



## Steganalysis Secret Message Using Rich Model Method for Stego Color Image

Fatimah Husam Kamil<sup>\*ID</sup>, Maisa'a Abid Ali Khodher<sup>ID</sup>, Layth Kamil Adday<sup>ID</sup>

Department of Computer Engineering, University of Technology, Baghdad 10011, Iraq

Corresponding Author Email: [ce.22.08@grad.uotechnology.edu.iq](mailto:ce.22.08@grad.uotechnology.edu.iq)

Copyright: ©2025 The authors. This article is published by IETA and is licensed under the CC BY 4.0 license (<http://creativecommons.org/licenses/by/4.0/>).

<https://doi.org/10.18280/ijssse.150710>

### ABSTRACT

**Received:** 12 March 2025

**Revised:** 10 May 2025

**Accepted:** 10 July 2025

**Available online:** 31 July 2025

#### **Keywords:**

*color-image, rich model, secure message, steganalysis, feature extraction, deep learning*

An important field of research called steganalysis looks for and extracts hidden messages that are contained in digital media. In order to discover and extract secret information from stego color images, this research focuses on using the rich model method. The rich model employs advanced statistical feature extraction techniques to uncover minor patterns and anomalies introduced during the embedding process. The suggested solution begins by preprocessing the stego image and extracting features using the rich model framework. Specifically, it targets steganographic techniques that operate in the spatial domain, particularly those using Least Significant Bit (LSB) embedding. The secret information is then translated into binary bits when pixel intensity variations are analyzed to find it. The original secret message is recreated by mapping these bits to ASCII characters. Experimental results confirm the method's effectiveness in accurately retrieving hidden content from color images. The technique exhibits strong performance in identifying and removing embedded data from color images with a high degree of efficiency and accuracy. This contribution supports the development of practical tools for digital content verification and secure communication. This work offers an efficient method for detecting hidden messages in multimedia images while also advancing steganalysis methods.

## 1. INTRODUCTION

As communication and internet technologies have advanced, a significant volume of images is shared via public networks. Has recently been discovered that a large number of criminal organizations use images to distribute their illegal data. These organizations use images to hide their harmful data [1]. They typically use steganography techniques for hiding their dangerous material within images [2]. As a result, scientists have begun using steganalysis models to identify images with embedded data. Therefore, one method for identifying data hidden in images is image steganalysis. As a result, steganalysis determines if the provided image is a normal image or a stego-embedded one [3].

Embedding hidden messages into an image such that only the intended recipients can recognize them is the aim of image steganography. It can be used to integrate patient data into medical images, personal information into smart ID (identification card) photos, and copyright information into professional images [4]. Image steganalysis is a technique used to try and find hidden messages in images [5]. As image steganography has advanced, numerous steganalysis techniques have been created to address these new developments [6]. Early on, it is presumed that some knowledge of steganographic algorithms that embed a secret message into images is already known [7]. We refer to this as targeted steganalysis, but in recent years, a more likely scenario has received greater attention. In other words, there is no knowledge about steganographic algorithms [8]. Blind

steganalysis is the process of attempting to distinguish between stego and cover images without being knowledgeable about steganographic embedding approaches [9]. We can create a classifier that distinguishes between cover and stego images in the feature space by using features taken from a training set of cover and stego images [10].

However, many existing steganalysis methods suffer from critical limitations. These include poor performance when dealing with high-resolution or color images, low generalization across various steganographic algorithms, and vulnerability to adaptive or content-aware embedding techniques that minimize detectable traces. Furthermore, traditional methods often rely on handcrafted features, which may not adequately capture the subtle statistical differences caused by data embedding. To address these challenges, the proposed method utilizes the Rich Model framework, which extracts high-dimensional statistical features and captures pixel-level intensity differences across color channels. This approach enables more accurate detection of hidden messages.

In 2020, Mohamed et al. [11] discussed how Deep Learning algorithms have outperformed conventional techniques in both the spatial and transform domains when used in steganalysis. Even better results have been achieved when steganalysis utilizing Deep Learning is combined with manual feature extraction and classification phases. Since this field is still developing and the initial results are encouraging, the authors suggest working on image steganalysis using deep learning.

In 2020, Xu [12] proposed the technique outperforms the One-class SVM methodology for anomaly identification and

for both steganographic and non-steganographic texts, the Type-1 Model's results demonstrate good precision, recall and F1-measure scores. Additionally, the LSTM and BI-LSTM models show strong text steganalysis precision, recall, and F1 measure scores. Thus, without the need for human interaction, the unsupervised deep learning method successfully detects text steganography in a completely unsupervised approach.

In 2021, Yamini et al. [13] proposed an adaptive image steganalysis system that used the support vector machine (SVM) classifier, achieving a 96.72% classification accuracy. As a result, the enhanced canny edge detection algorithm was selected for edge recognition in the suggested system after outperforming other segmentation algorithms.

In 2021, You et al. [14] proposed an innovative, deep learning, end-to-end method that delivers satisfactory performance for separating steganography images from original images. When producing the final classification based on the relationships between the noise of various image sub-regions, the suggested network first accepts the image as input. Preprocessing, feature extraction, and fusion/classification are the three steps of the algorithm's Siamese CNN-based architecture, which comprises two symmetrical subnets with common parameters. Generated datasets that included steganography images in various sizes and the equivalent normal images from BOSS-base 1.01 and ALASKA were used to validate the network. Our suggested network is flexible and well-generalized, according to experimental results derived from data collected through several methods.

