2011. Usability Evaluation of Touchless Mouse Based on Infrared Proximity Sensing. *Journal of Usability Studies* 7, 1 (2011), 31–39.

[78] Marwa E. Saleh, Abdelmgeid A. Aly, and Fatma A. Omara. 2016. Data Security Using Cryptography and Steganography Techniques. *International Journal of Advanced Computer Science and Applications* 7, 6 (32 2016). https://doi.org/10.14569/IJACSA.2016.070651

[79] Anirban Sengupta and Mahendra Rathor. 2020. Structural Obfuscation and Crypto-Steganography-Based Secured JPEG Compression Hardware for Medical Imaging Systems. *IEEE Access* 8 (2020), 6543–6565. https://doi.org/10.1109/ACCESS.2019.2963711

[80] Ashitha Shaji, Mariya Stephen, Seethal Sadanandan, S. Sreelakshmi, and K. A. Fasila. 2019. Phishing Site Detection and Blacklisting Using EVCS, Steganography Based on Android Application. 1384–1390. https://doi.org/10.1007/978-3-030-03146-6{_}162

[81] B Siregar, H Gunawan, MA Budiman, and Sulindawaty. 2019. Message Security Implementation by Using a Combination of Hill Cipher Method and Pixel Value Differencing Method in Mozilla Thunderbird Email Client. *Journal of Physics: Conference Series* 1255, 1 (8 2019), 012034. https://doi.org/10.1088/1742-6596/1255/1/012034

[82] Daniela Stanescu, Mircea Stratulat, Bogdan Ciubotaru, Dan Chiciudean, Razvan Cioarga, and Mihai Micea. 2007. Embedding data in video stream using steganography. *SACI 2007: 4th International Symposium on Applied Computational Intelligence and Informatics - Proceedings* (2007), 241–244. https://doi.org/10.1109/SACI.2007.375518

[83] Mansi S. Subhedar and Vijay H. Mankar. 2014. Current status and key issues in image steganography: A survey. *Computer Science Review* 13-14, C (11 2014), 95–113. https://doi.org/10.1016/J.COSREV.2014.09.001

[84] Xinlei Wang, Jianqing Zhang, Eve M. Schooler, and Mihaela Ion. 2014. Performance evaluation of Attribute-Based Encryption: Toward data privacy in the IoT. *2014 IEEE International Conference on Communications, ICC 2014* (2014), 725–730. https://doi.org/10.1109/ICC.2014.6883405

[85] Jiahui Wu, Xiaofeng Liao, and Bo Yang. 2018. Image encryption using 2D Hénon-Sine map and DNA approach. *Signal Processing* 153 (12 2018), 11–23. https://doi.org/10.1016/J.SIGPRO.2018.06.008

[86] Lizhi Xiong and Yunqing Shi. 2018. On the Privacy-Preserving Outsourcing Scheme of Reversible Data Hiding over Encrypted Image Data in Cloud Computing. *Computers, Materials & Continua* 55, 3 (1 2018), 523–539. https://doi.org/10.3970/cmc.2018.01791

[87] Shuying Xu, Ji-Hwei Horng, Ching-Chun Chang, and Chin-Chen Chang. 2022. Reversible Data Hiding with Hierarchical Block Variable Length Coding for Cloud Security. *IEEE Transactions on Dependable and Secure Computing* (2022), 1–14. https://doi.org/10.1109/TDSC.2022.3219843

[88] Mehmet Yamac, Mete Ahishali, Nikolaos Passalis, Jenni Raitoharju, Bulent Sankur, and Moncef Gabbouj. 2021. Multi-Level Reversible Data Anonymization via Compressive Sensing and Data Hiding. *IEEE Transactions on Information Forensics and Security* 16 (2021), 1014–1028. https://doi.org/10.1109/TIFS.2020.3026467

