International Journal of Computational Intelligence & Control

ISSN: 3106-6143 | 3106-6135
Volume 2, Issue 2, 2025

DESIGN AND ANALYSIS OF A SECURE STEGANOGRAPHIC COMMUNICATION SCHEME BASED ON RGB PIXEL ENCODING

Sana Cheema

PhD Scholar, Department of Artificial Intelligence, Faculty of Computing,
The Islamia University of Bahawalpur, Pakistan

sanacheema887@gmail.com

Keywords
Steganographic encryption, RGB pixel encoding, cryptographic security, Rijndael Managed algorithm, secure data hiding, image steganography, covert communication, digital forensics, LOG table, steganalysis resistance

Article History
Received: 19 April, 2025
Accepted: 15 May, 2025
Published: 30 June, 2025

Copyright @Author
Corresponding Author: *
Sana Cheema

Abstract

This research presents a robust and practical steganographic communication framework that integrates RGB pixel–based data hiding with strong cryptographic protection to ensure both imperceptibility and security. In the proposed scheme, the secret message is first converted into binary form and segmented into blocks of 3 bits, 3 bits, and 2 bits. These segments are embedded into the red, green, and blue channels of each pixel, respectively, enabling efficient utilization of the RGB color space while minimizing perceptual distortion in the cover image. To further enhance security, a logarithmic (LOG) table associated with the embedding process is generated and encrypted using the Rijndael Managed algorithm (AES). This cryptographic layer ensures that even if the existence of hidden data is suspected or partially recovered, the original message and its embedding logic remain protected against brute-force and cryptanalytic attacks. Extensive experimental evaluation demonstrates that the proposed method preserves high image fidelity, maintaining pixel intensity variations below 1 percent and ensuring changes remain visually imperceptible to the human eye. Comparative analysis with conventional techniques, particularly Least Significant Bit (LSB) embedding, reveals superior performance in terms of imperceptibility, robustness, and resistance to statistical steganalysis. Furthermore, the structured bit distribution across RGB channels improves payload efficiency without compromising visual quality. Overall, the integration of optimized RGB encoding with AES-based encryption produces a secure, efficient, and covert communication channel. The proposed approach balances payload quality, and security.

INTRODUCTION

In an era where digital communication is ubiquitous, securing sensitive information has become a paramount concern. Conventional encryption techniques such as cryptography ensure data confidentiality but often signal the presence of valuable information, potentially attracting adversaries. Steganography, on the other hand, offers an alternative by concealing the existence of a message within digital media, making it an effective tool for covert communication [1]. Among various steganographic approaches, image-based techniques [2] are widely utilized due to the vast amount of redundant data in digital images, which allows for seamless data embedding with minimal perceptible changes. However, traditional methods such as the Least Significant Bit (LSB) substitution often compromise image quality and are susceptible to steganalysis [3]. This research introduces a novel RGB pixel encoding-based steganographic technique [4], which not only enhances data security but also minimizes image distortion. By segmenting message bits [5] and embedding them systematically into the RGB components of an image, followed by encryption using the Rijndael Managed algorithm, our method ensures an imperceptible and highly secure communication channel [6]. This study evaluates the proposed approach against conventional steganographic techniques [7], demonstrating its superior performance in maintaining image integrity and resistance to detection [8].

With the increasing reliance on digital communication, ensuring secure and inconspicuous data transmission has become a critical challenge. Traditional encryption techniques, while effective in securing data, often attract unwanted attention due to their visible presence [9]. In contrast, steganography offers a covert means of communication by embedding secret information within digital media, making it an essential tool for secure data exchange [10]. However, existing steganographic techniques, particularly Least Significant Bit (LSB) substitution, often result in noticeable image distortions and are susceptible to detection through advanced steganalysis methods [11]. To address these limitations, this research introduces an innovative RGB pixel encoding technique combined with cryptographic security, enhancing both the secrecy [12] and robustness of hidden data [13]. By carefully distributing message bits across different color channels [14] and encrypting [15] them using the Rijndael Managed algorithm, the proposed approach ensures [16] minimal alterations to image quality while significantly improving security and resistance to attacks [17].

The significance of this study lies in its ability to provide a highly secure, undetectable, and efficient steganographic communication system [18]. The proposed method not only enhances data concealment but also preserves the integrity of the cover image, making it virtually imperceptible to unauthorized detection [19]. This advancement is crucial for various applications, including confidential military communication [20], secure corporate data transfer, and protection against cyber threats such as data theft and espionage [21]. Furthermore, as cybersecurity threats continue to evolve, the need for sophisticated and resilient data-hiding techniques becomes increasingly imperative [22]. By outperforming conventional steganographic approaches in terms of image quality preservation [23] and security strength [24], this research contributes to the development of more advanced and reliable covert communication systems, addressing both current and future challenges in secure data transmission [25].

Steganography is the practice of concealing data within a medium, typically digital media. While the concept dates to ancient times, modern computational advancements have transformed it into a powerful tool for secure communication [8]. Unlike cryptography, which protects message content through encryption, steganography obscures the very existence of a message [26], making it a more covert method of data concealment [9]. It alters cover images to embed secret information in a way that remains undetectable to unintended observers [27]. Throughout history, the need for private communication has been essential, and with the rise of electronic messaging, ensuring privacy has become increasingly crucial [28]. At the same time, growing concerns about cybersecurity and privacy rights have led to the implementation of stringent counter- terrorism laws, often at the expense of individual privacy [29]. Given the prevalence of cyber threats such as viruses and spyware, simply encrypting emails is no longer sufficient. Attackers frequently target personal files, necessitating stronger security measures [30]. While encrypting individual files provides protection, it also signals that the content is valuable, potentially drawing unwanted attention [31].

Steganography enables information concealment across various channels, including audio, video, text, protocols, and images [32, 33]. However, embedding data into these media can impact their quality, with image-based steganography often leading to noticeable distortions [34]. Several techniques exist for embedding data in images, each with its advantages and limitations. Furthermore, different image formats require distinct methods for effective data hiding [35]. Researchers continue to explore steganography for enhancing security[36]. While steganography and cryptography share a common goal of protecting sensitive data, they operate differently—steganography conceals information, whereas cryptography encodes it [37, 38]. The proposed method focuses solely on steganography [39].