In 2022, Vilkhovskiy [15] proposed that the algorithm utilized in the study can identify an area with a high density of unique pixel combinations and locate an LSB-insert and its location due to the steganalysis approach that was proposed and demonstrated in the study to have high detection and locating accuracy in a low stego payload of 25/10. Thus, LSB inserts in low stego-payload fake color images are successfully detected and located by the provided method.

## 2. STEGANALYSIS

The study of finding concealed information in digital media, such as text, audio files, movies, or images that have been inserted using steganography techniques, is known as steganalysis. Steganalysis seeks to uncover the existence of this hidden data, frequently without being aware of the embedding technique beforehand, while steganography works on safely hiding data to guarantee undetectability. Digital rights management, forensic analysis, and cybersecurity all heavily rely on this field [16].

The growing sophistication of steganographic techniques and the widespread use of digital communication have greatly increased the importance of steganalysis. For instance, secret communication techniques have been used for both legal (like digital authentication and watermarking) and illegal (like malware distribution and data exfiltration) objectives [17].

Two major categories can be used to classify steganalysis techniques:

1. Targeted steganalysis: this method looks for steganography that has a known algorithm included in it.
2. Blind Steganalysis: this method, which frequently relies on statistical anomalies in the media, aims to reveal hidden data without the user having any prior knowledge of the embedding approach.

Deep learning and machine learning approaches have been

used in recent steganalysis developments to improve detection skills. A 2023 study, for example, displayed the integration of neural networks with standard algorithms to enhance the reliability of steganographic methods by introducing a steganographic Assistant Convolutional Neural Network (SA-CNN) to increase the resilience of stego-images against detection by steganalysis. These developments show the dynamic character of steganalysis and the constant creation of methods to identify ever-more-advanced steganographic techniques. Deep learning and machine learning techniques have been combined to significantly improve Detection accuracy, making it possible to more successfully detect hidden information in digital media. The field of steganalysis must change with the developments of steganography technology, using creative approaches to show hidden information and maintain the integrity of digital communications [18].

## 3. RICH MODEL

The Rich Model is a high-dimensional feature extraction technique used in steganalysis to capture subtle embedding artifacts in digital images. It operates by applying a variety of high-pass filters to the image to compute residuals that emphasize the noise-like patterns introduced by data hiding processes. These residuals are then used to build co-occurrence matrices that reflect the statistical dependencies between neighboring pixel values.

In the case of color images, the Rich Model is extended to consider inter-channel correlations, such as differences between the red, green, and blue channels (e.g., R-G, G-B). This adaptation allows the model to capture complex embedding traces that may vary across different color components. These residuals are then used to extract higher-order co-occurrence features that capture complex statistical dependencies within the image. The resulting feature set, which can include tens of thousands of descriptors, provides a detailed representation of the image's structural patterns. These features are subsequently fed into a machine learning classifier—such as ensemble-based methods—to determine the presence or absence of hidden information.

By capturing complex dependencies in digital images, especially in color images where inter-channel interactions are intricate, rich models have significantly enhanced steganalysis. These techniques improve the detection of hidden information by extracting high-dimensional feature sets that represent different statistical features of images [19].

Three-dimensional co-occurrences of residuals calculated from all three color channels were introduced in one important application of the spatial rich model to color images. This method improved detection capabilities, particularly for images that included color interpolation artifacts, by successfully capturing dependencies across color channels. Researchers have improved rich models for color image steganalysis by building on this foundation. One method, for instance, was to use co-occurrences of color noise residuals that were divided based on the Bayer color filter array's structure. By taking into consideration the unique features of color image acquisition, this technique aims to enhance detection [20]. Rs analysis integrates a statistical study of the pixel positions where modifications happen with a steganalysis grounded in the Image fidelity metrics. Steganalysis based on image type or embedding method

includes the examination of images—such as those in JPEG format—to identify hidden content, it also includes methods for revealing hidden messages in stego images generated by steganography tools when the embedding algorithm is known. By analyzing selected features from image, artifact detection systems offer techniques to identify differences between the original and steganographic images [21].

#### 4. EVALUATE SYSTEM PROPOSE

Several measurements, such as the peak signal noise ratio (PSNR), Mean Square Error (MSE), histogram, correlation and information entropy, can be used to assess the proposed system. These measurements are used for evaluating any new algorithms. As a result, any new algorithm that exceeds these measurements can be considered good [22].