[89] Yang Yang, Xingxing Xiao, Xue Cai, and Weiming Zhang. 2019. A secure and high visual-quality framework for medical images by contrast-enhancement reversible data hiding and homomorphic encryption. *IEEE Access* 7 (2019), 96900–96911. https://doi.org/10.1109/ACCESS.2019.2929298

[90] L. Zhang, X. Hu, W. Rasheed, T. Huang, and C. Zhao. 2019. An Enhanced Steganographic Code and its Application in Voice-Over-IP Steganography. *IEEE Access* 7 (2019), 97187–97195. https://doi.org/10.1109/ACCESS.2019.2930133

[91] Xiao-Guang Zhang, Guang-Hong Yang, and Xiu-Xiu Ren. 2022. Network steganography based security framework for cyber-physical systems. *Information Sciences* 609 (9 2022), 963–983. https://doi.org/10.1016/j.ins.2022.07.081

[92] Xin Zhou and Xiaofei Tang. 2011. Research and implementation of RSA algorithm for encryption and decryption. *Proceedings of the 6th International Forum on Strategic Technology, IFOST 2011* 2 (2011), 1118–1121. https://doi.org/10.1109/IFOST.2011.6021216

Appendices

Appendix A LITERATURE SEARCH RESULTS (JOURNAL ARTICLES)

Table 7. Journal papers focussing on Application Domain (bold) and (optionally) Technological Domain

Paper Details		Domain Details		
Ref.	**Objective**	**Application Domain**	**Technological Domains**	**Functionalities**
[88]	Two-tiered video surveillance: anonymisation of sensitive parts with separate decode authorization levels.	**Government**	Internet of Things	Smart monitoring, Anonymisation
[76]	Implementation of E2E verifiable online voting system using voting receipts.		Web Applications	Voting
[57]	Securing patient details and images during transmission.	**Medical**	N/A[15]	Healthcare data transmission
[62]	Embedding Electronic Patient Records (EPR), watermark and checksum in medical images using RDH.		N/A[15]	Healthcare data transmission
[89]	Performing embedding and encryption of privacy sensitive data into medical images client-side, and storing in the cloud using RDH.		Cloud Computing	Healthcare data transmission and storage, Privacy protection
[34]	Securing transmission of signals of remote Electrocardiogram (ECG) monitoring systems.		Internet of Things	Remote Patient Monitoring
[22]	Encrypt and hide diagnostic text data in medical images using RDH.		Internet of Things	Healthcare data transmission
[42]	Securing patient details during transmission for remote diagnosis by hiding them inside (Non-Region of Interest) NROI medical images using RDH.		N/A[11]	Healthcare data transmission, DICOM
[45]	Securing transmission of DICOM images.		N/A[15]	Healthcare data transmission, DICOM
[13]	Securing transmission of Electronic Patient Information (EPI) using RDH.		N/A[15]	Healthcare data transmission
[79]	Securing a JPEG at hardware level used in medical image transmission from counterfeiting, cloning and Trojan insertion.		N/A[15]	Healthcare data tampering protection
[49]	Securing transmission of vehicle diagnostics (DoIP) and software updates (OTAs).	**Transportation**	Cloud Computing, Edge Computing	Vehicle diagnostics and updates
		End of Table 7		

Table 8. Journal papers focussing on Technological Domains (bold) and (optionally) recommended Application Domains.

Paper Details		Domain Details		
Ref.	**Objective**	**Application Domain**	**Technological Domains**	**Functionalities**
[86]	Protecting image data in cloud computing using RDH.	*Military*[14], *Cross-Domain*	**Cloud Computing**	Access Control, Privacy protection
[87]	A Reversible Data Hiding scheme for securing customer data storage using RDH.	*Medical*	**Cloud Computing**	Access Control
[9]	Operating on homomorphically encrypted images to securely handle data in the cloud using RDH.	*Medical, Military*[14]	**Cloud Computing**	Privacy Protection
[14]	Improving performance and confidentiality of big data transmissions using GPU.	*Energy, Medical, Finance*[12]	**Cloud Computing, Big Data**	Data transmission, *Healthcare data transmission*[12]

Continued on the next page

[11] There is no apparent involvement of a technology in the topic.