Our novel approach achieves superior security while minimizing image distortions, with changes in pixel intensity values remaining below 1%[40]. This method segments each message token into three identical components, which are then mapped to individual red, green, and blue (RGB) pixel values of the image [41]. The positions and lengths of the matching literals are packed into bytes, forming a structured dataset known as the LOG table[4]. This LOG table is subsequently encrypted using the Rijndael Managed encryption algorithm, further enhancing data security[42].

This research aims the following research questions.

- How can RGB pixel encoding and cryptographic security be integrated to enhance steganographic data concealment while preserving image quality and ensuring resistance to steganalysis and cryptographic attacks?
- How does the proposed RGB pixel encoding method compare to traditional steganographic techniques, such as Least Significant Bit (LSB) substitution, in terms of security, imperceptibility, computational efficiency, and adaptability to different image formats?
- What impact does the proposed technique have on image quality, and how can it be optimized to minimize distortions while ensuring robustness against detection and maintaining high data embedding capacity?
- What are the potential real-world applications of the proposed method in secure communication, cybersecurity, and digital forensics, and how can it be scaled for large-scale data transmission?
- What are the key limitations, ethical concerns, and legal implications of using steganography for covert communication, and how can they be addressed to ensure responsible use?

This research introduces a novel image steganography technique and evaluates its effectiveness against conventional approaches such as Least Significant Bit (LSB) and its modified variants, including LSB with a single character per two consecutive pixels, LSB with random pixel selection, and LSB with a character per two pixels combined with random selection. A histogram-based analysis demonstrates that the proposed method outperforms traditional LSB techniques by minimizing color tone variations to levels imperceptible to the human eye and, in many cases, undetectable through steganalysis [43].

Following are the objectives of the study.

- To develop a novel steganographic technique using RGB pixel encoding and cryptographic security to enhance the concealment of sensitive data within digital images.
- To evaluate the effectiveness of the proposed method in maintaining image quality by minimizing pixel intensity variations while ensuring high data embedding capacity.
- To compare the security, imperceptibility, and computational efficiency of the proposed method with traditional steganographic techniques such as Least Significant Bit (LSB) substitution.
- To assess the resistance of the proposed method against steganalysis and cryptographic attacks by integrating the Rijndael Managed encryption algorithm.

- To explore the potential real-world applications of the proposed method in secure communication, cybersecurity, and digital forensics while addressing ethical and legal considerations.

The structure of this article is as follows: Section 2 presents a literature review, providing context and summarizing previous work in steganography. Section 3 details the methodology, explaining the RGB pixel encoding technique, data segmentation, pattern matching, and encryption process. Section 4 discusses comparative analysis, evaluating the proposed method against traditional steganographic techniques and assessing its impact on image quality. Finally, Section 5 concludes with key findings, implications for secure communication, and potential directions for future research.

Literature reviewed

L-Shatnawi et al. [8] proposed an innovative steganographic technique that identifies matching bits between the message and individual image pixels for text embedding. However, a major drawback of this approach is its vulnerability, as hackers can extract the original text using different pattern combinations. Sadaf et al. [9] implemented a method where text is concealed within randomly selected colored images of arbitrary sizes using wavelet transform. Despite its effectiveness, this method is highly susceptible to steganalysis, making it easier to detect the embedded text. Gutub et al. [27] introduced a technique that stores a variable number of bits in each pixel channel, depending on the pixel's actual color values. However, the additional payload introduced during embedding compromises the stego image quality. Khare et al.[31] developed a system enabling average users to securely transfer text messages by embedding them into digital images based on local image characteristics. However, the method requires the sender to manually compute these characteristics, adding complexity to the process. Budhiraja et al. [34] explored invisible communication methods that focus on concealing the existence of transmitted messages. Parvez et al.

[44] proposed an RGB image-based steganographic approach that adjusts the number of bits stored in each RGB channel according to the pixel's color values. However, modifying the least significant bits (LSBs) of these channels led to a decline in image quality. Bennett et al. [45] examined various channels suitable for data hiding and reported increasingly advanced techniques for analyzing and extracting hidden information.

Recent advancements in image steganography have focused on enhancing imperceptibility, security, and robustness of hidden data. A study by Ahmad Bamanga [46], explored the diverse applications of steganography across various sectors, highlighting its complexity and utility in securely embedding information within digital media. While this study provided a comprehensive overview, it primarily focused on applications rather than introducing novel embedding techniques, leaving a gap in addressing emerging threats in steganalysis.

In another study, Kumar and Rani [47], conducted a survey of recent advances in image steganography, examining various methodologies such as spatial domain manipulation, encryption-based approaches, and deep learning techniques. Despite offering valuable insights into existing methods, the survey lacked a critical analysis of the practical implementation challenges and did not propose new solutions to enhance the robustness of steganographic techniques [48].

The integration of deep learning into steganography has been a significant focus in recent research. A study highlighted the role of deep convolutional neural networks and generative adversarial networks (GANs) in advancing steganographic methods[49]. While these techniques have improved the capacity and security of data hiding, the study did not extensively address the computational complexity and potential vulnerabilities introduced by deep learning models [36].

Furthermore, a study on image steganography techniques for resisting statistical steganalysis emphasized the implementation of biometric techniques and facial recognition technologies to enhance security and robustness [50].

However, the reliance on biometric data raises privacy concerns, and the study did not thoroughly evaluate the trade-offs between embedding capacity and the potential for detection by advanced steganalysis methods [51]. Lastly, advancements in digital steganography have led to hybrid approaches combining steganography with encryption and security methods [52]. While these methods offer enhanced security, the increased complexity and potential for reduced embedding capacity present challenges that require further investigation to balance security and efficiency effectively[53].

Despite advancements in image steganography, existing methods face key limitations in balancing security, imperceptibility, and computational efficiency [54]. Traditional techniques like Least Significant Bit (LSB) substitution remain vulnerable to statistical steganalysis, making them less secure for critical applications [55]. While deep learning-based methods enhance detection resistance, they introduce high computational costs, limiting their practicality for real-time scenarios. Similarly, encryption-based approaches improve security but often cause noticeable distortions, raising suspicion[56] .