##### 4.1 Mean Square Error (MSE)

MSE is calculated through a comparison of corresponding byte values between the two images. The pixel consists of 8 bits. Consequently, 256 gray levels can be represented. MSE is useful for comparing the bytes of one image with the corresponding bytes of another image. In Eq. (1), it is used to calculate MSE as follows:

$$MSE = \frac{\sum_{m \times n} [I_1(m \times n) - I_2(m \times n)]^2}{2m \times n} \quad (1)$$

##### 4.2 Peak signal to noise ration

The imperceptibility is measured in dB using the PSNR parameter. It compares pair of images quality. high peak signal-to-noise ratio value suggested these two images were not very different from one another. Otherwise, there is a considerable amount of distortion between two images, as shown by a low PSNR value. PSNR can be achieved by applying the formula below in Eq. (2):

$$PSNR = 1 - \log_{10} \frac{R^2}{MES} \quad (2)$$

##### 4.3 Correlation coefficient (r)

To determine (r), the linear association between the two random variables — range and trend — is computed. when two variables are close to one another, the correlation coefficient (r) is close to one. If the correlation coefficient (r) is close to zero, they are irrelevant. value of (r) in Eq. (3) can be determined by applying the formula below:

$$r = \frac{\sum_i (x_i - x_m)(y_i - y_m)}{\sum_i \sqrt{\sum_i (x_i - x_m)^2} \sqrt{\sum_i (y_i - y_m)^2}} \quad (3)$$

##### 4.4 Histogram

In indexed color picture, histogram that is computed provides a graphical representation which shows the quantity of pixels corresponding to every intensity level or measurement value. It contains essential information for normalizing an image and contributes to a meaningful level of contrast, especially when the image contains a wide range of pixel values. It's possible that this histogram normalization method is evolving. Normalization expanded the domain of

pixel levels is expanded to its maximum extent in order to its full measure so as to improve image contrast. In order to implement this approach, Eq. (4) formulates the process for computing the adjusted pixel value during the equalization step:

$$p(m, n) = \frac{\text{number of pixels with scale level} \leq (m, n)}{\text{Total number of pixels}} \times (\text{maximum scale level}) \quad (4)$$

#### 4.5 Information entropy

Numerous fields, such as machine learning, cryptography, lossless data compression and statistical inference, information entropy (IE) is a key measure of randomness. It serves as an essential property for evaluating image complexity. The distribution of gray values in an image can be measured through this criterion. A higher value of information entropy indicates a more uniform distribution of gray levels. Information Entropy (IE) serves as a key metric for evaluating the security level of a steganographic system. Given m possible elements with associated probabilities, the entropy quantifies the level of uncertainty or randomness within the data distribution,  $P(e_1), P(e_2), \dots, P(e_m)$ , let  $e_1, e_2, \dots, e_m$  [20]. The entropy Eq. (5) is as follows [23]:

$$H(e) = \sum_{i=1}^m P(e_i) \log_2 P(e_i) \quad (5)$$

#### 5. RICH MODEL MEASUREMENTS

Steganalysis is the process of examining digital content, such images, to find hidden messages. A high-dimensional feature set obtained from an image's statistical and spatial properties is used by the rich model, a complete framework. Equations and applications are included in this thorough presentation of the main ideas [24].

##### 5.1 Mean intensity ( $\mu$ )

The mean intensity represents the average brightness of all pixel values in an image. It provides a baseline to identify anomalies embedding process. For a grayscale image with pixel intensities ranging from 0 to 255:

$$\mu = \frac{1}{N} \sum_{i=1}^N I_i \quad (6)$$

where,

- $N$  is the total number of pixels.
- $I_i$  is the intensity of the  $i$ -th pixel.

**Application:** the mean intensity may change somewhat to facilitate identification if embedding changes pixel values in the manner that is desired.

##### 5.2 Standard deviation of intensity ( $\sigma$ )

The standard deviation highlights variances by calculating the distribution of pixel values around the mean. It is computed as follows:

$$\sigma = \sqrt{\frac{1}{N} \sum_{i=1}^N (I_i - \mu)^2} \quad (7)$$

**Application:** local pixel values are frequently changed by embedding, increasing or decreasing intensity variations that can be identified by changes in  $\sigma$ .

### 5.3 Skewness of intensity

The asymmetry of the pixel intensity distribution is measured by skewness. A tail on the right (greater intensity values) is indicative of positive skewness, and a tail on the left is indicative of negative skewness.

$$\text{Skewness} = \frac{\frac{1}{N} \sum_{i=1}^N (I_i - \mu)^3}{\sigma^3} \quad (8)$$

**Application:** skewness is a crucial metric since many steganographic techniques try to prevent symmetry in embedding.

### 5.4 Kurtosis of intensity

Kurtosis quantifies the intensity distribution's "tailenders" or peak sharpness. The calculation for excess kurtosis is:

$$\text{Kurtosis} = \frac{\frac{1}{N} \sum_{i=1}^N (I_i - \mu)^4}{\sigma^4} - 3 \quad (9)$$

**Application:** unusual pixel value clustering brought on by embedding may be indicated by abnormal kurtosis values.

### 5.5 Third moment of intensity ( $M_3$ )

The third moment generates an unnormalized measure of asymmetry, helping detect small distribution changes:

$$M_3 = \frac{1}{N} \sum_{i=1}^N (I_i - \mu)^3 \quad (10)$$

### 5.6 Fourth moment of intensity ( $M_4$ )

An unnormalized indicator of distribution "peakedness" or flatness is given by the fourth moment:

