International Journal of Safety and Security Engineering
Vol. 15, No. 2, February, 2025, pp. 315-321
Journal homepage: http://iieta.org/journals/ijsse

Steganalysis of Secret Messages Using the Blockiness Method on Stego Color Images

Fatimah Husam Kamil*, Maisa'a Abid Ali Khodher, Layth Kamil Adday

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

Corresponding Author Email: ce.22.08@grad.uotechnology.edu.iq

https://doi.org/10.18280/ijsse.150212

Received: 24 December 2024
Revised: 21 January 2025
Accepted: 12 February 2025
Available online: 28 February 2025

Keywords:
steganalysis, color-image, blockiness, secret message, one domination

ABSTRACT

Information hiding is the art of concealing the existence of communication using embedded concealed letters inside unhurt, shown covering color images, detection of hiding, estimate of letters, and its extraction, which belong in the field of steganalysis. Sometimes, there are important messages hidden inside stego-color images. Due to the difficulty of extracting secret messages from color images, this paper proposed a system using the blockiness method to detect and extract secret messages from stego-color images. Using several steps: in the first step, split the size of the stego-color image for 8×8 blocks; in the second step, decompose each block for one domination array according to the size of the image of each block, then search for a hidden message. In the last step, it found a secret message from each pixel in each block by blockiness to find the binary bit from pixels to extract the secret message; this involves converting the binary bit to decimal and converting it to ASCII characters that generate a set of symbols that compress the secret message. The results obtained are efficient, fast, and powerful in detecting secret messages and transparency, by using several measurements, PSNR, MSE, Entropy, correlation, histogram, and capacity to detect the secret message in stego-color images.

1. INTRODUCTION

With 5G technology advances, the number of images transmitted via the Internet of Things is increasing [1]. The massive amounts of images provide many covers for criminals to covertly transmit sensitive company data via image steganography or stolen private [2]. Steganography, an essential part of multimedia security, is a method that hides information from others by embedding it in public carriers and distributing it over public channels [3, 4]. In addition, steganalysis is designed to extract data that Steganography has hidden in order to secure data [5]. The technique used to hide sensitive information in a multimedia cover is called Steganography [6]. Steganalysis, a steganography adversary [7], aims to ascertain whether secret information is included within a multimedia cover [8].

In 2019, Zeng et al. [9] proposed the wider separate-then-reunion network or WISERNet for color image steganalysis. They provided a theoretical defense for the claim that a typical convolution's summation constitutes a particular kind of "linear collusion attack" that preserver highly correlated patterns while destroying uncorrelated noises. Thus, researchers adopted different channel-wise convolutions without summation in the bottom convolutional layer, which aims to suppress correlated image contents. On the other hand, they believe that the summation in standard convolution is helpful in the higher convolutional layers.

Thus, the suggested wide-and-shallow, separate-then-reunion network structure is especially appropriate for color image steganalysis.

In 2019, Sun et al. [10] proposed a novel image steganalysis method based on deep neural networks, wavelet transformation, and feature selection. The method included extracting high-frequency features via wavelet transformation, extracting high-dimensional steganography characteristics using deep neural networks, and selecting informative features based on entropy. The steganalysis model constructed using a parallel SVM model using a huge number of training samples. The effectiveness of the suggested method clarified through the analysis of a practical image steganalysis example. The outcomes showed the effectiveness of the suggested method in detecting hidden messages in images and highlighted its possibility for enhancing steganalysis performance.

In 2020, Neamah et al. [11] proposed a method that produced little distortion and hiding ability. In contrast to the original image, the concealment method, which involved applying the LSB algorithm to hide the encrypted information in a color image, produced a good image resolution after hiding. Mean-squared Error (MSE) and peak signal-to-Noise Ratio (PSNR) were the two measurements used to assess the performance of the suggested technology.

In 2021, Hashim and Alzubaydi [12] proposed in this paper to create a unique CNN framework and an entropy-based regional selection approach to distinguish between a cover image and stego image. This could have increased the detection accuracy of content-adaptive steganographic methods and the technique of finding hidden information in images that allows differentiation between cover and suspect images was known as image steganalysis. Current steganalysis approaches struggled to achieve the required detection performance due to the adaptive integration of knowledge into regions with rich textures. The paper's findings included a method focused on complicated textures in image regions by selecting blocks with the maximum entropy, reducing computing complexity, two subnets with different kernel sizes made up the CNN framework, which enhanced performance with a reasonable number of epochs for training. The experiments conducted in the paper demonstrated that the suggested method improved the detection accuracy of content-adaptive steganographic methods.

In 2021, Singh et al. [13] proposed scheme outperforms the state-of-the-art steganalysis schemes against the state of art, The application of deep learning techniques for steganalysis is discussed in the paper, specifically emphasis on image steganography detection. The authors suggested a method that included learning denoising kernels to obtain more precise noise residuals, these kernels are then used to train a CNN-based steganalysis detector, then improving detection performance. Consequently, the suggested scheme outperforms state-of-the-art steganalysis schemes against state-of-the-art steganographic approaches.

In 2022, Salunkhe and Bhosale [14] proposed and focused on steganalysis, which used global and local information from several embedding domains to show across-domain steganalysis technique that sought to uncover hidden meanings in segno videos. The objective and outcome are to develop and apply video steganography methods in various domains and suggest a deep learning classifier-based cross-domain steganalysis approach for enhanced performance.