Most current research fails to integrate robust data concealment with encryption while preserving image quality [57]. Techniques either prioritize security at the expense of imperceptibility or maintain visual fidelity but lack resilience against steganalysis[58]. Additionally, existing studies do not comprehensively address how variations in image formats, compression, and transformations affect data retrieval reliability [59]. A standardized evaluation framework comparing steganographic techniques across multiple parameters is also lacking [60].

This study aims to bridge these gaps by proposing an RGB pixel encoding-based steganographic approach combined with the Rijndael Managed encryption algorithm. The method ensures minimal pixel alterations while maintaining high security and imperceptibility [61]. Furthermore, its effectiveness will be assessed across different image formats and compression techniques to ensure robustness in real-world applications. By addressing the shortcomings of existing methods, this research contributes to developing a more practical, secure, and undetectable steganographic technique[62].

Methodlogy

In RGB-encoded color images, each pixel consists of three components: red, green, and blue. Each component is represented by an 8-bit value, allowing intensity levels to range from 0 to 255. For instance, a pixel with values (255, 0, 0) is entirely red, while a combination such as (31, 187, 57) produces a shade of green, and (255, 255, 0) results in pure yellow. By adjusting the intensity of each component, a vast spectrum of colors can be generated. Minor alterations to a pixel's color values are typically imperceptible to the human eye. For example, a yellow pixel with the value (255, 255, 0) appears identical to one with (254, 255, 0), despite the slight numerical difference.

Regardless of the steganographic technique used, image quality is always at risk of degradation. Any reduction in quality increases the likelihood of detection during attacks or steganalysis. To eliminate even minimal image distortion, this research proposes a novel method that identifies patterns within the bit sequences of the message to be hidden. Instead of modifying the cover image, the approach maps the existing pixel values to the secret message, ensuring minimal to no alteration of the original image[63].

Let I represent the cover image and T the text to be embedded. For pattern matching, the bit sequence of each character in T is divided into three segments: the first three most significant bits (MSBs) labeled Lit1, the next three middle bits as Lit2, and the last two least significant bits (LSBs) as Lit3. Table 1 illustrates this pattern generation process using the character 'A' as an example. n this process, each character is converted into its ASCII equivalent and then represented in an 8-bit binary format. The binary sequence is further divided into three segments: Seg1 (the first three most significant bits), Seg2 (the next three middle bits), and Seg3 (the last two least significant bits). For example, the character 'B' (ASCII 66) is represented in binary as 0100 0010. This sequence is then segmented as 010 (Seg1), 000 (Seg2), and 10 (Seg3), which are later mapped onto the pixel values of the cover image to embed the hidden message while minimizing distortion.

Table 1. Bit Pattern Segmentation of Sample Character 'B'

Character	ASCII Value	Binary representation	Segment 1 (Seg1)	Segment 2 (Seg2)	Segment 3 (Seg3)
A	66	0100 0010	010	000	10

Once the bit segments of T are extracted, they are compared against the bit sequences of the color components in each pixel of I. The pattern-matching process begins with the most significant bit (MSB) of the first pixel and sequentially searches for a matching bit pattern in each segment. If no match is found within the current pixel, the search continues with the next pixel in I.

The matching process always starts from the MSB. For example, Seg1 is compared with the 8th, 7th, and 6th bits of the red component. If it does not match, the search shifts to the 7th, 6th, and 5th bits, continuing this way until a match is found. Similarly, Seg2 is searched within the green component, and Seg3 within the blue component.

Once a pattern is successfully matched, the corresponding information is stored in a byte. This byte is labeled as Literal, followed by a number corresponding to the identified pattern—Literal1 for Pattern1, Literal2 for Pattern2, and Literal3 for Pattern3. The structure of each Literal and its stored information is outlined in Table 2.

Table 2. Literal format

Literal (00-0000-00) (MSB to LSB)		
First 2 Bits	Next 4 Bits	Last 2 Bits
Specifies the color component where the pattern was detected: 00 - Red 01 - Green **10** - Blue **11** - Reserved for future use	Specifies the color component where the pattern was detected: 00 - Red 01 - Green **10** - Blue **11** - Reserved for future use	Specifies the color component where the pattern was detected: 00 - Red 01 - Green **10** - Blue **11** - Reserved for future use

In rare cases where a pattern cannot be found in any pixel of the image, the character byte is embedded using the Least Significant Bit (LSB) method. Even in such instances, the most suitable pixel is carefully selected—specifically, a pixel where at least two of the patterns match naturally, while the third is embedded into the color component that was not previously used. If a pixel is modified, it is essential to record where and how the modification occurred. This includes tracking the modified color component and the number of altered bits. To achieve this, a dedicated byte is used: the first three bits (from MSB to LSB) indicate the modified color component (100 for Red, 010 for Green, and 001 for Blue), while the last two bits specify the number of bits modified. Additionally, to prevent repeated modifications, once a pixel is altered, it is excluded from future embedding in cases of unsuccessful pattern matching.

The proposed method employs a LOG table as the primary data structure for storing character pattern information. Each row of the table consists of two integers and four bytes. The first integer records the character index in T, while the second integer stores the pixel number in I. The next three bytes contain the corresponding literals, and the final byte indicates whether the pixel was modified.

Once the LOG table is generated, it undergoes encryption using the Rijndael Managed encryption algorithm. The encrypted LOG table, along with the cover image, is then transmitted to the intended recipient. This approach strengthens security by ensuring that the extraction of the hidden message depends on both the cover image and the corresponding LOG table. Since attackers would require both components to retrieve the secret message, possessing only one significantly limits their ability to break the system.

