SSRG International Journal of Electrical and Electronics Engineering
ISSN: 2348-8379/ https://doi.org/10.14445/23488379/IJEEE-V12I11P110

Volume 12 Issue 11, 112-123, November 2025
© 2025 Seventh Sense Research Group®

Original Article

Coverless Image Steganography Method Based on Snellen-Chart Generation

Aziza Hussein[1], Mohamed Gamal[2], Ahmed El-Sawy[3], Al Hussien Seddik[4]

[1]*Electrical and Computer Engineering Department, Effat University, Jeddah, KSA.*
[2]*Electrical and Computer Engineering Department, Faculty of Engineering, Minia University, Egypt.*
[3]*Department of Electrical Engineering, Faculty of Engineering, Minia University, Egypt.*
[4]*Computer Science Department, Faculty of Science, Minia University, Egypt.*

[2]*Corresponding Author : 29003252400051@eng.s-mu.edu.eg*

Received: 07 September 2025 Revised: 09 October 2025 Accepted: 08 November 2025 Published: 28 November 2025

Abstract *- Conventional Image Steganography typically hides data via pixel-level modifications within digital images, a process that can leave detectable statistical traces when analyzed with advanced steganalysis methods. To overcome this, a coverless data hiding method is proposed. Coverless data hiding does not mean there is no cover at all. Image generation is essential for creating a robust coverless steganography system capable of addressing various information hiding challenges effectively. An Image-Generation-Based Coverless Steganography System is presented in this paper for the secure transmission of hidden messages. The generated image resembles the well-known Snellen chart utilized in vision/eye tests, and is therefore referred to as "Eye Vision Test" within the paper. The proposed method has two phases. First, the sender uses a hiding algorithm to create an "Eye Test Image" from the secret message bits. Then, the receiver uses a method to get the original secret message from the Eye Test Image. The paper ends by showing a coverless steganography system based on the proposed algorithms. Tests and analysis demonstrated that the proposed system performed exceptionally well in terms of strength, security, and hiding ability, outperforming other coverless image steganography methods. Testing indicated that the proposed system is capable of hiding 98 bits within each generated cover image while achieving a complete success rate against various attacks, including scaling, compression, and noise. The results indicate that the method utilizing the Snellen chart is superior to existing coverless steganography techniques in terms of robustness, security, and data capacity.*

Keywords *- Coverless Information Hiding, Eye Vision Test Sheet Image, Image Steganography, Data Hiding, and Image Generation.*

1. Introduction

In the contemporary technological landscape, characterized by the widespread use of images, sound, and videos, the digital sharing of confidential information has become a significant necessity. Steganography involves the transmission of confidential information through hidden methods [1]. Digital steganography serves as a significant method for safeguarding information. This approach utilizes multimedia elements, including images, audio, and video, to conceal messages. For effective hiding of information, it is essential that the selected medium is readily recognizable and that any modifications implemented remain imperceptible to others. Digital images are frequently regarded as the optimal option for this purpose due to the substantial amount of additional data they contain, which can be leveraged to convey significant messages discreetly [2]. This paper centers on this topic. Traditional steganography alters the cover image to conceal secret messages, rendering it vulnerable to detection by steganalysis tools, which can reveal the hidden information. Despite the increasing number of coverless steganography techniques, most existing methods either rely on large-scale image databases for mapping or apply deep generative models that require extensive training, making them computationally intensive and less adaptable. Moreover, the majority of existing systems depend on image hashing or pixel-level transformations that, while robust, still leave subtle traces that may be identified by advanced steganalysis tools. Consequently, a clear research gap remains in developing a lightweight, generation-based coverless technique that can produce visually natural images without directly embedding any information into pixel values. To address this gap, the present study proposes a framework for image generation based on the Snellen chart, which embeds binary information into organized optometric layouts. The application of Snellen charts as steganographic carriers offers a novel approach to hiding information without a cover. Unlike standard image generation methods, their organized and hierarchical structure allows for the precise embedding of secret message bits into visually coherent patterns. This mechanism bridges the gap between perceptually meaningful image generation and secure information hiding, achieving both visual plausibility and technical robustness while eliminating the need for external databases or deep generative models. In 2013 [3], Bilal et al. presented "Zero-steganography" with the aim of significantly reducing the detection of steganography and increasing the robustness of steganography. Zhou et al. (2016) reported that experts from Beijing and Shanghai had proposed the novel concept of "coverless" information hiding in May 2014 to enhance security [4]. Unlike traditional steganography, "Coverless" steganography still requires carriers. It highlights that it may "generate/acquire" stego-carriers without the need for additional carriers by using secret data as a driving force [5].

The primary aim of this paper is to introduce a new approach for coverless image steganography, which involves generating an eye test sheet image, commonly referred to as a "Snellen chart," that conceals a hidden message. Rather than using traditional hiding methods (for instance, Least Significant Bit (LSB) and Pixel-Value Differencing (PVD) methods), this approach keeps the cover image pixels unchanged. It generates an eye-test image that represents the bits of the secret message. The proposed approach stands out for its completely generation-based design, which makes the use of pre-existing image databases or computationally expensive deep generative models unnecessary.

Unlike most existing coverless steganography techniques, which rely on external image datasets or deep network training, the proposed Snellen-chart generation method creates the stego-image directly from the secret message. The proposed method does not alter any pixels, requires less computation, and provides enhanced security and strength, serving as a straightforward and effective alternative to traditional coverless methods. This paper is organized into five sections: Section 2 discusses related work on coverless image steganography. Section 3 describes the proposed coverless image steganography method based on the Eye vision test. Section 4 focuses on the results and evaluation of our proposed method. Finally, Section 5 provides the conclusion and a summary of the main topics discussed in the paper.

2. Related Work

2.1. Traditional Image Steganography

Traditional image steganography refers to the process of embedding confidential data into a digital image by slightly modifying its pixel or coefficient values [6]. The primary objective of this technique is to conceal secret information within an image, making the hidden data undetectable. The hidden content, also known as the payload, can take various forms, including text, images, or multimedia files. After the embedding process is complete, the created image, known as the stego-image, is transmitted through an unsecured communication channel [2]. To improve security, many systems utilize encryption and secret keys that determine aspects such as where to store the data or how to encode it. The sender and the receiver must have the same parameters in order to accurately recover the hidden message.