$$M_4 = \frac{1}{N} \sum_{i=1}^N (I_i - \mu)^4 \quad (11)$$

### 5.7 Percentiles of intensity

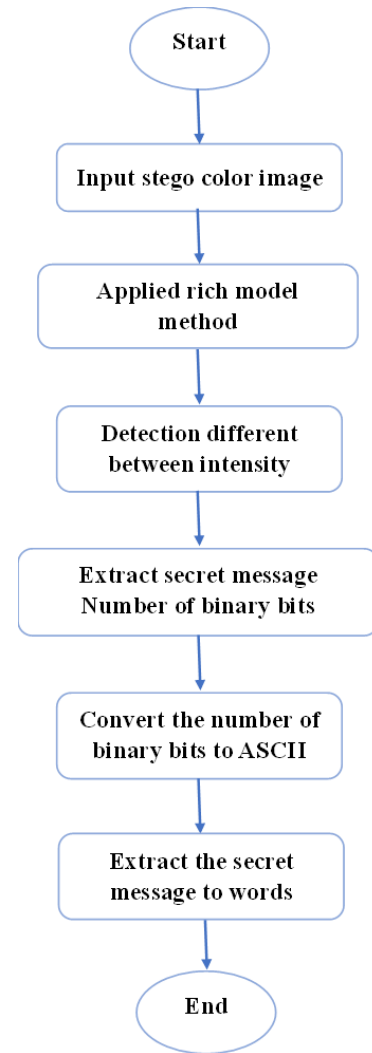
Percentiles are useful for tracking localized changes in intensity because they separate the data into different ranges. For instance:

- $P_{25}$ : 25th percentile (lower quartile)
- $P_{50}$ : Median
- $P_{75}$ : Upper quartile

**Application:** percentiles offer reliable measurements that are not impacted by extreme outliers [25].

## 6. PROPOSED SYSTEM

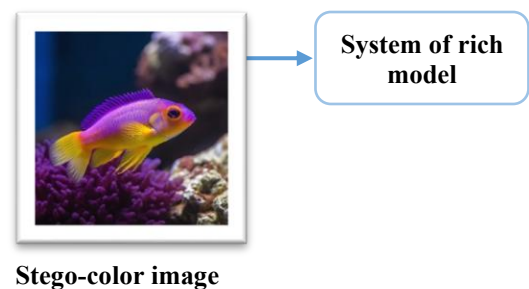
Figure 1 shows the flowchart of the suggested system, which consists of a steps series to steganalysis embedded text within stego color images.



**Figure 1.** Flowchart illustrating the proposed system architecture

#### 1. First step: Input stego-color image into system

To identify hidden messages within a collection of stego-color images, load them into the system in this step then, ensure the input set of color-image is validated to avoid format errors as shown in Figure 2.



**Figure 2.** Load stego-color image into the system

#### 2. Second step: Apply rich model method

Apply the experimental equation and measurements of rich model to extract features from the image. These features should be sensitive to differences caused by data embedding.

#### 3. Third step: Detect differences in intensity

Analyze pixels intensity variations to identify the hidden data patterns. For example, Figure 3.

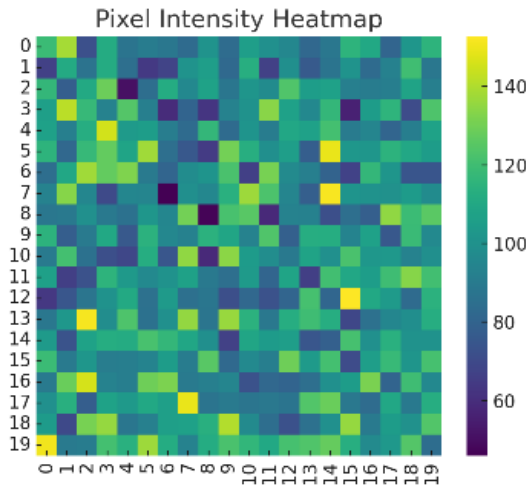


Figure 3. Pixels intensity variations

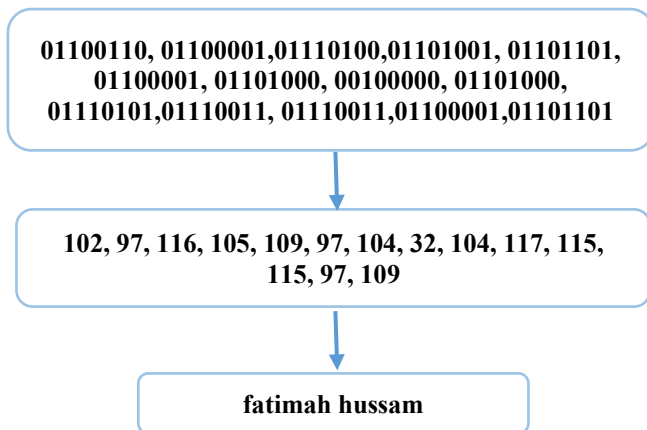


Figure 4. Extracting of the secret message

#### 4. Fourth step: Extract secret message as binary

Translate the identified differences into binary bits representing the hidden message (bits of the secret message are extracted by comparing the number of bits from the LSBs with the MSB in RGB for each pixel).

#### 5. Fifth step: Convert binary bits to ASCII

Map the binary representation to ASCII characters for meaningful interpretation.

#### 6. Sixth step: Extraction secret message as words

This step involved converting each eight-bit ASCII character to a word and then converting the character set to words. This process was applied to all of the bits to produce a large number of secret message words. Figure 4 illustrates these steps.

