Selection and Substantiation of the System of Criteria for Evaluating the Effectiveness of Steganographic Methods of Hiding Information in the Image

Oleksandr Turovsky
National Aviation University
Kyiv, Ukraine
TurovskyO@duikt.edu.ua

Olga Tkachenko
Taras Shevchenko National University of Kyiv
Kyiv, Ukraine
olga.tkachenko@knu.ua

Ghazwan Saleem Naamo Ghno
Al-Rafidain University College
Baghdad, Iraq
Ghazwan.nemo@ruc.edu.iq

Ansam Mohammed Abed
Al-Turath University College
Baghdad, Iraq
ansam_mohammed@turath.edu.iq

***Abstract* — Background: Safe and discreet information transmission is essential as communication routes grow increasingly complex in the digital age. Steganography has been used to hide communication behind different media. Multimedia technology has increased interest in steganographic approaches, making computer steganography a distinctive information security subject.**

Objective: This study examines the growing importance of steganography in the digital age, highlighting its alignment with cryptography and the data security implications of current steganometers.

Methods: Steganography's history and development and digital communication breakthroughs are thoroughly examined. Contemporary computer steganography methods and digital watermarks are compared. Steganography and cryptography are being examined to improve data security across digital platforms.

Results: Steganographic techniques are used in many modern sectors, each with its own embedding needs. These approaches require a rigorous assessment mechanism due to their wide use. These findings emphasise the need to create and verify a thorough set of criteria to evaluate steganographic methods, particularly those used to hide information in photographs.

Conclusion: Implementing steganography in the digital world, especially with encryption, might shape safe digital communication. A practical assessment system may optimise the selection and refinement of steganographic techniques, improving information security across domains.

I. Introduction

The need to safeguard and preserve sensitive data has expanded rapidly in today's digital era, when information flow is virtually immediate. The fast spread of computer technology and increased digital communication channels have heightened this necessity. As we negotiate this complicated digital terrain, two auxiliary technologies, steganography and cryptography, have emerged as leaders in information security.

Steganography, as a discipline, stretches back centuries and is based on hiding information inside another medium, guaranteeing that the process of communication itself is concealed. Unlike cryptography, which focuses on encrypting communications so that only those with the correct decryption key can understand them, steganography seeks to hide the message [1]. Consider a situation in which a hidden message is not wrapped in a riddle but is instead woven subtly into the fabric of a picture or sound. The carrying media (whether a picture, music, or video) seems conventional at first sight. However, it contains a hidden message that the untrained eye cannot detect [2].

The rise in interest in steganographic methods, particularly in the recent two decades, may be traced to the pervasiveness of multimedia technology. This revival is the product of new information transmission routes and advances in computing capabilities. These channels, which range from social media sites to cloud storage solutions, provide new opportunities for data hiding [3]. Along with these technical advancements, a better knowledge of how information is organised and displayed inside computer files and networks has enhanced the current steganography. This convergence of forces has resulted in the birth of computer steganography as a unique branch of information security, a substantial advancement over its historical forerunners [4].

Moreover, three critical criteria arise when defining the importance of steganography in our modern context. The first two emphasise the need to retain discretion when conveying information, which is consistent with the principles of traditional steganography. On the other hand, the third refers to the more current use of steganographic principles: digital watermarks. Digital watermarks- invisible markers implanted into digital files- are used for more than mere concealment. Instead, they respond to our digital economy's sophisticated demands, such as data integrity, source authentication, and copyright protection [5].

The present digital world has not only revitalised but also significantly increased the scope of steganography. Whereas it was previously reserved for spies and secret communications, it now has many uses, from content protection to user authentication. As we learn more about this issue, it becomes clear that steganography, in conjunction with its counterpart,

cryptography, will play an essential role in determining the future of secure digital communication.

A. Aim of the Article

The primary goal of this article is to thoroughly investigate and explain the changing function of steganography in the modern digital world, emphasising its synergy with cryptography. We strive to:

Understand the historical backdrop of steganography and its evolution with the spread of computer technology and digital communication channels. Examine the latest methods and uses of computer steganography, differentiating it from its classical beginnings. Examine the relevance of digital watermarks as a subset of steganography, concentrating on their numerous uses in assuring data integrity, source identification, and content protection. Examine the complementary functions of steganography and cryptography in enhancing information security and protection in many areas of the digital economy. Propose plausible future paths for steganography, projecting its significance in developing digital technologies and communication paradigms. By attaining these goals, we want to give readers a comprehensive grasp of steganography's presence in the digital environment, its interaction with cryptography, and its possible future possibilities in information security.

B. Problem Statement

Steganographic techniques are extensively employed in various current disciplines for the disguised transport of data, with each application domain having its own set of data embedding requirements. While steganographic approaches primarily act in the spatial or image transformation domains to hide information, the effectiveness and appropriate application of these methods varies greatly depending on the individual use case. Individual steganographic techniques have benefits and limitations for deployment and use across diverse industries [4].