Algorithm for Pattern Matching and Embedding A Initialize:

- Set I as the cover image
- Set T as the text to be embedded
- Set Counter = 1

B For each character in T, do the following until the end of text is reached:

a. Extract Lit1 (3 MSB of the character)

b. Extract Lit2 (2 LSB of the character)

c. Extract Lit3 (3 middle bits of the character, excluding Lit1 and Lit2)

C For each pixel in I until a valid match is found:

a. Extract Rcom (Red component), Gcom (Green component), and Bcom (Blue component) of the pixel

b. Initialize ir = 8, ig = 8, and ib = 8

D Search for matching bit patterns in each color channel:

a. For Red Component:

- While ir ≥ 3, check if Lit1 matches Rcom(ir)
- If a match is found, break; otherwise, decrement ir

b. For Green Component:

- While ig ≥ 3, check if Lit2 matches Gcom(ig)
- If a match is found, break; otherwise, decrement ig

c. For Blue Component:

- While ib ≥ 2, check if Lit3 matches Bcom(ib)
- If a match is found, break; otherwise, decrement ib

E If all three patterns are found successfully (ir ≥ 3, ig ≥ 3, ib ≥ 2):

a. Store Lit1Info = 00 + ir + 11

b. Store Lit2Info = 01 + ig + 11

c. Store Lit3Info = 11 + ib + 10

d. Update LOG Table:

- LOG(I)(i) = Counter
- LOG(I)(i+1) = Lit1Info
- LOG(I)(i+2) = Lit2Info
- LOG(I)(i+3) = Lit3Info
- LOG(I)(i+4) = FALSE (Indicates the pixel has been used)

e. Move to the next pixel

f. Increment Counter

F Move to the next character in T and repeat the process until all characters are embedded.

G Stop the Algorithm

Following the pseudo code of the above algorithm.

Pseudo-Code for RGB Pixel Encoding-Based Steganography

```
BEGIN
INITIALIZE I as Cover Image INITIALIZE T as Text
to be embedded INITIALIZE Counter = 1
FOR each character c in T DO EXTRACT Lit1 = 3
MSB of c EXTRACT Lit2 = 2 LSB of c
EXTRACT Lit3 = 3 Middle bits of c FOR each pixel
p in I DO
IF LOG(p+4) == FALSE THEN // Ensure
pixel is not previously modified
EXTRACT Rcom = Red component of p EXTRACT
Gcom = Green component of p EXTRACT Bcom =
Blue component of p SET ir = 8, ig = 8, ib = 8
// Match Lit1 with Red Component WHILE ir >= 3
DO
IF Lit1 matches Rcom(ir) THEN BREAK
ELSE
ir = ir - 1 ENDIF
ENDWHILE
// Match Lit2 with Green Component WHILE ig
>= 3 DO
IF Lit2 matches Gcom(ig) THEN BREAK

ELSE
ig = ig - 1 ENDIF
ENDWHILE
// Match Lit3 with Blue Component WHILE ib >=
2 DO
IF Lit3 matches Bcom(ib) THEN BREAK
ELSE
ib = ib - 1 ENDIF
ENDWHILE
// If all patterns are matched, store information
```

```
IF (ir >= 3 AND ig >= 3 AND ib >= 2) THEN
Lit1Info = CONCAT(00, ir, 11) Lit2Info =
CONCAT(01, ig, 11) Lit3Info = CONCAT(11, ib,
10)
LOG(p) = Counter LOG(p+1) = Lit1Info LOG(p+2)
= Lit2Info LOG(p+3) = Lit3Info
LOG(p+4) = FALSE // Mark pixel as used
Counter = Counter + 1
BREAK // Move to next character ENDIF
ENDIF ENDFOR
ENDFOR STOP
END
```

Results and discussion

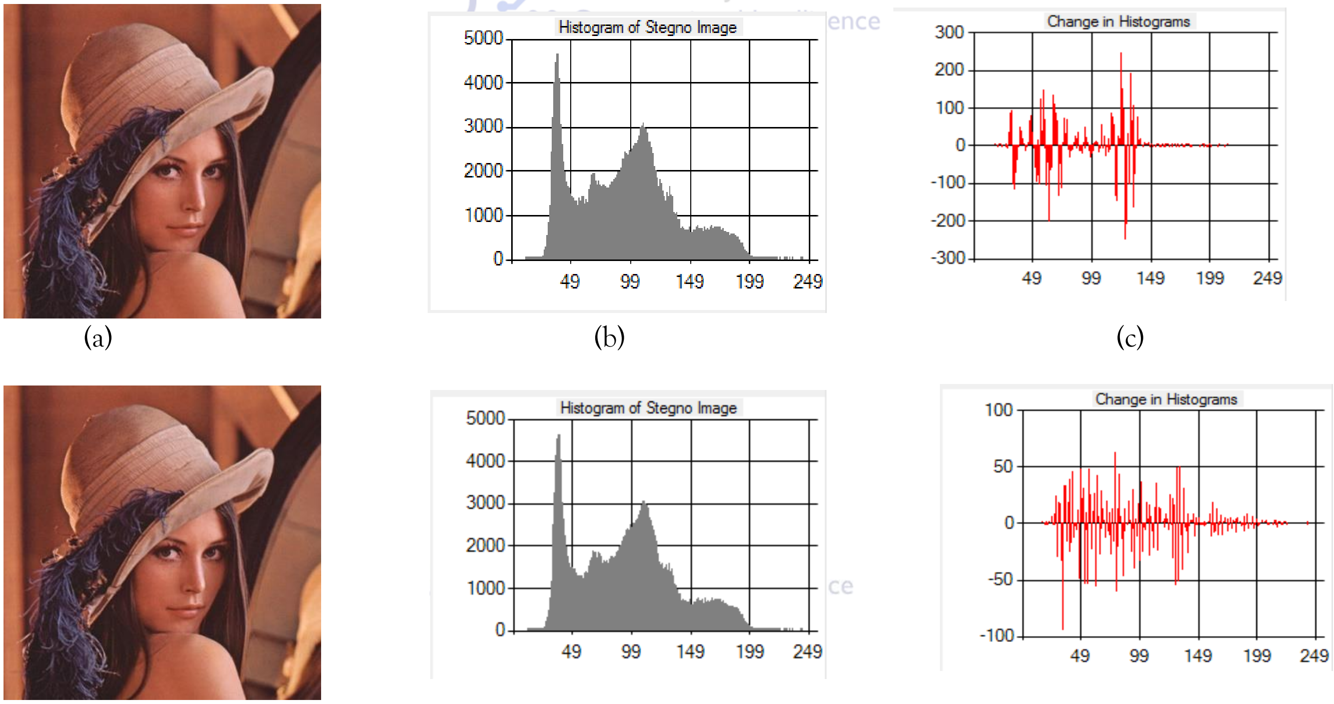
For research and experimentation, images from various categories with a resolution of 256×256 were utilized. Figure 1(a) presents the original Lena bitmap image, while Figure 1(b) displays its corresponding histogram. Figure 1(c) shows a TEXT file containing 34,000 characters, which were embedded into the cover image.