#### Algorithm: *Extraction Secret Message for Color Image*

```

1: procedure EXTRACTMESSAGE( $I_s$ )
2: Input: Stego color image  $I_s$ 
3: Output: Secret message  $M$ 
4: Step 1: Load Stego Image
5:  $I \leftarrow \text{Load}(I_s)$ 
6: Step 2: Apply Rich Model
7:  $\text{Features} \leftarrow \text{RichModelFeatureExtraction}(I)$ 
8: Step 3: Detect Intensity Differences
9:  $\text{Intensity Diff} \leftarrow \text{AnalyzeDifferences}(\text{Features})$ 
10: Step 4: Extract Binary Bits
11:  $\text{BinaryBits} \leftarrow \text{ExtractBinary}(\text{Intensity Diff})$ 
12: Step 5: Convert Binary to ASCII
13:  $\text{ASCII} \leftarrow \text{BinaryTOASCII}(\text{Binary Bits})$ 
14: Step 6: Construct Secret Message
15:  $M \leftarrow \text{CombineCharacters}(\text{ASCII})$ 
16: Return:  $M$ 
17: end procedure

```

## 7. EXPERIMENTAL RESULTS

This section presents all experimental evaluations conducted on stego color images and the retrieval of hidden messages. Table 1 displays a stego color image and its corresponding cover image. Table 2 presents a comparison of metrics between the stego-color image and the original cover image, including Information Entropy (IE), Mean Square Error (MSE), Correlation Coefficient, and Peak Signal-to-Noise Ratio (PSNR). Meanwhile, Table 3 displays the histogram analysis of both images. stego color image and the cover image. Table 4 shows the result of applying properties of the rich model on the stego color images, and Table 5 shows the result of applying properties of the rich model on color images without stego.

Table 1. Color image sans stego and stego-image

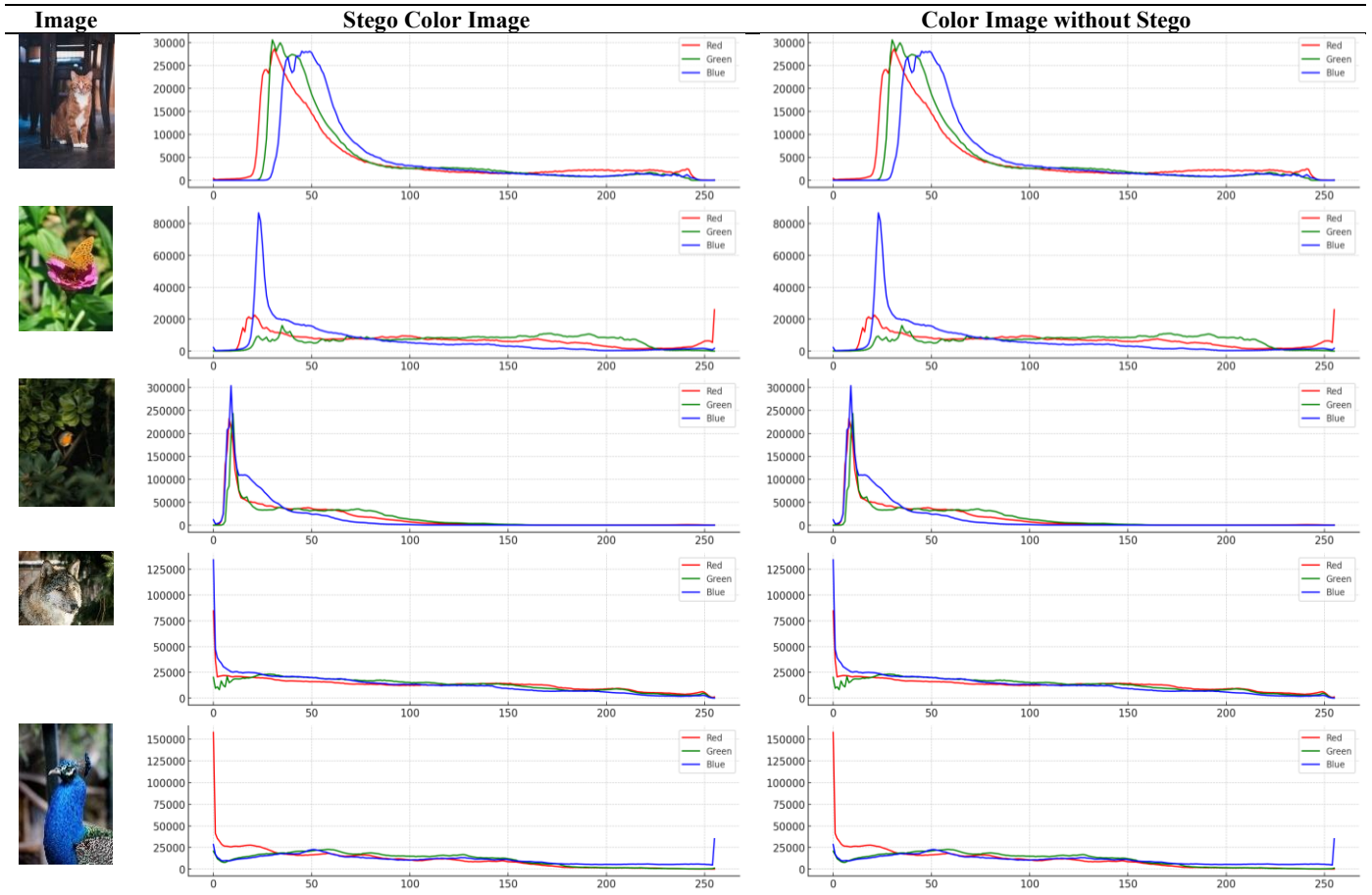
Name of Image	Stego-Color Image	Color Image without Stego
Cat		
Butterfly		