According to the classification reported in [1], traditional image steganography techniques can generally be divided into three categories: spatial-domain, frequency-domain, and adaptive methods. Data bits are immediately integrated into the pixel intensity values of the cover image's spatial domain. Methods including Least Significant Bit (LSB) substitution and Pixel-Value Differencing (PVD) exploit local pixel redundancies to encode information. Variants of these techniques include the LSB replacement [7], LSB matching [8], color palette [9], and histogram-based methods [10]. Although these techniques are computationally simple and visually imperceptible, they are often vulnerable to statistical or visual steganalysis attacks [11].

In order to overcome these shortcomings, methods in the frequency-domain steganography have been invented, where secret information is hidden in transformed coefficients rather than the actual pixel values. In many cases, the Discrete Wavelet Transform (DWT) [12], the Discrete Fourier Transform (DFT) [13], and the Discrete Cosine Transform (DCT) [14] are used to hide information in non-zero frequency bands during a transformation. These techniques are usually more computationally intensive and also more resistant to compression and noise, but can still be detected by sophisticated attacks on analysis.

The third category, referred to as adaptive steganography, dynamically modifies the embedding process in response to local image characteristics, such as edges and texture complexity. Common examples include locally adaptive coding [15] and edge-based [16]. These adaptive approaches serve as a middle stage between spatial and frequency-domain techniques, offering invisibility and moderate robustness. In general, traditional steganography methods are well researched, but since they depend on changing pixels, they are naturally easy to detect. This has led to the development of coverless steganography as a safer option.

2.2. Coverless Image Steganography

The concept of coverless information hiding involves sending information without altering the cover's image. The term 'coverless' does not indicate that a cover is unnecessary [17]. Coverless steganography, a relatively recent concept introduced in 2015, does not mean data can be hidden without any carrier image. Instead, it involves embedding/hiding the secret information (payload) within a generated carrier or by directly mapping the message onto the carrier's properties [18]. The primary advantage of coverless steganography is that it eliminates the need to modify the stego-image for secret communication, rendering current detection techniques ineffective in identifying hidden data. It falls into two broad categories, i.e., image mapping techniques and image generation techniques. This is divided into categories according to the correlation established between the secret message and the carriers used in the steganography process [19]. These methods used to generate images depend on the nature of the hidden data, and methods typically employed include the construction of texture-based images that conceal the information. The methods also avoid constructing index structures, instead depending on generative models to generate stego-images that are direct carriers of hidden information. The other method involves a mapping rule, in which the cover images are directly related to the hidden message. The image mapping procedures are applied to create a relationship between the confidential data and the carriers [19].

2.3. Advancements in Recent Years

Over the past few years, coverless image steganography has garnered substantial attention due to the increasing pressure to deliver secure information and communication in distributed and cloud environments. Many of the older embedding-based systems adjust the carrier image at the time that data hiding occurs, which makes them vulnerable to alteration of features and their detection. Researchers have, in turn, responded by adopting approaches that relate elements of the message to features of a set of existing images (mapping-based) or generate new images based on message information (generation-based). These methods are designed to maintain high robustness against steganalysis and minimize direct pixel modifications in the image.

The initial mapping-based one was introduced in [20], in which a large-scale image database was built on the Internet resources. Each image in the database was given a strong hash sequence that represented its visual features. The sender and recipient can access the shared database, as well as the attached hash mappings. The secret message was converted to binary format, and it was broken down into several parts. Each part was associated with an image that had a hash value equal to the same binary sequence. The chosen images were then used as stego-images in transmitting hidden information. The approach proved extremely strong at imaging changes, which is due to its hash-based nature, and it can withstand multiple changes, including resizing, lighting changes, and the occurrence of noise. This makes it very suitable for the safe transfer of information, whereby the image is not distorted.

In a similar work, Zheng et al. [19] proposed a coverless steganography technique that is based on a powerful hashing algorithm based on the Scale-Invariant Feature Transform (SIFT). All images were converted into 18-bit binary hash codes, which were used to create a local image index. However, the number of possible 18-bit codes required to include all possible codes was extremely large, which would complicate the processing. To address this issue, the authors permitted multiple images to use the same hash code, effectively reducing the overall database size. The secret message was split into 18-bit parts, and each part was linked to a matching image hash before being sent. Demonstrated improved robustness and efficiency, although it retained dependence on a local image database. The algorithm's hash was improved [20], along with an augmentation in the secrecy information.

A generative model–based technique was introduced in [21] where the sender used a generative function to create a new image having a histogram distribution identical to the secret image. The receiver reconstructed the secret date from the histogram-matched image using the same generation model. Although the method provides strong data security and can hide a large amount of information, its dependence on shared settings and databases between the sender and receiver makes it less flexible and harder to scale in larger systems.

The study in [22] presents a new technique that uses the "Grayscale Gradient Co-occurrence Matrix." This technique operates sequentially. Initially, the payload is transformed into a series of 0s and 1s. Subsequently, the series of 0s and 1s is divided into groups of eight bits each. Next, a turbo encoder is used to expand each 8-bit segment to 16 bits, which increases the data transmission speed. Following this, the 16-bit segment is used to find a matching image from a set of available images. This process is repeated until all payload segments are adequately represented. Additionally, the system selects an image with the same dimensions as the hidden message and places it immediately after the images that contain the secret date. At the end, all the images - those with the hidden message and those with the encoded date – are sent together to the person who is meant to receive them.

Hussein et al. [23] proposed a jigsaw puzzle–based coverless steganography approach, in which an image is divided into uniform blocks, and each block is modified according to the secret message bits. The system generated tabs and blank sections to form sub-images resembling a puzzle, which were subsequently reassembled to produce the complete stego-object. Overall, the experimental findings highlight the method's superior performance in terms of capacity and robustness, achieved by encoding data through spatial organization rather than altering the visual content of images.

In a recent research [24], a new hybrid architecture with mapping and generation-based algorithms was introduced based on the usage of the SIFT descriptor and the StarGAN generative architecture. The system split the secret message into two parts. The steganography involving SIFT, which encompasses both steganography with no cover and steganography with a cover, was utilized to conceal one part of the segment; the other part of the segment was also hidden using StarGAN's image-generation capabilities. The relationship between the facial features and the message data improved the accuracy of hiding, allowing for the concealment of more data. In another method, Al Hussien et al. [25] used a bubble-sheet form in which binary data was represented. The system utilized each element in a predetermined template, whether occupied or unoccupied, thereby eliminating the need for an image database. This architecture was effective, did not deteriorate over time, and operated autonomously without relying on external information.