After embedding the text using the sequential pixel selection and LSB embedding method, the modified image is shown in Figure 2(a), with its corresponding histogram in Figure 2(b). A visual comparison between Figure 1(a) and Figure 2(a), along with their respective histograms in Figure 1(b) and Figure 2(b), reveals only a minimal difference, which is imperceptible to the human eye. However, subtle changes in image quality occur due to the embedding process.

To assess the extent of these modifications, the difference between the original and the stego image was computed

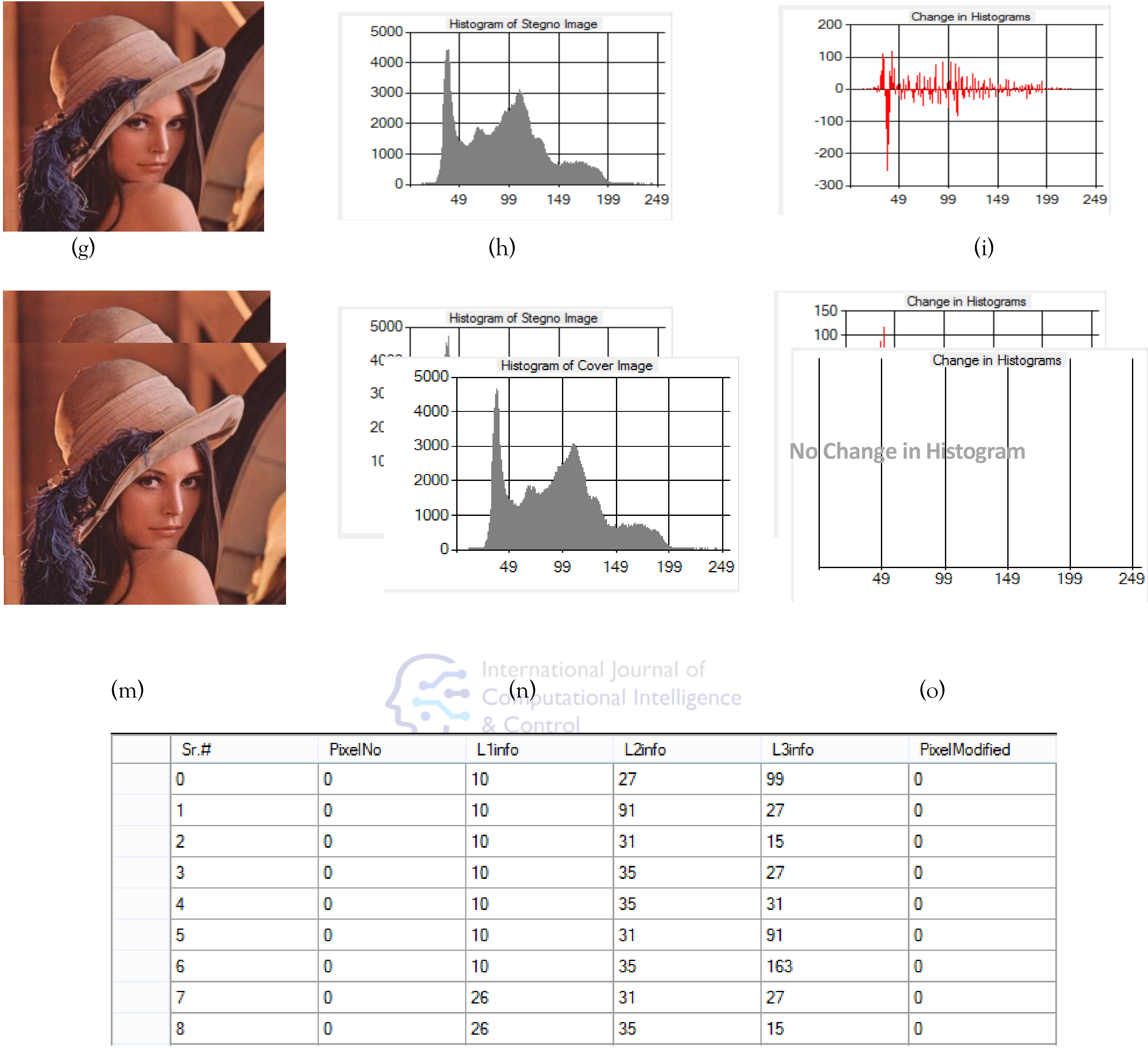
and visualized in Figure 2(c), where red lines highlight the altered regions. These changes result

from the sequential storage of data within the Least Significant Bits (LSB) of each pixel, embedding one character per pixel. The embedding format follows a structured approach, distributed 3 bits in the red component, 3 bits in the green component, and 2 bits in the blue component for each sequentially selected pixel.