[12] Possible domains based on the technology used (incl. but not limited to) [65]

Table 8 (continued)

Ref.	Objective	Application Domain	Technological Domains	Functionalities
[91]	Secure communication over a covert channel in the measurements of a dynamic system.	*Cross-Domain*[14]	**Cyber-Physical Systems**	N/A
[7]	Applying combined Improving capacity of image steganography.	*Cross-Domain*	**Internet of Things**	Data transmission
[33]	Securing communication between IoT devices and the cloud using fog computing.	*Cross-Domain*	**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*[14]	**Internet of Things,** **Unmanned Aerial Vehicles**	Industry 5.0
[1]	Securing UAV image transmissions and classification of images.	*Cross-Domain*[13]	**Internet of Things,** **Unmanned Aerial Vehicles**	Industry 4.0
[10]	Hiding malicious applications in images to evade detection by Android anti-malware tools.	*Cross-Domain*	**Mobile Computing**	Malware detection, Malware development
[19]	Customizing security level of the use of NFC on a phone for authentication: a 2FA system.	*Entertainment, Finance*[14]	**Mobile Computing,** **Cloud Computing**	Access control
[5]	Hiding encrypted data in available audio files to protect it from unwanted access.	*Cross-Domain*	**Personal Computing**	Data storage

End of Table 8

[13] Similar to [36]

[14] Suggested by the authors.

Appendix B LITERATURE SEARCH RESULTS (CONFERENCE PAPERS)

Table 9. Conference papers focussing on Application Domain (bold) and (optionally) Technological Domain.

Paper Details		**Domain Details**		
Ref.	**Article**	**Application Domain**	**Technological Domains**	**Functionalities**
[63]	Two-Layer Secure Mechanism for Electronic Transactions	**Financial**	N/A[15]	Online payments
[53]	Secure Transaction System using Collective Approach of Steganography and Visual Cryptography		N/A[15]	Online payments, Privacy protection
[29]	Based on IoT Healthcare Application for Medical Data Authentication: Towards A New Secure Framework Using Steganography	**Medical**	Internet of Things	Healthcare data transmission, Privacy Protection
[23]	Secure Transmission and Repository Platform for Electronic Medical Images: Case Study of Retinal Fundus in Teleophthalmology		Web Apps	Healthcare data transmission and storage
[48]	Reversible Data Hiding Scheme during Encryption Using Machine Learning		Machine Learning	Healthcare data transmission

End of Table 9

Table 10. Conference papers focussing on Technological Domains (bold) and (optionally) recommended Application Domains.

Paper Details		**Domain Details**		
Ref.	**Article**	**Application Domain**	**Technological Domains**	**Functionalities**
[39]	Stagchain - A Steganography based Application Working on a Blockchain Environment	*Cross-Domain*	**Blockchain, Decentralized Cloud Computing**	Data storage
[58]	An Efficient Image Encryption Reversible Data Hiding Technique to Improve Payload and High Security in Cloud Platforms	*Cross-Domain*	**Cloud Computing**	Privacy Protection
[12]	Secure File Storage using Hybrid Cryptography	*Cross-Domain*	**Cloud Computing**	Data storage
[74]	Pairing-free CP-ABE based cryptography combined with steganography for multimedia applications	*Cross-Domain*	**Cloud Computing**	Data storage
[67]	Encryption, File Splitting and File compression Techniques for Data Security in virtualized environment	*Cross-Domain*	**Cloud Computing**	Data storage
[44]	Enhanced Cloud Security using Cryptography and Steganography Techniques	*Cross-Domain*	**Cloud Computing**	Data storage
[24]	Multilayer Technique to Secure Data Transfer in Private Cloud for SaaS Applications	*Cross-Domain*	**Cloud Computing**	SaaS
[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	*Cross-Domain*	**IPv6**	Node Protection
[17]	Blocksight: A mobile image encryption using advanced encryption standard and least significant bit algorithm	*Cross-Domain*	**Mobile Computing**	Data storage
[80]	Phishing Site Detection and Blacklisting Using EVCS, Steganography Based on Android Application	*Cross-Domain*	**Mobile Computing**	Phisihing prevention
[81]	Message Security Implementation by Using a Combination of Hill Cipher Method and Pixel Value Differencing Method in Mozilla Thunderbird Email Client	*Cross-Domain*	**Personal Computing**	Email
[71]	Secure Fusion of Crypto-Stegano Based Scheme for Satellite Image Application	*Cross-Domain*	**Satellite Imaging**	Data transmission