Zou et al. [26] designed an algorithm that does not require a cover, using the structure of Chinese sentences. The message has been examined in terms of its grammatical elements, including the subject, verb, and object. The elements of the language were equated with numbered points on a picture that corresponded to every part of the message. The chosen pictures were then rearranged and sent to convey the hidden message subtly. The method was a new implementation of language use, but it constituted a strict installation and could be adversely limited by the principles of a language.

To conclude, earlier ways of hiding images without covers have proved to be more or less effective, secure, and data capacity-wise. Nevertheless, methods that utilize databases [19-21] face difficulties in scaling up and require a large storage facility. New image generation techniques [22-24] require both intensive training and substantial computational resources to be employed. Moreover, most such image generation methods do not utilize the parts of the image that convey different meanings to human perception. The problems experienced led to the invention of the new Snellen chart technique. The strategy utilizes properly organized and logical visual effects that can smoothly conceal confidential information within an otherwise natural and meaningful image.

3. Proposed Method

The problem of others getting personal information happens when two users connect through an app. This makes it more likely that secret information could be changed, lost, or damaged while being sent. So, it is clear that we need a safe and trusted way to send information. To address this issue, a new method was developed to conceal images without a cover. It uses Snellen chart eye test images to hide secret data. The proposed method keeps data safe during transmission and also addresses the issues identified in older methods.

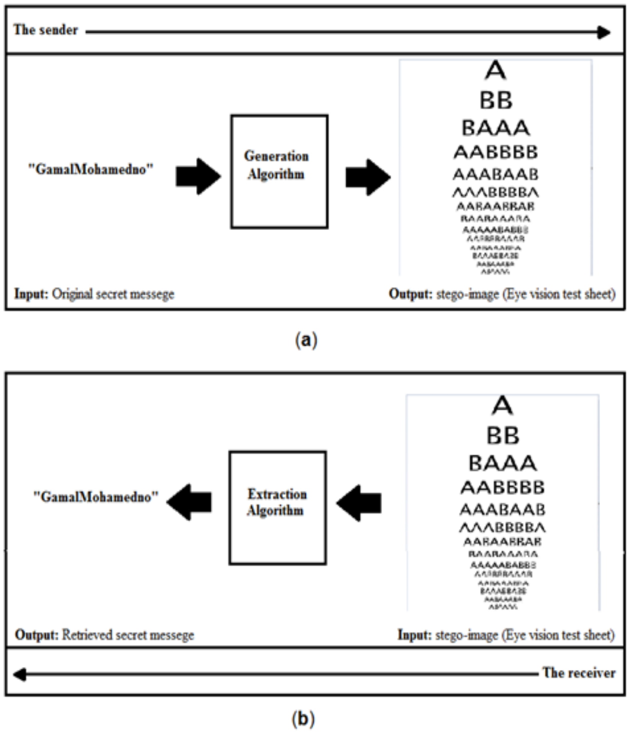
The methodology we employed consists of two primary components. The initial phase involves hiding, during which we create an eye test image, specifically a Snellen chart, that contains the hidden message. The subsequent phase involves extraction, during which we retrieve the hidden message from the Snellen image. The subsequent sections provide a comprehensive overview of the specific steps and techniques employed in the proposed method.

4. Proposed Method Components

The following components form the proposed method:

- White paper sheet image: This resembles the typical cover image for steganography. The secret information is hidden on a sheet of blank white paper.
- Payload or secret message: This is the secret data embedded within the eye test sheet.
- Snellen chart (Eye Vision Test Sheet): This is the outcome of hiding a hidden message within the image of a white paper sheet. It resembles the stego image used in traditional steganography.
- Generation algorithm: This technique fills in the white paper sheet image using the bits of the secret message to generate the eye test sheet.
- Extraction algorithm: This technique is used to reconstruct the secret message from the generated Snellen chart.

The structure of the proposed system is illustrated in Figure 1 below.



(a)

(b)

Fig. 1 The design of the proposed system (a)The sender side, and (b) The receiver side.

4.1. The Hiding Phase

As previously mentioned, the proposed method is based on generating an eye vision test image (Snellen chart) according to the binary bits of the secret message. Therefore, the following subsection will offer a brief explanation of the vision testing chart image and the generation process.

4.1.1. Snellen-Chart (Eye Vision Test Sheet)

The Snellen eye chart was developed in the 1860s and is believed to have been developed by Dutch ophthalmologist Dr. Hermann Snellen [27]. He used this chart together with Dr. Franciscus Donders to diagnose visual problems by asking people to look at a chart on a wall and describe what they saw.

Different types of eye charts can be used. Some charts display images or patterns, while others display letters or symbols. The most widely used and recognizable eye chart is the eye chart. Dr. Snellen also designed the "Tumbling E" eye chart. In our method, we will utilize the letters A and B to generate the eye vision test [27].

4.1.2. Bit Distribution and Layout Design

In our version, the Snellen chart layout was enlarged significantly, but we retained the standard row design and the same visual balance. The chart has 14 rows of letters arranged in a triangle shape. The number of letters grows from 1 at the top row to 14 at the bottom. An A3 image (3308 × 2338 pixels) was used to fit all the rows. The text size in each row was reduced to resemble a real Snellen chart.

4.1.3. The Generation Algorithm

The coverless generation method works as follows: the system begins with a white paper image and the secret message. The secret message is split into separate letters, then converted into a line of 0s and 1s. Each character is shown with 7 bits. After that, this bit stream will fill the white paper sheet image with several letters. In the first row, there is a solitary large letter, either an A or a B. As the rows progress, the number of letters increases, but their size decreases, resulting in lines and white spaces of equal thickness. Finally, if the secret bit to be represented is 1, the capital letter A will be printed on a white paper sheet. Otherwise, if the secret bit to be represented is 0, the capital letter B will be printed on a white paper sheet. This process will be repeated until the entire secret message is fully represented in the image. The final generated image, along with the eye test sheet (Snellen chart), will then be sent to the recipient. (Figure 2) depicts the key stages involved in concealing a secret message.