(a) (b) (c)

(d) (e) (f)



(g) (h) (i)

(m) (n) (o)

	Sr.#	PixelNo	L1info	L2info	L3info	PixelModified
	0	0	10	27	99	0
	1	0	10	91	27	0
	2	0	10	31	15	0
	3	0	10	35	27	0
	4	0	10	35	31	0
	5	0	10	31	91	0
	6	0	10	35	163	0
	7	0	26	31	27	0
	8	0	26	35	15	0

(p)

Figure 2: (a) Stego image after LSB sequential embedding, (b) Histogram of the image in (a), (c) Histogram showing differences between the images in Figure 1(b) and Figure 2(b), (d) Stego image after LSB sequential embedding with one character per two pixels, (e) Histogram of the image in (d), (f) Histogram highlighting changes between Figure 1(b) and Figure 2(e), (g) Stego image after LSB embedding with random pixel selection, (h) Histogram of the image in (g), (i) Histogram showing differences between Figure 1(b) and Figure 2(h), (j) Stego image after LSB random embedding with one character per two pixels, (k) Histogram of the image in (j), (l) Histogram illustrating the change between Figure 1(b) and Figure 2(j), (m) Stego image obtained using the proposed algorithm, (n) Histogram of the image in (m), (o) Histogram comparing changes between Figure 1(b) and Figure 2(m), (p) LOG table generated

after applying the proposed steganography method on the image shown in Figure 1(a) Figure 2(d) presents the image after embedding the text message using sequential pixel selection, where each character byte is distributed across two consecutive pixels. Figure 2(e) shows the corresponding histogram. Comparing Figure 1(a) (p) and Figure 2(a) along with their respective histograms in Figure 1(b) and Figure 2(b) reveals only minor changes in image quality, which are imperceptible to the human eye. To highlight these subtle modifications, the difference between the histograms is calculated and illustrated in Figure 2(f) using red lines. Although minimal, these changes confirm the effects of embedding text through sequential pixel selection, where one character is divided between two adjacent pixels. Specifically, one bit modifies the LSB of the Red component, the next bit modifies the LSB of the Green component, and the following two bits modify the blue component of the first pixel. The same pattern is then applied to the second pixel in the same sequence.

Figure 2(g) displays the stego image obtained using random pixel selection for embedding the text, with its histogram shown in Figure 2(h). While visual differences between the original and stego image remain imperceptible, their histogram differences are illustrated in Figure

2(i). The changes observed in Figure 2(i) are like those in Figure 2(c); however, due to random pixel selection, modifications are distributed across the image rather than occurring in a structured manner.

Figure 2(j) shows the stego image produced using a method like Figure 2(d) but with randomly selected pixels instead of sequential placement. Figure 2(k) presents its histogram, while Figure 2(l) highlights the histogram differences between Figure 2(b) and Figure 2(k). The observed changes are comparable to those in sequential embedding across two pixels per character, but random selection disperses the alterations throughout the image. These conventional data embedding techniques share similarities and cause detectable modifications in image quality, making them susceptible to detection by automated steganalysis systems. In contrast, Figure 2(m) displays the stego image generated using the proposed novel steganography method, embedding the same 34,000-character text file. Figure 2(n) shows its corresponding histogram, and Figure 2(o)

confirms that the proposed method does not alter the pixels of the cover image. Instead of modifying pixel values, a pattern selection technique extracts bit patterns from the byte values of different color components, preserving the original image. The extracted information is systematically stored in a LOG table, as depicted in Figure 2(p), ensuring secure and undetectable data embedding without affecting image quality.

Conclusion

In this research, we proposed and implemented a novel steganographic method that ensures high efficiency, with less than a 1% probability of altering image quality. The method demonstrated impressive results across various image types. It works by partitioning the textual message into three segments and identifying their patterns within pixel components. Upon successfully matching character bit sequences, the extracted information is packed into bytes and stored in a LOG table, which is subsequently encrypted using the Rijndael Managed encryption algorithm for secure transmission. Experimental results indicate that over 99% of images already contain these patterns, eliminating the need for any pixel modifications to embed data. The LOG table serves as a secret key, removing the necessity of an additional encryption key for secure communication.

Future research will focus on optimizing the algorithm for different image formats and resolutions while exploring its real-time application potential. Additionally, integrating machine learning techniques to automate pattern detection could enhance robustness against steganalysis. Further investigations will extend the applicability of this method to multimedia formats beyond images, including audio and video streams, expanding its utility for secure data transmission.

REFERENCES

[1] G. Gilanie et al., "Coronavirus (COVID-19) detection from chest radiology images using convolutional neural networks," Biomedical Signal Processing and Control, vol. 66, p. 102490, 2021.

[2] E. A. Khera et al., "Characterization of Nickel Oxide Thin Films for Smart Window Energy Conversion Applications: Comprehensive Experimental and Computational Study," Available at SSRN 4235112.

[3] G. Gilanie, N. Nasir, U. I. Bajwa, and H. Ullah, "RiceNet: convolutional neural networks-based model to classify Pakistani grown rice seed types," Multimedia Systems, pp. 1-9, 2021.

[4] E. Wazir, G. Gilanie, N. Rehman, H. Ullah, and M. F. Mushtaq, "Early Stage Detection of Cardiac Related Diseases by Using Artificial Neural Network," in International Conference on Soft Computing and Data Mining, 2022, pp. 361-370: Springer.

[5] G. Gilanie et al., "Digital Image Processing for Ultrasound Images: A Comprehensive," Digital Image Processing, vol. 15, no. 3, 2021.

[6] G. Gilanie, U. I. Bajwa, M. M. Waraich, Z. Habib, H. Ullah, and M. Nasir, "Classification of normal and abnormal brain MRI slices using Gabor texture and support vector machines," Signal, Image and Video Processing, vol. 12, pp. 479- 487, 2018.

[7] M. Yaseen et al., "In-vitro Evaluation of Anticancer Activity of Rhodamine-640 perchlorate on Rhabdomyosarcoma cell line," 2022.

[8] M. Attique et al., "Colorization and automated segmentation of human T2 MR brain images for characterization of soft tissues," PloS one, vol. 7, no. 3, p. e33616, 2012.

[9] G. Gilanie, M. Attique, S. Naweed, E. Ahmed, and M. Ikram, "Object extraction from T2 weighted brain MR image using histogram based gradient calculation," Pattern Recognition Letters, vol. 34, no. 12, pp. 1356-1363, 2013.

[10] M. J. Iqbal, U. I. Bajwa, G. Gilanie, M. A. Iftikhar, and M. W. Anwar, "Automatic brain tumor segmentation from magnetic resonance images using superpixel-based approach," Multimedia Tools And Applications, vol. 81, no. 27, pp. 38409-38427, 2022.