Continued on the next page

[15] There is no apparent involvement of a technology in the topic.

Table 10 (continued)

Ref.	Article	Application Domain	Technological Domains	Functionalities
[66]	Enhancing cyber security using audio techniques: A public key infrastructure for sound	*Cross-Domain*	**Voice Operated Systems**	Voice Recognition
[52]	Web authentication security using image steganography and AES encryption	*Cross-Domain*	**Web Applications**	Password Protection
[11]	Protecting User Credentials against SQL Injection through Cryptography and Image Steganography	*Cross-Domain*	**Web Applications**	Password Protection

End of Table 10

Appendix C SCHEMES AND CHARACTERISTICS (JOURNAL ARTICLES)

Table 11. Schemes used and characteristics of journal articles

Ref.	Steganographic algorithms	Steganography type	Cryptographic algorithms	Operation order	Advantages
[88]	Custom: obfuscation matrix in "obfuscated sensitive data"	Image (not reversible)	CS (Compressed Sensing)	encrypt, hide stego key, encrypt	No need for secret channel, robust against cipher attacks
[76]	F5 with DCT and Huffman encoding	Image	PBKDF2 with HMAC-SHA1, SHA1PRNG, (k,n)-threshold scheme	encrypt, hide	Application in user receipt verification
[57]	LSB	Image (not reversible)	PRNG using Chaotic 2D-Henon map	hide, encrypt	Two patients' data in one signal, high data hiding capacity
[62]	EPR, ISBS	Image (reversible)	Chaotic encryption	encrypt, hide	Fragile nature, tamper verification, high data hiding
[89]	Histogram-shifting based, adaptive PEE	Image (reversible)	Homomorphic based on Chaotic Map. Key generation using PLCM.	hide, encrypt	Minimal lesion area impact, high non-lesion area capacity
[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
[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
[42]	LSB-Based	Image (reversible)	RSA	encrypt, hide	No embedding key storage, robustness via ROI hash
[45]	3-LSB with DWT	Image (reversible, encrypted domain)	XOR Cipher	encrypt, hide	Higher encryption speed
[13]	LSB using dynamic key	Image (reversible, encrypted domain)	XOR Cipher	hide, encrypt	High capacity at maintained quality, immunity to under- and overflow
[79]	Custom	Hardware[16]	TRIFID Cipher	N/A	Low cost design
[49]	LSB using Fuzzy Edge Detection, normal LSB	Image (not reversible)	Modified RSA	encrypt, hide, hide	Data integrity maintenance
[86]	Custom	Image (reversible, encrypted domain)	ElGamal with homomorphic encryption and re-encryption	encrypt, hide	Re-encryption, errorless image recovery, specific data extraction order
[87]	LSB	Image (reversible)	Stream cipher with XOR	hide, encrypt	Superior embedding rate, entropy and MAE
[9]	Custom using rhombus pattern prediction	Image (reversible, encrypted domain)	Additive homomorphic encryption	encrypt, hide	Low computational complexity, high PSNR, quality decrypted image, capacity balance
[14]	LSB-based	Audio (not reversible)	S-DES	encrypt, hide	Confidentiality, robustness, low information loss, GPU speed enhancement
[91]	LSB in bit stream	Network	Linear encryption	encrypt, hide	No communication overhead, statistical undetectability, eavesdropping resistance
[7]	LSB-based with bit interchange method, and IPM + 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
[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