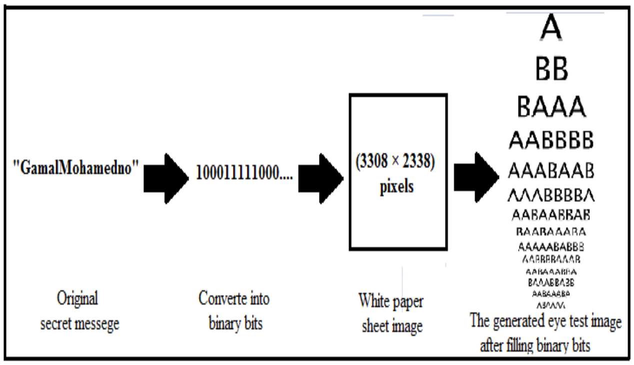


Fig. 2 The process of hiding a secret message

```
Algorithm 1: Hiding Algorithm (Generation of Snellen Chart)
Input: Secret message SM, white sheet image W
Output: Generated Snellen-chart image S
Steps:
1. Convert SM to binary stream B using ASCII encoding
2. For each bit bi ∈ B:
     If bi = 1 → print letter ‘A’;
     else → print letter ‘B’
3. Arrange characters in 14 rows with decreasing font size
End
```

4.2. Extracting Phase

4.2.1. Optical Character Recognition (OCR)

The extraction step in our method mainly uses OCR to read the hidden binary message from the Snellen chart image. We used MATLAB's built-in OCR function and set it to recognize only specific letters used in extraction, such as 'A' and 'B'.

The OCR result is checked row by row, following the same top-down order used to hide the bits. The detected letters are changed back to their bit values using the extraction dictionary. It is essential to note that the decoding process depends on the accuracy of the OCR.

4.2.2. Extraction Process

The extraction process mirrors the hiding process, but in reverse order. The receiver takes the generated eye test sheet image (Snellen chart) and puts it into the extraction system. To retrieve the embedded message, the system applies OCR to analyze the image and extract the visible letters line by line. Every letter is considered a hidden bit by the OCR engine as it scans the image. Letters 'A' and 'B' stand for secret bits 1 and 0, respectively. This process is done letter by letter, extracting the whole stream of secret bits. The bit stream is then separated into 7-bit segments, which are subsequently transformed into characters using the ASCII encoding system. The secret message is then created by combining these characters.

```
Algorithm 2: Extraction Algorithm
Input: Received Snellen-chart image S
Output: Reconstructed message M
Steps:
1. Apply OCR() function with character set {A, B}
2. For each detected symbol si:
    If si = ‘A’ → bit = 1;
    else → bit = 0
End
3. Group bits in sets of 7 and convert each to an ASCII
     character
```

(Figure 3), illustrates the stages involved in extracting a secret message.

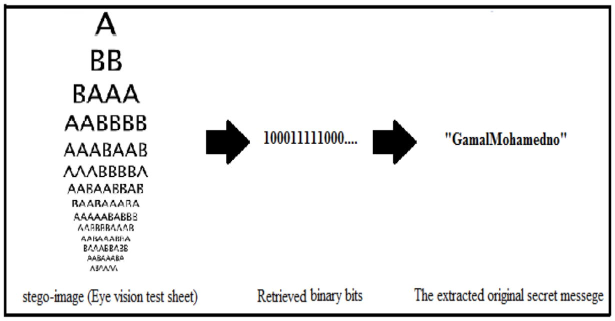


Fig. 3 The extraction process of the secret message

4.3. Simulation Experiments: Evaluation and Comparisons

To clearly differentiate the proposed framework from existing coverless steganography techniques, it is essential to emphasize that all experimental results reported in this section were obtained using a fully self-generated Snellen-chart image, without relying on any external datasets or previously published data. The fixed shape of the chart helps the OCR read it correctly, even if the image is resized, compressed, or has some noise. This method gave very strong results - 100% success under many attacks and 98 bits of data in each image, as shown in Tables 2-8. These results stem from the design of the chart and demonstrate that our method has a unique design and strong performance, not derived from past studies. The following subsections present the detailed evaluation procedures and comparative performance results.

The proposed method was tested and compared to other coverless image steganography methods to assess its effectiveness and efficiency through experimental evaluation. All experiments were performed utilizing MATLAB, a white paper sheet image of size A3 (3308 × 2338). The evaluation metrics are hiding capacity, security, and robustness. In addition, a detectability analysis was conducted to evaluate the extent to which the generated Snellen charts visually resemble standard charts, and to assess the likelihood of an observer detecting the presence of hidden information. The results and discussion related to visual detectability are presented in subsection 4.3.

4.4. Capacity

4.4.1. Capacity Calculation

In the proposed Snellen-chart–based coverless steganography system, the total data capacity depends on the number of available glyph positions (i.e., 'A' and 'B') across all rows of the generated chart. Since the layout follows a hierarchical structure of 14 rows with gradually decreasing font sizes, each row contains a different number of recognizable characters determined by the available horizontal space and minimum OCR-detectable font size. The total number of glyph positions is expressed as Equation (1):

$$N_{\text{glyphs}} = r\sum_{r=1}^{R} = \frac{R(R+1)}{2} \tag{1}$$

Where:

R represents the total number of rows in the generated Snellen chart that equal 14; r is the row index.

Each glyph printed represents one binary bit of the binary stream (A→1, B→0). Therefore, the total raw bit capacity is equal to the total number of glyph positions.

$$C_{row} = N_{\text{glyphs}} \tag{2}$$

In practical data-hiding systems, a small portion of the available capacity is often reserved for control or verification purposes. In this work, 7 bits are allocated as a header H corresponding to a Cyclic Redundancy Check (CRC-7) code.

The usable payload capacity is then calculated as:

$$C_{usable} = C_{row} - H \tag{3}$$

Accordingly, these 7 bits are excluded from the effective payload capacity, resulting in a usable capacity of 98 bits per generated Snellen chart.

Finally, assuming that each character in the recovered message is embedded using b bits (7-bit ASCII), the total number of storable message characters that can be represented in one chart is:

$$N_{chars} = \frac{C_{usable}}{b} \tag{4}$$

Table 1 summarizes the amount of data that can be hidden in previous studies. It also compares the amount of data that can be hidden in these studies to the amount of data that can be hidden using our method.

The suggested algorithm has a higher hiding capacity than the existing coverless image steganography algorithms. In this case, the bit content of each cover image was 98 bits; this was adjustable. The bigger cover images make it easier to hide some other data.

This improvement demonstrates that our approach is effective in addressing the low-capacity problem of coverless data hiding. There is a compromise between the amount of data that can be hidden and the effortlessness with which it can be uncovered.

The more letters are added, the more data can be hidden; however, this modification can alter the visual appearance of the chart and raise suspicions among those who observe it.