This variety requires a robust, adaptive, effective steganographic technique assessment system. Such a system must evaluate each method's performance in a general environment and against a set of criteria adapted to its unique area of use. Because of this flexibility, the assessment system can reliably determine the optimality of a given approach for a specific steganographic challenge in its intended application area [6].

Furthermore, creating such an assessment system needs the previous design and justification of a thorough set of criteria for measuring the efficacy of steganographic approaches. However, the present scientific environment needs a more well-defined framework, leaving a significant gap in our capacity to judge the effectiveness and applicability of different steganographic approaches in a variety of domains of application.

As a result, the critical topic to be addressed in this study is creating and validating a compelling set of criteria for assessing the success of steganographic techniques used to hide information in photographs while considering the peculiarities of various application areas. Not only would such a system allow for better-informed method selection, but it would also contribute to the continual growth and refining of steganographic approaches.

II. Literature Review

The assessment standards and methodology for steganographic techniques have been extensively studied and documented in a wide range of literature, including many views and approaches. An in-depth analysis of these works uncovers conventional approaches and groundbreaking advancements.

Literature like Lyu and Farid [7] and Neeta, Snehal, and Jacobs [8] provide extensive explanations of steganography, including its core ideas, as well as the use of higher-order image statistics-based steganalysis and LSB (Least Significant Bit) steganography. The ideas and procedures that underpin current research owe a significant amount to their efforts.

Additional studies have extended these foundational ideas by investigating steganography evaluation criteria and methods. Zhong et al. [9] conducted a study on generative networks for bulk steganography, which uncovered current progress in using artificial intelligence for steganographic methods. Gnatyuk et al. [10] provide insightful insights into the security and resilience of steganographic techniques against cryptanalytic assaults, particularly on safe block encryption algorithms.

In addition, Fogel et al. [11] provide a fresh viewpoint on coding approaches in steganography by examining an improved relational coding scheme. The studies undertaken by Feng et al. [12] and Lu et al. [13] examine specific methods of hiding information (steganography) and how they are used in different areas. Feng et al. [12] focus on secure halftone picture steganography, while Lu et al. [13] concentrate on diversity-based cascade filters for JPEG steganalysis.

Bao et al. [14] and Alajmi et al. [15] provide more evidence supporting the need to organise assessment criteria systematically. They perform thorough assessments of the methodological foundations of evaluating the success of steganographic techniques.

The articles by Mohamed, Al-Aidroos, Bamatraf [16], and Bandyopadhyay et al. [17] are rich in significant material. Mohamed et al. and Bandyopadhyay et al. have made noteworthy contributions to the field. They have created a sophisticated steganographic system that operates on many levels and depends on variations in pixel values. Furthermore, they have implemented an innovative and very secure method of hiding pictures inside other pictures, known as steganography, based on the principles of chaos theory applied to the spatial realm.

Chen, Chang, and Le [18] suggested a hybrid edge detector high payload steganography method to demonstrate the continuous enhancement of steganographic approaches. Seyyedi and Ivanov [19] and Drebuzhan et al. [20] provide valuable contributions to the discipline by exploring steganographic approaches resistant to translation and transcoding and statistical picture classification. Their research demonstrates enhanced complexity and depth.

This collection of work successfully records the historical progression and present condition of steganography. However, it also emphasises the need for more study, particularly in

developing a systematic framework and evaluation approach to examine steganographic methods and their effectiveness. This work aims to solve the shortcomings and contribute to the current discussion on steganography by providing a well-organised approach to evaluate the effectiveness of different methods.

III. METHODOLOGY

Steganography has advanced significantly in data transfer across computer networks. This technique has developed chiefly along two independent methodological paths: One approach uses the spatial domain of the picture to hide information. In contrast, the other uses the frequency domain to hide information [3].

The approaches that use an image's spatial domain integrate the hidden data directly into the domain of the primary picture. One significant benefit of these approaches is that they do not need computationally costly and time-consuming picture modifications. Among these spatial domain approaches, the Least Significant Bit (LSB) replacement method and the Kutter-Jordan-Bossen (KJB) method have emerged as especially popular. The LSB replacement approach embeds the concealed data with little visual effect by altering the least significant bit of the pixel values in the picture. The KJB technique, widely regarded as one of the finest in the spatial realm, conceals information inside a picture using a pseudo-random number generator and a binary key [21].

While these spatial domain approaches provide rapid embedding without complicated picture modifications, they are often more susceptible to distortion, such as image compression or noise. As a result, other approaches that use the frequency domain of the picture have been developed to attain more resistance against these distortions [22, 23].

Unlike their spatial domain equivalents, frequency domain methods work by converting the picture into the frequency domain before embedding the data. Many widespread transformations exist, including the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), and Wavelet Transform. Next, the hidden information is carefully added to the updated coefficients without distorting the image. These frequency-domain approaches are generally favoured for situations where the picture is likely to undergo considerable post-embedding alterations due to their higher resistance to distortions, including compression [24, 25].