[11] H. A. Hafeez et al., "A CNN-model to classify low-grade and high-grade glioma from mri images," IEEE Access, vol. 11, pp. 46283-46296, 2023.

[12] G. Gilanie et al., "An Overview on X-Rays ImagesProcessing: Methods, Challenges& Issues, and Future Work."

[13] G. Gilanie, "Automated Detection and Classification of Brain Tumor from MRI Images using Machine Learning Methods," Department of Computer Science, COMSATS University Islamabad, Lahore campus, 2019.

[14] F. Afzal et al., "Detection of Uric Acid in UV-VIS wavelength Regime," JOURNAL OF NANOSCOPE (JN), vol. 4, no. 1, pp. 75-81, 2023.

[15] A. A. Ghaffar et al., "Refined Sentiment Analysis by Ensembling Technique of Stacking Classifier," in International Conference on Soft Computing and Data Mining, 2022, pp. 380-389: Springer.

[16] H. U. Janjua and G. G. Janjua, "Histogram based spectroscopy of T2 weighted brain MR image for object."

[17] G. Gilanie, U. I. Bajwa, M. M. Waraich, and Z. Habib, "Computer aided diagnosis of brain abnormalities using texture analysis of MRI images," International Journal of Imaging Systems and Technology, vol. 29, no. 3, pp. 260-271, 2019.

[18] H. Ullah, G. Gilanie, F. Hussain, and E. Ahmad, "Autocorrelation optical coherence tomography for glucose quantification in blood," Laser Physics Letters, vol. 12, no. 12, p. 125602, 2015.

[19] S. N. Batool et al., "Forensic Radiology: A robust approach to biological profile estimation from bone image analysis using deep learning," Biomedical Signal Processing and Control, vol. 105, p. 107661, 2025.

[20] A. Nazir, H. Ullah, G. Gilanie, S. Ahmad, Z. Batool, and A. Gadhi, "Exploring Breast Cancer Texture Analysis through Multilayer Neural Networks," Scientific Inquiry and Review, vol. 7, no. 3, pp. 32- 47, 2023.

[21] G. Gilanie, U. I. Bajwa, M. M. Waraich, and M. W. Anwar, "Risk-free WHO grading of astrocytoma using convolutional neural networks from MRI images," Multimedia Tools and Applications, vol. 80, no. 3, pp. 4295-4306, 2021.

[22] G. Gilanie, N. Rehman, U. I. Bajwa, S. Sharif, H. Ullah, and M. F. Mushtaq, "FERNet: A Convolutional Neural Networks Based Robust Model to Recognize Human Facial Expressions," in International Conference on Soft Computing and Data Mining, 2022, pp. 353-360: Springer.

[23] S. F. Rubab et al., "The Comparative Performance of Machine Learning Models for COVID-19 Sentiment Analysis," in International Conference on Soft Computing and Data Mining, 2022, pp. 371-379: Springer.

[24] E. A. Khera et al., "Characterizing nickel oxide thin films for smart window energy conversion applications: Combined experimental and theoretical analyses," ChemistrySelect, vol. 8, no. 37, p.e202302320, 2023.

[25] G. Gilanie et al., "An Automated and Real-time Approach of Depression Detection from Facial Micro-expressions," Computers, Materials & Continua, vol. 73, no. 2, 2022.

[26] A. Saher, G. Gilanie, S. Cheema, A. Latif, S. N. Batool, and H. Ullah, "A Deep Learning-Based Automated Approach of Schizophrenia Detection from Facial Micro-Expressions," Intelligent Automation & Soft Computing, vol. 39, no. 6, 2024.

[27] N. F. Johnson, Z. Duric, and S. Jajodia, Information hiding: steganography and watermarking-attack and countermeasures: steganography and watermarking: attacks and countermeasures. Springer Science & Business Media, 2001.

[28] G. Gilanie et al., "A Robust Method of Bipolar Mental Illness Detection from Facial Micro Expressions Using Machine Learning Methods," Intelligent Automation & Soft Computing, vol. 39, no. 1, 2024.

[29] M. S. Rashid, G. Gilanie, S. Naveed, S. Cheema, and M. Sajid, "Automated detection and classification of psoriasis types using deep neural networks from dermatology images," Signal, Image and Video Processing, vol. 18, no. 1, pp. 163-172, 2024.

[30] M. Ghani and G. Gilanie, "The IOMT-Based Risk-Free Approach to Lung Disorders Detection from Exhaled Breath Examination," INTELLIGENT AUTOMATION AND SOFT COMPUTING, vol. 36, no. 3, pp. 2835-2847, 2023.

[31] A. Anderson, "Steganography: an Inside Look at Hiding Messages and Data," University of Exeter, 2006.

[32] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," Computer, vol. 31, no. 2, pp. 26-34,1998.

[33] Z. N. Al-Kateeb, M. J. Al-Shamdeen, and F. S. Al-Mukhtar, "Encryption and Steganography a secret data using circle shapes in colored images," in Journal of Physics: Conference Series, 2020, vol. 1591, no. 1, p. 012019: IOP Publishing.

[34] S. Rahman et al., "A novel approach of image steganography for secure communication based on LSB substitution technique," Computers, Materials & Continua, vol. 64, no. 1, pp. 31-61, 2020.

[35] S. K. Bandyopadhyay, D. Bhattacharyya, D. Ganguly, S. Mukherjee, and P. Das, "A tutorial review on steganography," in International conference on

contemporary computing, 2008, vol. 101, pp. 105-114.

[36] G. Gilanie, U. I. Bajwa, M. M. Waraich, and Z. Habib, "Automated and reliable brain radiology with texture analysis of magnetic resonance imaging and cross datasets validation," International Journal of Imaging Systems and Technology, vol. 29, no. 4, pp. 531-538, 2019.

[37] M. K. I. Rahmani, K. Arora, and N. Pal, "A crypto-steganography: A survey," International Journal of Advanced computer science and applications, vol. 5, no. 7, 2014.

[38] K. Challita and H. Farhat, "Combining steganography and cryptography: new directions," International Journal on New Computer Architectures and Their Applications (IJNCAA), vol. 1, no. 1, pp. 199-208, 2011.