[16] Reversibility not applicable

Table 11 (continued)

Ref.	Steganographic algorithms	Steganography type	Cryptographic algorithms	Operation order	Advantages
[36]	Multilevel 2D-DWT with QBCO pixel selection	Image (not reversible)	Signcryption, ElGamal, Kernel Homomorphic	encrypt, hide	Lower computation time, lower MSEs
[1]	Multilevel 2D-DWT with CSO pixel selection	Image (not reversible)	Signcryption	encrypt, hide	Lower MSE, higher PSNR, higher CC, lower CT
[10]	LSB (PNG), DCT (JPEG)	Image (not reversible)	XOR cipher	encrypt, hide	Not detected by anti-malware software, encryption/steganography aids circumvention
[19]	LSB	Image (not reversible)	AES-256	encrypt, hide	Two-factor authentication acceptance, user security preference
[5]	3-LSB	Image (not reversible)	RSA	encrypt, hide	RSA asymmetric, less noise with 3-bits

End of Table 11

Appendix D EVALUATION METHODS (JOURNAL ARTICLES)

Table 12. Analysis or Evaluation Methods

Ref.	Analysis or Evaluation Methods
[88]	PSNR, SSIM
[76]	Steganography: size, RS analysis, BSM analysis. Usability tested: user acceptance
[57]	PSNR, MSE
[62]	Capacity, PSNR, bpp, SSIM. Salt & pepper noise. Additive White Gaussian Noise. Attacks: median filtering, lowpass filtering, weiner filtering, sharpening, histogram equalization attack, rotation attack
[89]	Steganograpy: bpp, PSNR, SSIM, NR-CDIQA, NR-ICDIQA. Cryptography: Key pace, histogram, correlation of adjacent pixels, absolute correlation coefficient of adjacent pixels, correlation coefficient between marked and encrypted images, Shannon entropy of encrypted images.
[34]	Probability of key being broken at different lengths. PRD, WWPRD. Doctors inspected ECGs.
[22]	PSNR, MSE, BER, SSIM, SC, CC
[42]	PSNR, MSE, bpp
[45]	Histogram, Entropy, CC (verical, horizontal, diagonal), Key sensitivity, encryption speed
[13]	PSNR, BER, bpp, CT
[79]	Steganography: PSNR, MSE
[49]	DoIP: Encryption time, embedding time, final image time, stego extract time, cipher extract time. SOTA: Same metrics. Slightly different for receiver side but it's all time-based
[86]	PSNR, bpp
[87]	MAE, bpp, pitch removal attacks, bit-plane removal attacks
[9]	PSNR, SSIM, BER, bpp, histogram, Entropy, Deviation from Ideality, CC, keyspace analysis, key sensitivity,
[14]	SNR, AD, AE, BPC, TP, Il, UER
[91]	X^2, KLD
[7]	X^2, HVS, MSE, PSNR, HA, SSIM, capacity in %
[33]	NCCC, entropy, NPCR, UACI, SSIM, MSE, PSNR, CT
[36]	MSE, PSNR, CT, CC
[1]	PSNR, MSE, CC, CT with UCM and AID datasets
[10]	PSNR, StegExpose (PNG), Stegdetect (JPEG)
[19]	Reliability: CA, CR. Validity: AVE. Behavioural Intention: SEM, Normalised X^2, goodness-of-fit (GFI), root mean square error (RMSEA), NFI, TLI, CFI.
[5]	Capacity, PSNR

End of Table 12