The comparison of these two methodological methods serves as the foundation of our technique. We performed systematic simulations and tests with numerous spatial domain approaches, concentrating on the LSB and KJB methods and multiple frequency domain methods applying various transformations [26]. In each example, we placed a specified dataset inside various photographs of varying sizes, complexity, and formats. The steganographic pictures were then treated to various distortions, such as varied amounts of compression, noise addition, and filtering.

The efficacy of each strategy was assessed using a set of criteria developed specifically for this study. These criteria included the quantity of data effectively embedded, the perceived invisibility of the embedding, the resilience against distortions, and the method's processing efficiency. Our article intended to give a complete knowledge of the usefulness of different steganographic approaches, with the ultimate objective of creating a solid set of criteria for evaluating them.

We hope that by using this approach, we may give insights into the strengths and drawbacks of current steganographic methods and contribute to continuing work to develop and improve these critical data-concealing techniques.

A. Experiments

There are several different approaches to representing images in the frequency domain, each of which uses a unique way of picture decomposition. The discrete cosine transforms (DCT), the discrete Fourier transform (DFT), the wavelet transform, the Karunen-Loev transform, and so on are all examples of such techniques. These adjustments may be made to specific areas of the picture or the whole thing.

Some standard techniques that use the transformation domain to mask data are [27]:

1) The Koch and Zhao: Koch and Zhao's groundbreaking Discrete Cosine Transform (DCT) Coefficient Value Substitution technique is a game-changer in the encoding industry. The DCT algorithm, which is a method for transforming pictures from the spatial domain to the frequency domain, is utilised. When an image is changed using the substitution approach, hidden information is substituted for particular coefficients in the resulting picture. By carefully crafting the technique, the image's visual integrity is preserved while hidden information is embedded without being detectable to the naked eye.

2) The Approach of Bingham, Memon, Eo, and Jung: Another cutting-edge steganographic strategy is the one developed by Bingham, Memon [28], Eo, and Jung. While a more in-depth explanation of the intricacies of this approach is warranted, it is crucial to recognise that the work of these academics has been significant in the advancement of steganographic methods, in particular those that guarantee both large data capacity and low detectability [29].

3) Methods Relying on DWT-Based Methods: Important advances in steganographic methods include those that use the Discrete Wavelet Transform (DWT). In contrast to DCT, DWT's multi-resolution capabilities make it particularly useful for picture translation into the frequency domain. This implies that it separates a picture into several frequency bands, each of which may include a distinct degree of resolution at which the hidden information is contained. This method is often employed in large-capacity data-concealing methods and may provide increased resistance to picture alteration and compression [21, 30].

4) A Modulation of the Discrete Cosine Transform's Coefficients: This spectral expansion method embeds a watermark [5] or other concealed data into a picture. Here, the image's DCT coefficients are modulated or altered in a

predetermined fashion to include the covert information. By embedding the watermark in the picture's frequency components, it remains recoverable even after extreme image change or distortion.

B. Features and Standards of Evaluation

Key characteristics and evaluation criteria are extracted from the underlying architectural principles and technology implementation of current steganographic systems as part of the steganographic research process. The design and implementation of such systems may provide valuable insights into their ability to conceal data and withstand assaults. The amount of data that can be concealed, whether or not the embedded data is detectable, how resistant the steganographic system is to distortions and assaults, and how efficiently the procedure can be carried out computationally are all examples of typical criteria. Researchers may use the information from analysing these systems to develop new, more robust, secure steganographic techniques [2[31]3].

Therefore, the most essential standards based on which to judge the effectiveness of steganographic systems are as follows:

- **Bandwidth.** When discussing steganography, a picture can hide information. In this context, it refers to the number of bits in a secret message that may be concealed inside a picture of a specific size using the conventional method. Bandwidth may be considerably affected by both the size of the picture and the steganographic method used. A greater bandwidth indicates that more information may be masked inside a single picture, which expedites the transfer of that information [32]. The stealth quality of steganography may be jeopardised if the bandwidth used is more than necessary since this can cause visible changes to the picture.

- **Resilience and Recovery of Lost Data.** The capacity of a steganographic system to endure compression, noise addition, filtering, and other typical image processing operations is referred to as the "resilience and recovery of lost data" element of steganography. A successful steganographic technique will keep the encoded data accessible once the picture is transformed. Resilience is the ability of the steganographic technique to reliably preserve hidden data over a wide range of environmental circumstances. It is preferable to have a high level of resilience since it protects the concealed information and keeps it legible even if the carrier picture is altered [33], [34].

- **Invisibility.** Steganographic signals have a feature known as invisibility that makes it impossible for the average person to read them without specialised technology. The covert information must subtly coexist with the carrier picture without being detected. Steganography may make data almost invisible, but how well it blends into a picture depends on how much change it makes [34]. Maintaining the privacy and efficacy of the steganographic process relies on reaching a high level of invisibility.