To ensure confidentiality, the chart must be designed in a manner that balances the data it conceals and its realistic appearance.

Table 1. Comparison of the hiding capacity of the proposed method

Method in reference number, publishing year	Capacity in bits
[22], 2018	16
[26], 2019	80
[28], 2020	14
[29], 2020	15
[24], 2020	33
[30], 2022	32
[31], 2022	32
Proposed method	98

(Figure 4) shows that the proposed system can hide more bits of data than other systems.

4.5. Robustness

In coverless steganography, strength is a crucial measure of security. It assesses how well the method can withstand various attacks and still accurately extract the hidden data.

Algorithm failure can be attributed to various attacks, including scaling attacks, JPEG compression, Gaussian noise, salt-and-pepper noise, and speckle noise.

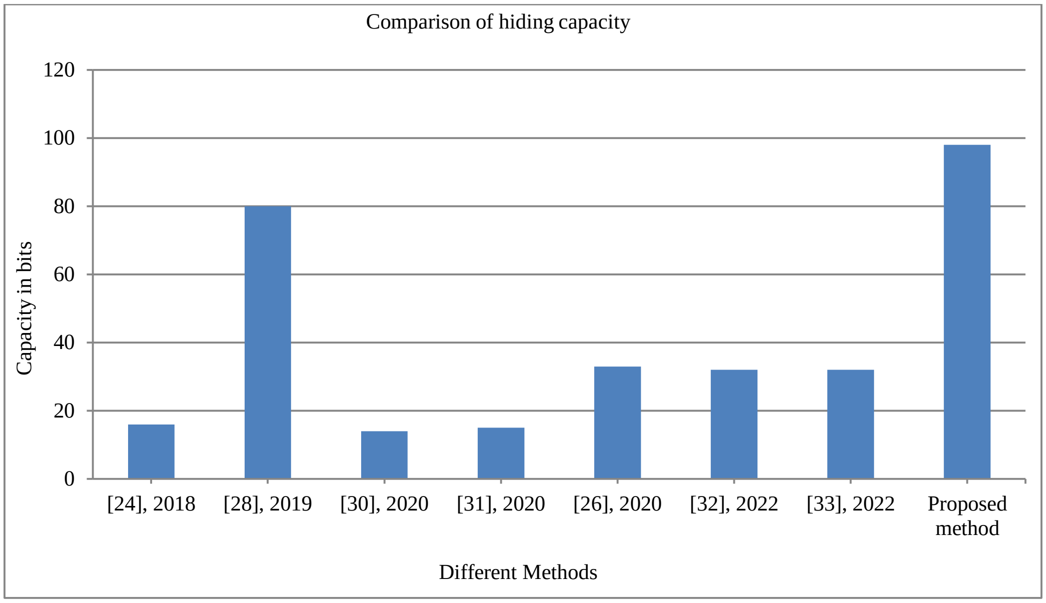


Fig. 4 Hiding capacity comparison

This section will test, evaluate, and confirm the proposed method's robustness by doing experiments and comparisons [22]. Bit Error Rate (BER) is a measure of how well the algorithm works during communication [22]:

$$BER = \frac{e}{n}, e = \sum_{i=1}^{n} p_i \oplus q_i \qquad (5)$$

Equation (5) uses the following variables: e, the number of errors that were found; n, the total number of bits; p, the original secret bits before they were attacked; and q, the secret bits after they were attacked. A Bit Error Rate (BER) of 0 indicates that no errors were found, and the secret bits were recovered perfectly, and the system achieves 100% as a Success Rate (SR). For example, an OCR misclassification of 'A' as 'B' would flip a '0' to a '1', thereby introducing a 1-bit error. When such recognition errors accumulate, the overall Bit Error Rate (BER) increases. This signifies the method's complete resilience against the specific attack; conversely, a BER greater than 0 implies the presence of errors in the recovered secret bits, suggesting that some bits have been corrupted or altered during the attack, and the success rate of the system is less than 100%.

The Success Rate (SR) is found using the Bit Error Rate (BER). It indicates the number of bits of the message that were correctly recovered. SR is calculated as follows [32]:

$$SR = 100\% - BER(\%) \qquad (6)$$

The value of BER is shown in Equation (5). The relationship between Success Rate (SR) and Bit Error Rate (BER) is opposite. When BER is high, SR becomes low, and when BER is low, SR becomes high. An SR of 100% means the recovered message is complete and has no mistakes or changes during extraction. If the SR is below 100%, it means some bits were changed. This may happen because of attacks or mistakes during data transmission [32].

4.5.1. Scaling Attack

Scaling is a strong type of attack. Changing the size of an image can cause the message to be lost or destroyed, including the hidden data. Table 2 shows the results of the scaling attack. Table 2 shows that the proposed method failed at scaling ratios of 0.2 and 3. When the stego-image was resized to 0.2, its size became 662 × 468 pixels. When it was resized to 3, its size became 9924 × 7014 pixels. In both instances, the lines intersected, resulting in the algorithm's inability to interpret the letters accurately.

Table 2. Comparison of BER after scaling attack

Ratio of scaling	[22], 2018	[28], 2020	[23], 2021	[25], 2021	Proposed method
0.2	—	—	—	—	Failed
0.25	—	—	—	—	0
0.3	0.015	0.899	Failed	0.025	0
0.5	0.009	0.589	0.011	0	0
0.75	0.002	0.235	0	0	0
1.25	—	—	—	—	0
1.5	0.025	0.058	0	0	0
2	—	—	0	—	0
3	0.098	0.050	0	—	Failed

When the scaling ratios were between 0.25 and 2 or higher, no errors appeared. The Bit Error Rate (BER) in these cases was 0. This indicates that the message was successfully found and extracted with 100% accuracy. This demonstrates that the method is robust and reliable within these ranges.

Table 3. Comparison of SR after scaling attack

Ratio of scaling	[22], 2018	[23], 2021	[25], 2021	Proposed method
0.2	—	—	—	Failed
0.25	—	—	—	100%
0.3	98.5%	Failed	97.5%	100%
0.5	99.1%	98.9%	100%	100%
0.75	99.8%	100%	100%	100%
1.5	97.5%	100%	100%	100%
2	—	100%	—	100%
3	90.2%	100%	—	Failed

As shown in Table 3, the system achieves an optimal SR value of 100% across all scaling ratios tested (0.25 to 2), confirming flawless extraction of the secret message without errors. However, at scaling ratios of 0.2 and 3, the system fails to recover the message accurately, resulting in a degraded SR. (Figure 5), illustrates how the proposed system compares to other systems when tested against image scaling attacks.