[39] K. Asghar, G. Gilanie, M. Saddique, and Z. Habib, "Automatic Enhancement of Digital Images Using Cubic BÃ© zier Curve And Fourier Transformation," Malaysian Journal of Computer Science, vol. 30, no. 4, pp. 300-310, 2017.

[40] H. Ullah et al., "Proteins and Triglycerides Measurement in Blood Under Ultraviolet (UV)/Visible (Vis) Spectroscopy at & lambda;= 190 to 1100 nm with an Additional He-Ne Laser Source," LASERS IN ENGINEERING, vol. 55, no. 3-6, pp. 157-167, 2023.

[41] L. Almazaydeh, "Secure RGB image steganography based on modified LSB substitution," International Journal of Embedded Systems, vol. 12, no. 4, pp. 453-457, 2020.

[42] H. U. Janjua, A. Jahangir, and G. Gilanie, "Classification of chronic kidney diseases with statistical analysis of textural parameters: a data mining technique," International Journal of Optical Sciences, vol. 4, no. 1, pp. 1-7, 2018.

[43] H. Ullah, G. Gilanie, M. Attique, M. Hamza, and M. Ikram, "M-mode swept source optical coherence tomography for quantification of salt concentration in blood: an in vitro study," Laser Physics, vol. 22, pp. 1002-1010, 2012.

[44] A. S. Ansari, M. S. Mohammadi, and M. T. Parvez, "A multiple-format steganography algorithm for color images," IEEE Access, vol. 8, pp. 83926-83939, 2020.

[45] S. Bhattacharyya, "A survey of steganography and steganalysis technique in image, text, audio and video as cover carrier," Journal of global research in computer science, vol. 2, no. 4, 2011.

[46] T. Morkel, J. H. Eloff, and M. S. Olivier, "An overview of image steganography," in Issa, 2005, vol. 1, no. 2, pp. 1-11.

[47] A. Kumar, R. Rani, and S. Singh, "A survey of recent advances in image steganography," Security and Privacy, vol. 6, no. 3, p. e281, 2023.

[48] H. Ullah et al., "Assessing Graphene Oxide (GO) and CuO Nanocomposites for Effective Antibacterial Properties Using Laser Interferometry," Lasers in Engineering (Old City Publishing), vol. 55, 2023.

[49] S. Asghar et al., "Water classification using convolutional neural network," IEEE Access, vol. 11, pp. 78601-78612, 2023.

[50] S. N. Batool and G. Gilanie, "CVIP-Net: A Convolutional Neural Network-Based Model for Forensic Radiology Image Classification," Computers, Materials & Continua, vol. 74, no. 1, 2023.

[51] G. Gilanie, U. I. Bajwa, M. M. Waraich, M. W. Anwar, and H. Ullah, "An automated and risk free WHO grading of glioma from MRI images using CNN," Multimedia tools and applications, vol. 82, no. 2, pp. 2857-2869, 2023.

[52] M. Amjad, H. Ullah, F. Andleeb, Z. Batool, A. Nazir, and G. Gilanie, "Fourier- Transform Infrared Spectroscopy (FTIR) for Investigation of Human Carcinoma and Leukaemia," Lasers in Engineering (Old City Publishing), vol. 51, 2021.

[53] G. Gilanie, H. Ullah, M. Mahmood, U. I. Bajwa, and Z. Habib, "Colored

Representation of Brain Gray Scale MRI Images to potentially underscore the variability and sensitivity of images," Current Medical Imaging Reviews, vol. 14, no. 4, pp. 555-560, 2018.

[54] H. Ullah, A. Batool, and G. Gilanie, "Classification of Brain Tumor with Statistical Analysis of Texture Parameter Using a Data Mining Technique," International Journal of Industrial Biotechnology and Biomaterials, vol. 4, no. 2, pp. 22-36, 2018.

[55] H. Shafiq, G. Gilanie, M. Sajid, and M. Ahsan, "Dental radiology: a convolutional neural network-based approach to detect dental disorders from dental images in a real-time environment," Multimedia Systems, vol. 29, no. 6, pp. 3179-3191, 2023.

[56] S. Naveed et al., "Drug efficacy recommendation system of glioblastoma (GBM) using deep learning," IEEE Access, 2024.

[57] M. Rafiq, U. I. Bajwa, G. Gilanie, and W. Anwar, "Reconstruction of scene using corneal reflection," Multimedia Tools and Applications, vol. 80, no. 14, pp. 21363-21379, 2021.

[58] M. Ahmed, G. Gilanie, M. Ahsan, H. Ullah, and F. A. Sheikh, "Review of Artificial Intelligence-based COVID-19 Detection and A CNN-based Model to Detect Covid-19 from X-Rays and CT images," VFAST Transactions on Software Engineering, vol. 11, no. 2, pp. 100-112, 2023.

[59] H. U. Janjua, F. Andleeb, S. Aftab, F. Hussain, and G. Gilanie, "Classification of liver cirrhosis with statistical analysis of texture parameters," International Journal of Optical Sciences, vol. 3, no. 2, pp. 18-25, 2017.

[60] G. Gilanie et al., "RiceAgeNet: Age Estimation of Pakistani Grown Rice Seeds using Convolutional Neural Networks."

[61] H. Ullah, M. Faran, Z. Batool, A. Nazir, G. Gilanie, and N. Amin, "Diagnosis of Ocular Diseases Using Optical Coherence Tomography (OCT) at λ= 840 nm," Lasers in Engineering (Old City Publishing), vol. 53, 2022.

[62] U. I. Bajwa, A. A. Shah, M. W. Anwar, G. Gilanie, and A. Ejaz Bajwa, "Computer-aided detection (CADe) system for detection of malignant lung nodules in CT slices-a key for early lung cancer detection," Current Medical Imaging, vol. 14, no. 3, pp. 422-429, 2018.

[63] G. Gilanie, "Spectroscopy of T2 weighted brain MR image for object extraction using prior anatomical knowledge based spectroscopic histogram analysis," 2013.