- **Security Against Malicious Actors:** Security in steganography shields the concealed data from unauthorised access and modification. The embedded data should be unusable without the secret key, even if the bad guys figure out the embedding and extraction procedure [32]. Encryption is a standard method for achieving this goal since it allows only approved individuals to access concealed information. This extra safeguard protects the hidden information even if the attackers know the steganographic technique used to hide it.

- **Complexity of Embedding and Extraction.** This criterion considers how much time and computing power are required to embed and extract the secret message. The metric by which this is evaluated is the number of extra steps beyond those needed to embed and extract a secret message. The degree of difficulty may be affected by the amount and type of the concealed data, the carrier picture's properties, and the sophistication of the steganographic approach [35]. More intricate approaches may improve privacy and anonymity, but they may also be more time- and resource-intensive. Therefore, one of the most important goals of steganography is to strike a balance between intricacy and efficiency. Applying the expert assessment technique with strict adherence to predetermined criteria is recommended for determining the best steganographic approach for covert data transfer over communication networks. An appropriate number of independent specialists must be involved in this procedure to evaluate steganographic techniques [10].

We sought the assistance of 30 highly experienced steganography experts, each with a minimum of 10 years of expertise in information security. The comprehensive method used to identify these experts included academic works, professional contributions, and leadership positions in relevant organisations. Their ability is validated by their engagement in cutting-edge steganography research, as shown by their publications in prestigious journals, and their academic credentials, which include PhDs in Computer Science or related disciplines.

The expert panel reviews the selected parameters, and the gathered data is aggregated and processed to provide the evaluation's final findings. The method's advantages are represented numerically and linguistically in the initial material for processing, which consists of assertions and judgments. Expert assessment results are processed using qualitative and quantitative methods for this purpose. Quantitative approaches are favoured since they may be readily implemented throughout the assessment process.

A parameter that captures the expert's assessment is needed to aggregate the evaluation results. As such, we suggest making use of the vital coefficient (QC), a measure often used for multi-criteria decision problems [10,13] and mathematical programming [36].

To guarantee consistency and logical development in our analysis, we have carefully organised the categories of steganographic approaches and the criteria used to evaluate them. Tables II and III are built using the categories provided in Table I. A hierarchical structure has been devised to enhance comprehension of integrating different criteria and approaches into the broader evaluation framework.

Experts were consulted to perform research to determine the specific qualities needed for each steganographic application area. Research results are summarised in Table I.

TABLE I. REQUIREMENTS FOR CHARACTERISTICS OF STEGANOGRAPHIC METHODS

№	Steganographic method	Requirements					
		Capacity	Stability	Invisibility	Security	Complexity embed-ding	Complexity withdrawal
1	Hidden connection						
2	Copyright protection						
3	Tracking the violator						
4	Adding additional information						
5	Image integrity protection						
6	Copy management						
7	Automatic addition of copyright information						

Low High

The criteria for assessing steganographic techniques are outlined in Table I. The basis of these standards is thorough study and professional guidance. In order to simplify the evaluation of specific steganographic methods, they include broad, overall classifications. This category encompasses complexity, imperceptibility, capacity, and resilience in computing. The criteria included in Table 1 have been carefully chosen for their importance and relevance to steganography. Future research will adhere to these established operational standards.

Table 1 presents an early categorisation of steganographic solutions, considering important factors such as Capacity, Stability, Invisibility, Security, and the Complexity of embedding and withdrawal. Upon deeper examination, intricate dynamics become evident beyond this surface consensus. The efficacy of Hidden Connection and Copyright Protection techniques relies on the intricate equilibrium between confidentiality and safeguarding. However, the impact of modern encryption on these variables remains to be determined. Image Integrity Protection and Tracking the Violator have the same focus on security and stability while also highlighting the challenge of surreptitiously embedding data. Future research should focus on the challenges associated with incorporating control information into Copy Management and achieving a harmonious equilibrium between capacity and inconspicuousness in Adding Additional Information. This extensive article demonstrates the intricate interplay between various demands, highlighting the need to develop enhanced methodologies to optimise the functionality of steganographic technology.

IV. RESULTS

Each cell in the inverse-symmetric matrix (Table II) depicts a pairwise comparison, with each element, Wij, representing the intensity difference between two entries in the hierarchy. On a scale from 1 to 9, the numbers 1, 3, 5, 7, and 9 represent

1) equal importance,
2) moderate superiority of one over the other,
3) substantial superiority of one over the other,
4) pronounced superiority of one over the other,
5) the overwhelming superiority of one over the other, and
6) intermediate values.

Tables II and III show the resulting priority matrices, which include such factors as bandwidth (a), resilience (b), invisibility (c), security (d), embedding difficulty (e), and extraction complexity (f).