**Table 2.** Measures of, PSNR, information entropy, MSE and correlation coefficient

Name of Image	MSE	PSNR	Correlation Coefficient	Information Entropy
Cat	0.010776678620633763	67.80595429237161	0.9999980653950657	6.7432446
Butterfly	0.02461669921875	64.21850541646545	0.9999970064221525	6.9440966
Bird	0.02073784722222223	64.96316690205225	0.9999871305723075	5.904284

**Table 3.** Histogram comparing stego color image against one without



**Table 4.** Properties of rich model in the stego color images

Name of Image	Cat	Butterfly	Bird
Mean Intensity	73.31910178093848	97.50572943793402	37.42350613064236
Standard Deviation of Intensity	52.77538425499152	64.12122409884232	28.383879190602197
Skewness of Intensity	1.6377093181025637	0.5376593852133252	1.5643909804126652
Kurtosis of Intensity	1.7625564576701738	-0.8010800016136574	4.756312353849365
Third Moment of Intensity	240730.4525394114	141746.59818650442	35773.42749211523
Fourth Moment of Intensity	36945857.71231161	37172061.54120997	5034337.0572594125
Percentiles of Intensity	[39. 52. 85.]	[38. 85. 147.]	[14. 31. 53.]



**Table 5.** Properties of rich model on the color images without stego

Name of Image	Cat	Butterfly	Bird
Mean Intensity	73.3190900042548	97.50531032986112	37.42302652994792
Standard Deviation of Intensity	52.77520286755223	64.12145861213537	28.38468899293303
Skewness of Intensity	1.6377126062037655	0.5376689599888236	1.5642957804160418
Kurtosis of Intensity	1.7625626332413038	-0.8010728885482892	4.755537206984932
Third Moment of Intensity	240728.45371770381	141750.6777271443	35774.31231089577
Fourth Moment of Intensity	36945397.69439377	37172725.5939962	5034408.430931827
Percentiles of Intensity	[39. 52. 85.]	[38. 85. 147.]	[14. 31. 53.]

## 8. ANALYSIS SYSTEM







The following equation in (12) can be used to compute capacity, which is a measure of the system's quality:

$$\text{capacity data stego rate} = \frac{\text{number of secret message}}{\text{size of image}} \quad (12)$$

For instance, using the equation will produce the following results. keep in mind that the hidden image and the original image will have different sizes. The first image (1) in Table 6 has a size of 11990 and a secret text size of 392 bits, that secret message is says "I am a hidden text inside a colorful bird image" the capacity of the image is 0.0000327. On the second image (2) of Table 6, the concealed text "Hello Fatimah Hussam I am a secret message" was extracted. About image size, when picture size is 1687500, hidden text size is 392 bits as result capacity will be equal to 0.000232 In a similar way when secret letter concealed from stego-image is (I am a hidden message in the rich model method), the third image (3) shown in Table 6 has sizes of 27852890 pixels, a message size of 384, and a capacity of 0.0000138. The time required to detect and extract hidden text from stego image is the most crucial of the many factors that need to be taken into consideration. The

requirements of computer use to implement system are the primary determinant of this component. It will take less time to extract hidden message from the color stego image if computer specifications are better. The MES value will be zero and the PSNR value will be infinity if the system is applied to couple of identical images. To add clarity, we compared the histogram results between the proposed system in this research paper and previous works, as shown in Table 7. This comparison shows the differences between the distribution patterns in the proposed system and previous works, which provides evidence of the system's effectiveness in handling with image characteristics. Then there is another comparison using the rich model features between the results that appeared in the proposed system and the results included in the related works as is clear in Table 8, where the table shows the results of the superiority of the proposed system in many measures and highlights its strengths and improvements in discovering hidden information. Finally, to provide an overview of the performance of the proposed system compared to previous methods in related works, Table 9 summarizes the basic performance metrics and their characteristics. The table supports the analysis and shows the general advantages of the proposed approach.