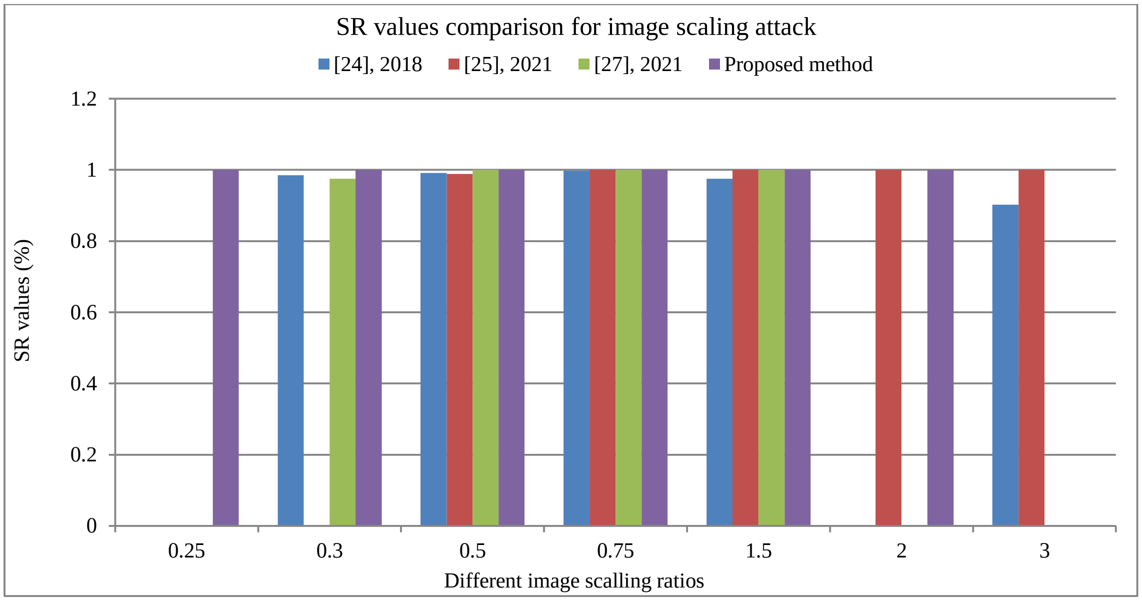


Fig. 5 Image scaling attack comparison

4.5.2. JPEG Compression Attack

JPEG is the widely adopted lossy compression standard for digital images, which permits data loss in the images during digital transmission [22]. When a stego-image is compressed, it may lose some/all of the secret messages during transmission.

The Bit Error Rate (BER) was calculated for the proposed method after it was attacked using JPEG compression. You can adjust the JPEG compression quality between 1 and 100. A rating of 100 indicates the least amount of compression, while a value of 1 indicates the greatest. During the investigation, JPEG compression was used at various quality levels, ranging from 90% to 10%. The first eye test picture was a 198 KB PNG file. The compressed JPEG files had a size range of 55.3 KB at 10% quality and 131 KB at 90% quality settings. Table 4's results showed that the proposed approach achieved the greatest performance at various compression levels with a Bit Error Rate (BER) of zero. This shows how completely robust the suggested approach is to JPEG compression assaults at these levels, enabling the accurate and thorough retrieval of the secret message.

Table 1. Comparison of BER after JPEG compression attack

Quality	[22], 2018	[29], 2020	[23], 2021	[25], 2021	[31], 2022	Proposed method
90	0	0.0034	0	0	0.0074	0
80	—	—	0	—	—	0
70	0.002	0.0052	0	0	0.0115	0
60	—	—	0	—	—	0
50	0.007	0.0079	0	0	0.0134	0
40	—	—	0	—	—	0
30	—	—	0	—	—	0
20	—	—	0	—	—	0
10	—	—	0.0167	—	—	0

Table 5. SR values for JPEG image compression attack

Quality	[22], 2018	[28], 2020	[31], 2022	Proposed method
90	100%	99.66%	99.26%	100%
80	—	—	—	100%
70	99.8%	99.48%	98.85%	100%
60	—	—	—	100%
50	99.3%	99.21%	98.66%	100%

Table 5 compares the SR value of the proposed system with other systems. The results in Table 5 show that the proposed system works at its best, reaching a 100% Success Rate (SR) for all image qualities. This proves that it can resist JPEG compression attacks and keep the hidden message safe and unchanged. (Figure 6) shows a visual comparison between the proposed system and other methods in terms of how well they resist JPEG compression.