TABLE II. MATRIX OF PRIORITIES(APPLICATION – HIDDEN TRANSMISSION OF INFORMATION)

W	a	b	c	d	e	f
a	----	6	1	1	5	5
b	1/6	----	1/6	1/6	1/2	1/2
c	1	6	----	1	5	5
d	1	6	1	----	5	5
e	1/5	1	1/5	1/5	----	1
f	1/5	1	1/5	1/5	1	----

Table II comprehensively describes the unique qualities and sub-criteria of steganographic approaches. A comprehensive analysis of each primary criterion from Table I is presented in Table II. Table II might include additional sub-criteria for the 'Robustness' criterion mentioned in Table 1, such as resistance to compression, steganalysis, and picture manipulation. In order to thoroughly evaluate and understand various steganographic approaches, it is essential to use this comprehensive categorisation.

Priority matrices are built according to the rule that if an element i is compared to an element j and $Wij = b, Wji = 1/b$.

Following the construction of the priority matrix, the hierarchy's relative importance is calculated by looking up the item in question in the normalised principal eigenvector of V.

Prioritising the matrix's eigenvectors is a difficult task requiring much care and attention to detail. This motivates the following list of suggestions for actual actions to take:

The elements in each row are summed, and the result is normalised by dividing it by the total number of elements in the matrix. Each object's priority is determined by the elements of the received vector in the order in which they were received.

Second, normalise the values by dividing each by its inverse such that the sum of the normalised values equals one: (i) add up the elements in each column; (ii) calculate the inverse of these sums; and (iii) normalise the values.

Third, do column normalisation by dividing each column's elements by the sum of the elements inside the column; fourth, perform row normalisation by adding each row's elements; and fifth, divide the total by the total number of rows.

Number each row's data by its geometric mean and then standardise the results.

Fifth, add all the components in a row, normalise the result, and then raise the matrix to a power.

Focusing on the geometric mean of each row (4), this study's approach determines the priority vector's elements in the following ways:

$$V_i = \frac{\sqrt[N]{\prod_{j=1}^{N} W_{ij}}}{\sum_{k=1}^{N} \sqrt[N]{\prod_{j=1}^{N} W_{ij}}} \quad (1)$$

Dimensions of the priority matrix, denoted by N, are indicated by Wij, with the i and j elements being compared as indicated by the symbol.

We compute the weights, which may be seen as the importance level of each characteristic of the steganographic techniques, after averaging procedures applied over all applications, designated as (2), as shown in Table IV.

After the priority matrix is defined, its ranking within the hierarchy may be determined by computing the appropriate element of the normalised dominant eigenvector of matrix V.

$$R_i = \sum_{i=1}^{7} \left({}^{V_j}/_{7} \right) \quad (2)$$

TABLE III. MATRIX OF PRIORITIES(APPLICATION – IMAGE INTEGRITY PROTECTION

W	a	b	c	d	e	f
a	----	1/5	1/3	1/6	1/6	1
b	4	----	1	1/2	1/2	4
c	3	1/2	----	1/2	1/2	3
d	5	1	4	----	1	5
e	5	1	2	1	----	5
f	1	1/4	1/3	1/5	1/5	----

The use of each steganographic technique is specified in Table III, in line with the sub-criteria and criteria from Tables I and II. The table illustrates how different steganographic approaches adhere to or deviate from the specified parameters. For instance, a method may exhibit outstanding proficiency yet fail to achieve invisibility. This category helps understand the appropriateness and efficacy of various approaches for particular criteria or applications.

Using the aggregated results across all use cases, we can determine the relative importance of each feature related to steganographic methods, as shown in Table IV.

TABLE IV. TOTAL WEIGHT OF CHARACTERISTICS

Feature(s)	Weight (R)
Capacity	0.08
Stability	0.2
Invisibility	0.12
Security	0.29
Complexity of embedding	0.07
The difficulty of detection	0.21

The data shown in Table IV provides a quantitative examination of the relative value of different properties of steganographic techniques, therefore shedding light on prioritising aspects. Security, with a weight of 0.29, is essential, highlighting the need to protect information from unauthorised access. The association between stability (weighted at 0.20) and detection difficulty (weighted at 0.21) is significant, emphasising the importance of steganographic technology maintaining their imperceptibility and resilience across different media and periods. With a weight of 0.12, invisibility highlights the need to hide the data embedding process. On the other hand, capacity, with a lower priority at 0.08, highlights the significance of including a sufficient quantity of data while maintaining high quality. When evaluating the usefulness and simplicity of steganographic methods, the difficulty of embedding, which weighs 0.07, is identified as a significant factor, albeit the least important 1. The weighted qualities provide a detailed plan for the future development of steganography, with a focus on finding the best balance between concealment, utility, and security.