**Table 6.** Stego and original images for computational analysis

No.of Image	Stego Color Image	Original Image
(1)		
(2)		
(3)		

**Table 7.** Comparison of histogram results between related works and proposed system

No. of Reference	Proposed Method	Histogram
Xu [12]	Unsupervised deep learning for text steganalysis	-

Yamini et al. [13]	Adaptive Image Steganalysis using SVM classifier	
You et al. [14]	Siamese CNN based Architecture	
Vilkhovskiy [15]	LSB-Inserts Detection in Low stego-Payload Artificial Color images	
Proposed system	Steganalysis Secret Message Using Rich Method for Stego color image	

**Table 8.** Comparison of results between related works and proposed system in this paper properties of rich model

No. of Reference	Proposed Method	Mean Intensity	Standard Deviation of Intensity	Skewness of Intensity	Kurtosis of Intensity	Third Moment of Intensity	Fourth Moment of Intensity	Percentiles of Intensity
Mohamed et al. [11]	Deep learning combined with manual feature extraction	-	-	-	-	-	-	-
Xu [12]	Unsupervised deep learning for text steganalysis	-	-	-	-	-	-	-
Yamini et al. [13]	Adaptive Image Steganalysis using SVM classifier	-	-	-	-	-	-	-
You et al. [14]	Siamese CNN based Architecture	-	-	-	-	-	-	-
Vilkhovskiy [15]	LSB-Inserts Detection in Low stego-Payload Artificial Color images	-	-	-	-	-	-	-
Proposed system	Steganalysis Secret Message Using Rich Method for Stego color image	73.319090 0042548	52.775202 86755223	1.63771260620 37655	1.762562633 2413038	240728.4537 1770381	36945397.69 439377	[39. 52. 85.]

**Table 9.** General comparison between the methods of related works and proposed system in this paper

No. of Reference	Proposed Method	Target Data Type	Technique / Model Used	Advantages	Limitations
Mohamed et al. [11]	Deep learning combined with manual feature extraction	Color Images	CNN + Handcrafted Features	High accuracy by combining domain knowledge and learning	Complex, requires longer training and processing time
Xu [12]	Unsupervised deep learning for text steganalysis	Text	Autoencoders or GANs	No need for labeled data, handles hidden patterns	Difficult to evaluate, sometimes less accurate
Yamini et al. [13]	Adaptive Image Steganalysis using	Color Images approaches	SVM + Handcrafted	Simple, works with small datasets	Lower performance compared to deep



SVM classifier			Features		learning
You et al. [14]	Siamese CNN based Architecture	Images	Siamese CNN	Good for comparison- based detection (image pairs)	Requires well-structured input pairs and more training data
Vilkhovskiy [15]	LSB-Inserts Detection in Low stego-Payload Artificial Color images	Low-Payload Images (LSB-based)	Statistical + LSB Detection Techniques	Effective for simple and low-payload steganography	Weak against modern and randomized embedding techniques
Proposed system	Steganalysis Secret Message Using Rich Method for Stego color image	Color Images	Rich Model	Highest detection accuracy using rich statistical features, High performance using high-dimensional co-occurrence features	Requires moderate computational resources

## 9. CONCLUSION

In this work, we introduced a steganalysis method that uses the rich model approach to identify and extract hidden messages in stego color images, making use of sophisticated statistical feature extraction, the technique effectively detects tiny embedding traces, allowing for accurate steganographic content detection. Pixel intensity differences are analyzed, binary data is extracted, and the secret message is systematically reconstructed. Results from experiments show how the rich model is reliable as well as adaptable when analyzing intricate color images while maintaining a high level of message extraction accuracy. Through using many tests in system, such as PSNR, MSE, Correlation, Entropy, and histogram. In addition, measurements of rich model. The suggested approach illustrates how the rich model can be used to improve steganalysis capabilities for data security and digital forensics. Looking forward, future studies may focus on increasing the computational efficiency of the method and extending its applicability to a wider range of steganographic techniques and multimedia formats such as video or audio. Additionally, integrating the proposed technique into real-time systems or digital forensics tools could enhance its practical value in areas like information security, content authentication, and copyright protection. This study highlights the critical importance of advancing steganalysis methods to ensure data confidentiality and integrity in today's increasingly digital environment.