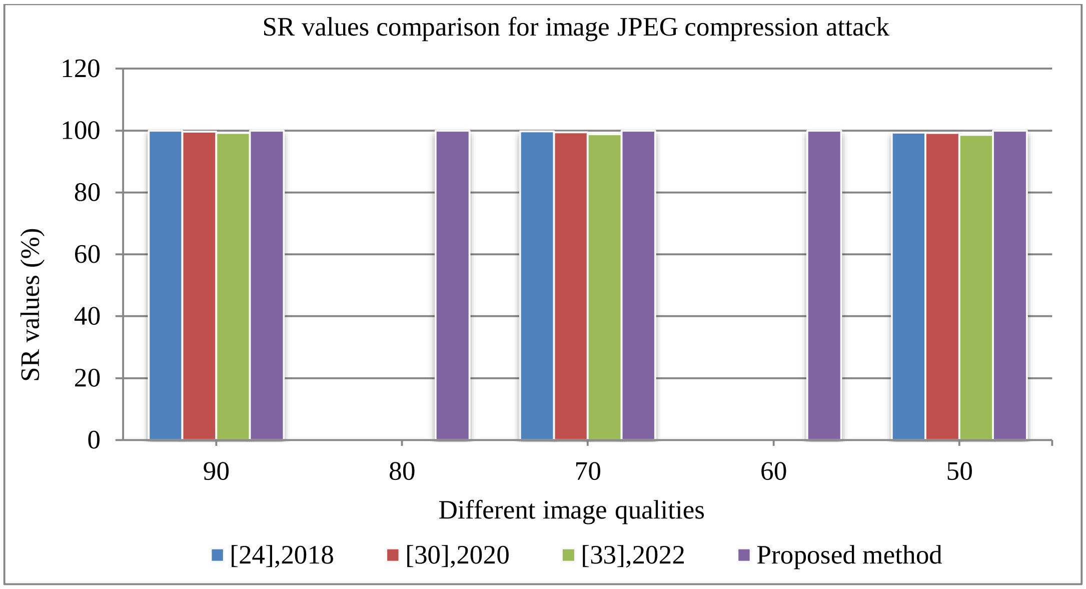


Fig. 6 JPEG image compression attack comparison

4.5.3. Noise Attack

Salt and Pepper Noise

"Salt and pepper" noise is a type of noise that randomly introduces black and white pixels into an image, while Maintaining a consistent overall noise level. This results in a speckled appearance with both dark and light spots scattered across the image. Noise density refers to the quantity of extra black or white pixels introduced into an image. Higher noise density levels result in greater distortion of the image and reduced visual quality [32]. In Table 6, the effects of salt and pepper noise on the proposed method are detailed. The results indicate that the Bit Error Rate (BER) of the proposed method remains at zero for the majority of noise densities, with the exception of a density of 0.005. The proposed method demonstrates exceptional resilience to "salt and pepper" noise attacks at the specified densities. The achievement of 100% accuracy in the extraction of secret messages, even amidst significant noise levels, clearly illustrates this point.

Table 2. Comparison of BER after salt and pepper noise attack

Noise density	[28], 2020	[29], 2020	[31], 2022	Proposed method
0.001	0.1609	0.004	0.0115	0
0.002	—	—	—	0
0.003	—	—	—	0
0.004	—	—	—	0
0.005	0.4904	0.0073	0.0195	Failed

Other Noise Attacks

The results demonstrate the impact of certain noise attacks that are difficult for nearly all image steganography methods to withstand, including Gaussian noise and Speckle noise. Table 7 shows the comparison results of BER after a Gaussian noise attack. The proposed method was tested with Gaussian noise levels between 0.001 and 0.9.

Table 3. Comparison of BER after gaussian noise attack

Noise density	[28], 2020	[29], 2020	[31], 2022	Proposed method
0.001	0.1548	0.0060	0.0151	0
0.005	0.4680	0.0107	0.0307	0
0.1	0.9638	—	—	0
0.5	—	—	—	0
0.8	—	—	—	0
0.9	—	—	—	Failed

Based on the results in Table 7, the proposed method exhibits a Bit Error Rate (BER) of zero for the majority of noise densities, except for a density of 0.9. This means that the proposed method can fully resist Gaussian noise attacks at these levels. Table 8 provides the results of the BER comparison after the Speckle noise attack. The proposed method was tested using Speckle noise levels between 0.01 and 0.1. Table 8 indicates that the proposed method performed effectively across a range of noise levels, maintaining a Bit Error Rate (BER) of zero, with the exception of a noise density of 0.1. The findings indicate that the proposed method is capable of fully mitigating Gaussian noise at the specified density levels.

Table 8. Comparison of BER after speckle noise attack

Noise density	[19], 2017	[28], 2020	Proposed method
0.01	0.6951	0.0972	0
0.05	0.8798	0.2341	0
0.1	0.9367	0.9107	Failed

5. Detectability Analysis

A key requirement of coverless steganography is that the generated image must appear natural and resemble typical images. Our approach involves utilizing a limited selection of characters, specifically "A" and "B", to embed binary data within the framework of the Snellen chart. Although this limitation aids in the accurate extraction of data by OCR, it simultaneously alters the appearance of the chart, making it deviate from the conventional Snellen chart, which typically features a greater variety of letters, including E, F, P, T, O, and Z. A delicate balance exists between the realism of the image and the ease with which data can be hidden within it. The utilization of solely the letters "A" and "B" effectively illustrates binary data and enhances OCR accuracy. Nonetheless, this alteration results in a chart that appears less diverse, potentially leading to a visual discrepancy when compared to an authentic Snellen chart. Incorporating additional letters may enhance the realism of the chart; however, it could also complicate data extraction and increase the likelihood of OCR errors. This balance is examined to ensure that the chart maintains a realistic appearance while remaining robust and precise in data extraction.

6. Limitations and Future Work

The developed approach leads to positive results, but there are still some limitations. The main weakness is that the use of only A and B gives an output that seems unnatural compared to a regular Snellen chart. Secondly, the decoding process is reliant on the quality of OCR, which can drop in the event that the image is distorted or is not clear. Moreover, the fact that the layout is static can be revealed in some of the attack circumstances. Finally, 98 bits give a viable data capacity, but it is still lower than the possibilities of some adaptive approaches. Further studies can be conducted on the use of random character mapping to increase the delicateness of the chart visibility. The approach could also be used with other types of charts to increase capacity, including tumbling E or symbol charts to give the charts more of a natural look.

7. Ethical Considerations

The system of coverless steganography proposed will be used in the sphere of safe data transmission for ethical and legal purposes. The first thing is to provide an increase in the privacy of data and guarantee the safety of the communication process, and at the same time, avoid any malicious or harmful usage. This method will not ruin the original content, and at the same time, will not create fake pictures. It ensures the creation of visual charts that are natural and have a simple, objective meaning. No human, biometric, or copyrighted information was used, and all of the evaluations were done with Snellen chart images built specifically to be part of this research. The principles of responsible innovation will be followed in this research, and the suggested approach will only be used on safe and legal grounds, i.e., data protection, better cybersecurity, and secure communication, and the inappropriate usage will be actively avoided.

8. Conclusion

This paper introduces a new coverless image steganography technique that produces images resembling the Snellen eye test chart images. As shown in Table 1, it has a high level of security, robustness, and capacity to hide 98 bits of data. The sender first converts the primary message into binary. Such bits are then converted into a snapshot of the Snellen chart using a predefined character mapping. The stego-image thus generated is in the form of a normal eye test chart, which is sent to the receiver. The image is processed by the receiver through OCR, which recognizes the coded characters and retrieves the secret message. The method achieves 100% extraction success rates with various distortions, as shown in Section 4 and Tables 2-8. The extraction process relies on the accuracy of the OCR and can be influenced by distortions of images. Detectability analysis is used to determine the effects of hidden data on the real appearance of the image. The major weaknesses are limited character repertoire, reliance on OCR, and fixed layout limitations. The next task to be considered in future work is random mapping of characters and a variety of chart styles that will enhance the ability to hide and bulk of the data. The technical and ethical aspects of the proposed approach were also investigated in the research.