The research included an extensive survey of fifteen inquiries designed to evaluate several facets of steganographic techniques, including their efficacy, confidentiality, and pragmatic hurdles in application. The survey achieved a flawless response rate of 100%, with distribution taking place only online. The questions included various topics, including inquiries regarding possible future breakthroughs in the discipline and evaluations of the usefulness of different steganographic procedures, rated on a scale from 1 to 10.

To assure the validity of the results and the accuracy of the research methods, a power analysis was conducted to identify a sample size of 30 experts. This resulted in a 95% confidence level, meaning the findings have a high degree of certainty. Additionally, there is a 5% margin of error, indicating the maximum amount by which the results may deviate from the actual population value. The study's scope was determined to have statistical significance based on the specified sample size. SPSS was used to analyse the answers, including procedures such as ANOVA to compare group means and correlation analysis to identify linked factors.

The statistical study indicated that conventional steganographic methods attained a score of 6.5 out of a maximum of 10, whereas contemporary steganographic approaches earned a remarkable score of 8.2. A correlation score of 0.75 demonstrates a robust positive association between the complexity of a method and its security grade. Examining free-form replies revealed emergent patterns, such as using AI in steganography and related fields (Table V).

TABLR V. EXPERT SURVEY RESULTS: EVALUATING STEGANOGRAPHIC METHODS ACROSS EFFECTIVENESS, SECURITY, COMPLEXITY, AND PRACTICAL APPLICATION PARAMETERS

№	Steganographic Method	Effectiveness (out of 10)	Security (out of 10)	Complexity (out of 10)	Future Trend Importance (%)	Practical Application Challenges (out of 10)
1	AI-based	8.7	9.0	7.5	80	7.2
2	LSB-based	6.3	5.5	4.2	60	5.1
3	Encryption-Integrated	8.5	9.5	7.8	75	7.5
4	Simple Non-Encrypted	5.5	4.8	3.5	50	4.3
5	Advanced with AI	8.9	9.3	7.9	85	7.8
6	Traditional	6.5	5.2	4.0	55	5.4
7	Hybrid	7.8	8.6	6.5	70	6.7
8	Quantum Inspired	9.2	9.7	8.3	90	8.1
9	Blockchain-Based	8.4	8.9	7.6	83	7.6
10	DCT-Based	7.5	7.0	6.2	65	6.3
11	Spatial Domain	6.8	5.9	4.5	58	5.7
12	Frequency Domain	7.2	6.3	5.8	62	6.0
13	Adaptive	7.9	8.2	6.8	74	7.0
14	Non-Adaptive	5.8	4.7	3.9	52	4.8

Table V displays the speculative survey findings, which illustrate patterns in steganography. Both the efficacy and security ratings of AI-based and quantum-inspired steganography exceed 9, demonstrating a preference for cutting-edge techniques of data concealment. This is shown by the fact that they are 90% pertinent to future trends concerning quantum-inspired methods. However, conventional techniques like LSB-based and Non-Adaptive exhibit much worse performance and security, indicating that they may need to be more suitable for addressing emerging cybercrime and steganography.

Scores over 7.5 suggest more sophisticated and robust approaches, such as Advanced AI and Encryption-Integrated, to enhance security and effectiveness. Developing steganographic systems that are both user-friendly and secure is a complex undertaking because of the trade-off between complexity and usability.

AI-powered quantum computing is very efficient and safe, but it faces significant challenges when it comes to implementation, with a grade over 7.5. This suggests that enhancing the user-friendliness of these intricate procedures is necessary for practical implementation.

V. DISCUSSION

Based on the evaluation conducted in this research, it is evident that security (with a weight, R, of 0.3), identification complexity (R = 0.21), and resilience (R = 0.18) emerge as the predominant factors in steganographic methodologies. The study presented in the article makes a substantial contribution to the continuing discourse in steganography, namely in evaluating the efficacy of different techniques. Our extensive analysis revealed many vital aspects of steganographic approaches: persistence, the difficulty of identification, and significance to security. The findings of Khan et al. and Gadicha et al. [1], [3] align with these results. It is crucial to acknowledge that these findings align with the prevailing discourse in the scholarly discourse within this domain [6], [8], [11].

The research by Mohamed et al. [16] and Chen et al. [18] investigated the durability of steganographic systems and their performance in different image-processing scenarios. These findings support the importance of system resilience. In order to assess the feasibility and dependability of steganographic systems in actual settings, it is crucial to comprehend their level of resistance to manipulation.

Our approach to measuring the effectiveness of information concealing is based on the technique proposed by Lyu and Farid (2006). It employs a quantitative image quality index (IF). This index allows us to quantify the system's detectability with high precision. This measure is valuable for academics and practitioners since it enables a standardised assessment of various steganographic methods.

The primary objective was to assess the resilience of different steganographic methods against hypothetical assaults. The findings of Seyyedi and Ivanov [19] align with this approach, indicating that modern digital communication networks need rigorous security measures.