## REFERENCES

- [1] Iskanderani, A.I., Mehedi, I.M., Aljohani, A.J., Shorfuzzaman, M., Akther, F., Palaniswamy, T., Latif, S.A., Latif, A. (2021). Artificial intelligence-based digital image steganalysis. *Security and Communication Networks*, 2021(1): 9923389. <https://doi.org/10.1155/2021/9923389>
- [2] Tan, S., Wu, W., Shao, Z., Li, Q., Li, B., Huang, J. (2020). CALPA-NET: Channel-pruning-assisted deep residual network for steganalysis of digital images. *IEEE Transactions on Information Forensics and Security*, 16, 131-146. <https://doi.org/10.1109/TIFS.2020.3005304>
- [3] Yang, L., Men, M., Xue, Y., Wen, J., Zhong, P. (2021). Transfer subspace learning based on structure preservation for JPEG image mismatched steganalysis. *Signal Processing: Image Communication*, 90: 116052. <https://doi.org/10.1016/j.image.2020.116052>
- [4] Jarrallah, Z.H., Khodher, M.A.A. (2022). Satellite images classification using CNN: A survey. In 2022 International Conference on Data Science and Intelligent Computing (ICDSIC), Karbala, Iraq, pp. 111-116. <https://doi.org/10.1109/ICDSIC56987.2022.10075828>
- [5] Ruan, F., Zhang, X., Zhu, D., Xu, Z., Wan, S., Qi, L. (2020). Deep learning for real-time image steganalysis: A survey. *Journal of Real-Time Image Processing*, 17: 149-160. <https://doi.org/10.1007/s11554-019-00915-5>
- [6] Chaumont, M. (2020). *Deep Learning in Steganography and Steganalysis*. Elsevier, pp. 321-349. <https://doi.org/10.1016/B978-0-12-819438-6.00022-0>
- [7] Yousfi, Y., Fridrich, J. (2020). An intriguing struggle of CNNs in JPEG steganalysis and the OneHot solution. *IEEE Signal Processing Letters*, 27: 830-834. <https://doi.org/10.1109/LSP.2020.2993959>
- [8] Khodher, M.A.A., Alabaichi, A., Altameemi, A.A. (2022). Steganography encryption secret message in video raster using DNA and chaotic map. *Iraqi Journal of Science*, 63(12): 5534-5548. <https://doi.org/10.24996/ij.s.2022.63.12.38>
- [9] Hussain, A.Z., Khodher, M.A.A. (2023). Medical image encryption using multi chaotic maps. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, 21(3): 556-565. <http://doi.org/10.12928/telkomnika.v21i3.24324>
- [10] Mohammed, R.A., Khodher, M.A.A., Alabaichi, A. (2023). Image encryption in IOT using hyper-chaotic system. *International Journal of Intelligent Engineering & Systems*, 16(6): 101-112. <http://doi.org/10.22266/ijies2023.1231.09>
- [11] Mohamed, N., Rabie, T., Kamel, I. (2020). A review of color image steganalysis in the transform domain. In 2020 14th International Conference on Innovations in Information Technology (IIT), Al Ain, United Arab Emirates, pp. 45-50. <https://doi.org/10.1109/IIT50501.2020.9299075>
- [12] Xu, Y. (2020). Unsupervised deep learning for text steganalysis. In 2020 International Workshop on Electronic Communication and Artificial Intelligence (IWEC AI), Shanghai, China, pp. 112-115. <https://doi.org/10.1109/IWEC AI50956.2020.00030>
- [13] Yamini, B., Madhurikkha, S., Chettali, S.H. (2021). Adaptive image steganalysis: Adaptive image segmentation using enhanced canny edge detection algorithm. In Proceedings of the First International Conference on Computing, Communication and Control System, I3CAC 2021, Chennai, India. <https://doi.org/10.4108/eai.7-6-2021.2308867>
- [14] You, W., Zhang, H., Zhao, X. (2020). A Siamese CNN for image steganalysis. *IEEE Transactions on Information Forensics and Security*, 16: 291-306.

- <https://doi.org/10.1109/TIFS.2020.3013204>
- [15] Vilkhovskiy, D.E. (2022). Steganalysis for LSB inserts in low stego-payload artificial color images. *Journal of Physics: Conference Series*, 2182(1): 012102. <https://doi.org/10.1088/1742-6596/2182/1/012102>
- [16] Havard, A., Manikas, T., Larson, E.C., Thornton, M.A. (2023). CNN-assisted steganography-integrating machine learning with established steganographic techniques. *arXiv preprint arXiv:2304.12503*. <https://doi.org/10.48550/arXiv.2304.12503>
- [17] Zhang, Y., Chen, Y., Dou, H., Tan, C., Luo, Y., Sang, H. (2024). Image steganography without embedding by carrier secret information for secure communication in networks. *Plos One*, 19(9): e0308265. <https://doi.org/10.1371/journal.pone.0308265>
- [18] Wen, W., Huang, H., Qi, S., Zhang, Y., Fang, Y. (2024). Joint coverless steganography and image transformation for covert communication of secret messages. *IEEE Transactions on Network Science and Engineering*, 11(3): 2951-2962. <https://doi.org/10.1109/TNSE.2024.3354941>
- [19] Li, Q., Wang, X., Ma, B., Wang, X., Wang, C., Xia, Z., Shi, Y. (2021). Image steganography based on style transfer and quaternion exponent moments. *Applied Soft Computing*, 110: 107618. <https://doi.org/10.1016/j.asoc.2021.107618>
- [20] Michaylov, K.D., Sarmah, D.K. (2025). Steganography and steganalysis for digital image enhanced Forensic analysis and recommendations. *Journal of Cyber Security Technology*, 9(1): 1-27. <https://doi.org/10.1080/23742917.2024.2304441>
- [21] Agarwal, S., Kim, C., Jung, K.H. (2022). Steganalysis of context-aware image steganography techniques using convolutional neural network. *Applied Sciences*, 12(21): 10793. <https://doi.org/10.3390/app122110793>
- [22] Al-Dabbas, M.A.A.K., Alabaichi, A., Abbas, A.S. (2020). Dual method cryptography image by two force secure and steganography secret message in IoT. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, 18(6): 2928-2938. <http://doi.org/10.12928/telkomnika.v18i6.15847>
- [23] Kamil, F.H., Khodher, M.A.A., Adday, L.K. (2025). Steganalysis of secret messages using the blockiness method on stego color images. *International Journal of Safety and Security Engineering*, 15(2): 315-321. <https://doi.org/10.18280/ijss.150212>
- [24] Gonzalez, R.C., Woods, R.E. (2020). *Digital Image Processing*. Upper Saddle River, NJ, USA: Pearson.
- [25] Sonka, M., Hlavac, V., Boyle, R. (2014). *Image Processing, Analysis, and Machine Vision*. Stamford, CT, USA: Cengage Learning.