References

[1] Abbas Cheddad et al., "Digital Image Steganography: Survey and Analysis of Current Methods," *Signal Processing*, vol. 90, no. 3, pp. 727-752, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[2] Mehdi Hussain et al., "Image Steganography in Spatial Domain: A Survey," *Signal Processing: Image Communication*, vol. 65, pp. 46-66, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[3] Muhammad Bilal et al., "Zero-Steganography using DCT and Spatial Domain," *2013 ACS International Conference on Computer Systems and Applications (AICCSA)*, Ifrane, Morocco, pp. 1-7, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[4] Zhou Zhili, Cao Yi, and Sun Xingming, "Coverless Information Hiding based on Bag-of-Words Model of Image," *Journal of Applied Sciences*, vol. 34, no. 5, pp. 527-536, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[5] Jiaohua Qin et al., "Coverless Image Steganography: A Survey," *IEEE Access*, vol. 7, pp. 171372-171394, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[6] Jian Ye, Jiangqun Ni, and Yang Yi, "Deep Learning Hierarchical Representations for Image Steganalysis," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 11, pp. 2545-2557, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[7] H.-C. Wu et al., "Image Steganographic Scheme based on Pixel-Value Differencing and LSB Replacement Methods," *IEE Proceedings-Vision, Image and Signal Processing*, vol. 152, no. 5, pp. 611-615, 2005. [CrossRef] [Google Scholar] [Publisher Link]

[8] Jarno Mielikainen, "LSB Matching Revisited," *IEEE Signal Processing Letters*, vol. 13, no. 5, pp. 285-287, 2006. [CrossRef] [Google Scholar] [Publisher Link]

[9] Neil F. Johnson, and Sushil Jajodia, "Exploring Steganography: Seeing the Unseen," *Computer*, vol. 31, no. 2, pp. 26-34, 1998. [CrossRef] [Google Scholar] [Publisher Link]

[10] Zhuo Li et al., "Lossless Data Hiding Scheme based on Adjacent Pixel Difference," *2009 International Conference on Computer Engineering and Technology*, Singapore, pp. 588-592, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[11] Paul Alvarez, "Using Extended file Information (EXIF) File Headers in Digital Evidence Analysis," *International Journal of Digital Evidence*, vol. 2, no. 3, pp. 1-5, 2004. [Google Scholar] [Publisher Link]

[12] Wen-Yuan Chen, "Color Image Steganography Scheme using set Partitioning in Hierarchical Trees Coding, Digital Fourier Transform and Adaptive Phase Modulation," *Applied Mathematics and Computation*, vol. 185, no. 1, pp. 432-448, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[13] Robert T. McKeon, "Strange Fourier Steganography in Movies," *2007 IEEE International Conference on Electro/Information Technology*, Chicago, IL, USA, pp. 178-182, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[14] I.J. Cox et al., "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673-1687, 1997. [CrossRef] [Google Scholar] [Publisher Link]

[15] C.C. Chang, T.D. Kieu, and Y.C. Chou, "Reversible Information Hiding for VQ Indices based on Locally Adaptive Coding," *Journal of Visual Communication and Image Representation*, vol. 20, pp. 57-64, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[16] Weiqi Luo, Fangjun Huang, and Jiwu Huang, "Edge Adaptive Image Steganography based on LSB Matching Revisited," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 5, pp. 201-214, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[17] Yuanjing Luo et al., "Coverless Image Steganography based on Image Segmentation," *Computers, Materials and Continua*, vol. 64, no. 2, pp. 1281-1295, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[18] Xiang Zhang, Fei Peng, and Min Long, "Robust Coverless Image Steganography based on DCT and LDA Topic Classification," *IEEE Transactions on Multimedia*, vol. 20, no. 12, pp. 3223-3238, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[19] Shuli Zheng et al., "Coverless Information Hiding based on Robust Image Hashing," *International Conference on Intelligent Computing*, Liverpool, United Kingdom, pp. 536-547, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[20] Zhili Zhou et al., "Coverless Image Steganography without Embedding," *International Conference on Cloud Computing and Security*, Nanjing, China, pp. 123-132, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[21] Xintao Duan et al., "Coverless Steganography for Digital Images based on a Generative Model," *Computers, Materials & Continua*, vol. 55, no. 3, pp. 483-493, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[22] Jianbin Wu et al., "A Coverless Information Hiding Algorithm based on Grayscale Gradient Co-Occurrence Matrix," *IETE Technical Review*, vol. 35, no. sup1, pp. 23-33, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[23] Al Hussien Seddik Saad, M.S. Mohamed, and E.H. Hafez, "Coverless Image Steganography based on Jigsaw Puzzle Image Generation," *Computers, Materials & Continua*, vol. 67, no. 2, pp. 2077-2091, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[24] Xianyi Chen et al., “Novel Coverless Steganography Method based on Image Selection and StarGAN,” *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 1, pp. 219-230, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[25] Al Hussien S. Saad, M.S. Mohamed, and Eslam H. Hafez, “Coverless Image Steganography Based on Optical Mark Recognition and Machine Learning,” *IEEE Access*, vol. 9, pp. 16522-16531, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[26] Liming Zou et al., “A Novel Coverless Information Hiding Method based on the Average Pixel Value of the Sub-Images,” *Multimedia Tools and Applications*, vol. 78, no. 7, pp. 7965-7980, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[27] Marcio Zapparoli, Fernando Klein, and Hamilton Moreira, “Snellen Visual Acuity Evaluation,” *Brazilian Archives of Ophthalmology*, vol. 72, no. 6, pp. 783-788, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[28] Yi Cao et al., “Coverless Information Hiding based on the Generation of Anime Characters,” *EURASIP Journal on Image and Video Processing*, vol. 2020, no. 1, pp. 1-15, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[29] Qiang Liu et al., “Coverless Steganography based on Image Retrieval of DenseNet Features and DWT Sequence Mapping,” *Knowledge-Based Systems*, vol. 192, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[30] Xiyao Liu et al., “Robust Coverless Steganography using Limited Mapping Images,” *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 7, pp. 4472-4482, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[31] Yung-Hui Li et al., “Coverless Image Steganography using Morphed Face Recognition based on Convolutional Neural Network,” *EURASIP Journal on Wireless Communications and Networking*, vol. 2022, no. 1, pp. 1-21, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[32] Mohammed Salah Reda et al., “Information Hiding using Coverless Steganography System based on Image Generation,” *Scientific Journal for Damietta Faculty of Science*, vol. 12, no. 1, pp. 39-49, 2022. [CrossRef] [Google Scholar] [Publisher Link]