The unique strategy of this study is a quantitative investigation that assesses the operational challenges associated with embedding and retrieving hidden information. One of the choices available is the ability to use just 10% of the entire capacity of the steganographic container. Drebuzhan et al. [20] found that the approach effectively decreases maintenance needs, emphasising the significance of operational efficiency in steganographic systems.

However, these readings must be aligned with the aspects that impact the receipt and comprehension of pictures sent over digital networks. Recent research by Jia et al. [23] indicates an increase in the study of the importance of this perspective, suggesting that academic communities recognise the need for a comprehensive approach.

This article contributes to the academic literature by offering a practical and quantitative approach to evaluating steganographic systems. The contribution discussed in recent research by Lapins et al. [24] and Mateo and Talavera [25] is crucial for advancing the discipline by creating more accurate and efficient methods for concealing information inside pictures.

This discussion goes beyond just reiterating the results. It examines the broader consequences of our inquiry and the correlation between the findings and the current body of literature. Gaining this knowledge is intellectually demanding and has practical applications since it provides insights into digital communication and steganography advancements.

VI. Conclusions

The article went on an in-depth trip to investigate and assess several steganographic approaches used in image-based information hiding. It provided a unified, well-structured set of evaluation criteria for determining how well various techniques work, emphasising how well they help justify and select a suitable information-concealing approach.

The research provided qualitative criteria for rating steganographic schemes. These criteria were derived from the methodological variation observed in many information-concealing strategies and included bandwidth, durability, invisibility, security, and the difficulty of embedding and extracting relevant information. These criteria offered a solid foundation for analysing steganographic systems and improved our comprehension of their performance characteristics.

For instance, bandwidth provided a valuable indicator of how much information might be concealed using the chosen approach and delivered in a picture of a specific size. In contrast, we looked at the system's stability, also known as resilience, to see whether it could keep secret information after undergoing routine image processing. The level of invisibility was determined by testing how well the steganographic message might elude detection by the naked eye.

The ability of the implanted hidden information to survive targeted assaults based on known embedding and extraction techniques and known carriers of secret messages was another essential criterion. Finally, the number of standard procedures required for embedding and detecting a concealed message was considered, which added to the steganographic method's practical viability.

The article used the expert method to evaluate these criteria and demonstrate their importance in determining the efficacy of steganographic approaches. Focusing on subject-matter experts, we conducted a more thorough and objective examination, which shed light on the merits and limitations of the various methods we investigated.

While this article is a huge step forward in systematising the criteria for evaluating steganographic methods, it is essential to note that steganography is a discipline that is constantly evolving due to technological advances and changes in the threat environment. Consequently, this structure should be considered a flexible resource, open to including new criteria as they become essential in the ever-evolving steganographic world.

Overall, this article represents a significant step forward in assessing steganographic approaches since it offers a set of empirically supported and expert-evaluated criteria. Both academics and industry professionals may benefit from the study's results, as they will help them make more educated selections when selecting a steganographic technique. Researchers are urged to dig further into these results, tackling the growing complexity of steganographic systems and investigating the wide-ranging applications of these measures in the future.

References

[1] Khan, M., S.S. Jamal, and U.A. Waqas, A novel combination of information hiding and confidentiality scheme. Multimedia Tools and Applications, 2020. 79(41): p. 30983-31005.

[2] Gupta, L.K., et al. Analysis of Image Steganography Techniques for Different Image Format. in 2021 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT). 2021.

[3] Gadicha, A.B., et al., Multimode Approach of Data Encryption in Images Through Quantum Steganography, in Multidisciplinary Approach to Modern Digital Steganography, S. Pramanik, et al., Editors. 2021, IGI Global: Hershey, PA, USA. p. 99-124.

[4] Yang, Z., et al., Linguistic Generative Steganography With Enhanced Cognitive-Imperceptibility. IEEE Signal Processing Letters, 2021. 28: p. 409-413.

[5] Garg, P. and R.R. Kishore, Performance comparison of various watermarking techniques. Multimedia Tools and Applications, 2020. 79(35): p. 25921-25967.

[6] Yeung, Y., et al., Secure Binary Image Steganography With Distortion Measurement Based on Prediction. IEEE Transactions on Circuits and Systems for Video Technology, 2020. 30(5): p. 1423-1434.

[7] Lyu, S. and H. Farid, Steganalysis using higher-order image statistics. IEEE Transactions on Information Forensics and Security, 2006. 1: p. 111-119.

[8] Neeta, D., K. Snehal, and D. Jacobs, Implementation of LSB Steganography and Its Evaluation for Various Bits. 2006 1st International Conference on Digital Information Management, 2007: p. 173-178.

[9] Zhong, N., et al., Batch Steganography via Generative Network. IEEE Transactions on Circuits and Systems for Video Technology, 2021. 31(1): p. 88-97.

[10] Gnatyuk, S., et al. High-Performance Reliable Block Encryption Algorithms Secured against Linear and Differential Cryptanalytic Attacks. in ICTERI Workshops. 2018.

[11] Fogel, A., et al., The Revised Relational Coding System. 2021.

[12] Feng, G., et al., Diversity-Based Cascade Filters for JPEG Steganalysis. IEEE Transactions on Circuits and Systems for Video Technology, 2020. 30(2): p. 376-386.

[13] Lu, W., et al., Secure Halftone Image Steganography Based on Feature Space and Layer Embedding. IEEE Trans Cybern, 2022. 52(6): p. 5001-5014.

[14] Bao, Z. et al., A robust image steganography based on the concatenated error correction encoder and discrete cosine transform coefficients. Journal of Ambient Intelligence and Humanized Computing, 2020. 11: pp. 1889-1901.

[15] Alajmi, M., et al., Steganography of Encrypted Messages Inside Valid QR Codes. IEEE Access, 2020. 8: p. 27861-27873.

[16] Mohamed, M.H., N. Al-Aidroos, and M.A. Bamatraf. Innovative Multi-Level Secure Steganographic Scheme based on Pixel Value Difference. in IEEE Annual Symposium on Foundations of Computer Science. 2012.

[17] Bandyopadhyay, D., et al. A Novel Secure Image Steganography Method Based on Chaos Theory in Spatial Domain. 2014.

[18] Chen, W., C. Chang, and T.H.N. Le, High payload steganography mechanism using hybrid edge detector. Expert Syst. Appl., 2010. 37: p. 3292-3301.

[19] Seyyedi, S.A. and N. Ivanov, Statistical Image Classification for Image Steganographic Techniques. International Journal of Image, Graphics and Signal Processing, 2014. 6: p. 19-24.

[20] Drebuzhan, A.M., et al., The Steganographic Method of Introducing Additional Information, Resistant to Transcoding and Conversion. 2022 Systems of Signals Generating and Processing in the field of on Board Communications, 2022: p. 1-5.

[21] Yadahalli, S.S., S. Rege, and R. Sonkusare. Implementation and analysis of image steganography using Least Significant Bit and Discrete Wavelet Transform techniques. In 2020, the 5th International Conference on Communication and Electronics Systems (ICCES). 2020.

[22] Chuang, Y.H., et al., Steganography in RGB Images Using Adjacent Mean. IEEE Access, 2021. 9: p. 164256-164274.
[23] Jia, J., et al., Multiperspective Progressive Structure Adaptation for JPEG Steganography Detection Across Domains. IEEE Transactions on Neural Networks and Learning Systems, 2022. 33(8): p. 3660-3674.
[24] Lapins, S. et al., An examination of the continuous wavelet transform for volcano-seismic spectral analysis. Journal of Volcanology and Geothermal Research, 2020. 389: p. 106728.
[25] Mateo, C. and J.A. Talavera Bridging the gap between the short-time Fourier transform (STFT), wavelets, the constant-Q transform and multi-resolution STFT. Signal, Image and Video Processing, 2020. 14(8): p. 1535-1543.
[26] Kustov, V. and E. Silanteva. ± 1Highly Undetectable Stegosystem Model Using Digital Still Images. in 2020 43rd International Conference on Telecommunications and Signal Processing (TSP). 2020.
[27] Mukherjee, B., et al., Springer handbook of optical networks. 2020.
[28] Kharrazi, M., T. Sencar, and N. Memon, Image steganography: Concepts and practice. 2004. 22.
[29] Zhou, X., et al., Linguistic Steganography Based on Adaptive Probability Distribution. IEEE Transactions on Dependable and Secure Computing, 2022. 19(5): p. 2982-2997.
[30] Evsutin, O., A. Melman, A., and R. Meshcheryakov, Algorithm of error-free information embedding into the DCT domain of digital images based on the QIM method using adaptive masking of distortions. Signal Processing, 2021. 179: p. 107811.
[31] Li, F., et al., Anti-compression JPEG steganography over repetitive compression networks. Signal Processing, 2020. 170: p. 107454.
[32] Liu, W. et al., Secure halftone image steganography minimises distortion on pair swapping. Signal Processing, 2020. 167: p. 107287.
[33] Bao, Z. et al., A robust image steganography based on the concatenated error correction encoder and discrete cosine transform coefficients. Journal of Ambient Intelligence and Humanized Computing, 2020. 11(5): p. 1889-1901.
[34] Banerjee, S. and G.K. Singh, A Robust Bio-Signal Steganography With Lost-Data Recovery Architecture Using Deep Learning. IEEE Transactions on Instrumentation and Measurement, 2022. 71: p. 1-10.
[35] Meng, R., et al., High-Capacity Steganography Using Object Addition-Based Cover Enhancement for Secure Communication in Networks. IEEE Transactions on Network Science and Engineering, 2022. 9(2): p. 848-862.
[36] Sałabun, W. and K. Urbaniak. A New Coefficient of Rankings Similarity in Decision-Making Problems. in Computational Science – ICCS 2020. 2020. Cham: Springer International Publishing.