In 2024, Sultana et al. [15] proposed a method for edge detection-based data hiding called prediction error Space (PES), which outperformed its competitors regarding payload, stego image quality, and attack resistance. The paper's findings illustrated that the suggested method outperformed current approaches in terms of embedding capacity, stego image quality, and attack resistance.

2. STEGANALYSIS

Steganalysis is the art of countering steganography in a continuous conflict. The goal of passive steganalysis is to destroy evidence of covert communication, not by uncovering the hidden message but by using many methods, such as manipulating image formats, flipping all the least significant bits, or using JPEG compression. Conversely, Active Steganalysis uses advanced algorithms to identify the presence of a stego-image [16]. Steganalysis consists of two primary types: Signature Steganalysis and Statistical Steganalysis. Each type can be either specific, targeting a certain steganographic embedding approach, or universal, which is flexible to any steganographic technique [17], including those that are still to be known [18]. The purpose of steganalysis is to detect covert communication established using steganography. At present, image content adaptation powers most steganographic techniques, which considerably enhances the security of the steganography. This has led to steganalysis challenges of great proportions [19].

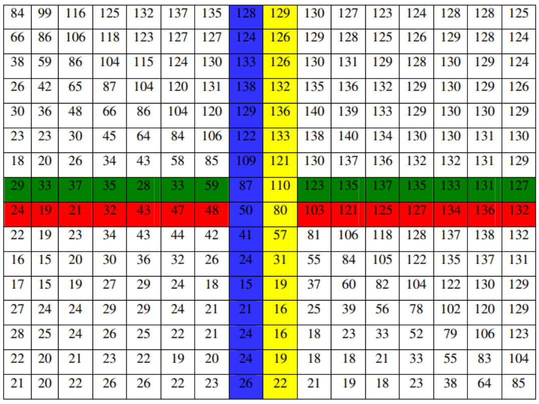
Techniques applied to Steganalysis the following list includes some of the Steganalysis approaches:

1. Visual Detection; 2. Detection of steganographic Artifacts; 3. Steganalysis Based on Image Quality Metrics; 4. First-order statistical Analysis; 5. Steganalysis Based on JPEG Compatibility; 6. RS Analysis; 7. Pairs Analysis; 8. Palette Quick Pairs Analysis; 9. Raw Quick Pairs Analysis; 10. Chi square Attack; 11. Alternative Methods. Visual detection is the process that occurs when the data embedding generates an image that is detectable to the human eye and is different from the original image. As an alternative, visual detection happens by detecting the image's defects and features when the initial image is unexpected. However, in this situation, it will be impossible to tell the difference between self-noise and stego images. It is clear that there is debate on the accuracy of visual detection [20]. Pixel value pairs are the end outcome of embedding data into an image, and steganalysis is used to statistically predict these combinations based on image quality measurements. Rs analysis combines statistical analysis of the pixel position where the change occurs with a steganalysis based on image quality measures. Identifying by type or algorithm includes steganalysis studies of images like JPEG and techniques for revealing the message in a stego image produced by steganography applications where the algorithm is known. An artifact detection system provides methods to differentiate between the original and stego images by extracting specific elements from the image. Fridrich and the other researchers developed an RQP (Raw Quick Pairs) analysis. This technique was developed to analyze similar color image pairs created via LBS hiding. The ratio of comparable color pairings to all color pairs is first computed using the selected image. After hiding the test message in this image, the ratio is then calculated. It is considered that there is no hidden information in the image if there is a noticeable difference between the measured ratios. When ratios are close to one another, it indicates that there is information hidden in the image [21].

3. BLOCKINESS

Blockiness defines the total of the spatial discontinuities at the boundaries of all 8*8 JPEG blocks and calculates the difference between the pixel values at each block's boundaries. Blockiness rating is the result of adding the differences in pixel values for the column and row boundaries. The formula determines the difference at the boundaries of the blocks, except those on the edges, because the blocks at an image's edges do not have boundaries on all sides. Figure 1 shows the General Blockiness illustration on a 16×16 block of greyscale values [22]. Blockiness can be calculated using the bellow formula in Eq. (1):

$$f(x) = a_0 + \sum_{n=1} \left(a_n \cos\frac{n\pi x}{L} + b_n \sin\frac{n\pi x}{L} \right) \tag{1}$$



84	99	116	125	132	137	135	128	129	130	127	123	124	128	128	125
66	86	106	118	123	127	127	124	126	129	128	125	126	129	128	124
38	59	86	104	115	124	130	133	126	130	131	129	128	130	129	124
26	42	65	87	104	120	131	138	132	135	136	132	129	130	129	126
30	36	48	66	86	104	120	129	136	140	139	133	129	130	130	129
23	23	30	45	64	84	106	122	133	138	140	134	130	130	131	130
18	20	26	34	43	58	85	109	121	130	137	136	132	132	131	129
29	33	37	35	28	33	59	87	110	123	135	137	135	133	131	127
24	19	21	32	43	47	48	50	80	103	121	125	127	134	136	132
22	19	23	34	43	44	42	41	57	81	106	118	128	137	138	132
16	15	20	30	36	32	26	24	31	55	84	105	122	135	137	131
17	15	19	27	29	24	18	15	19	37	60	82	104	122	130	129
27	24	24	29	29	24	21	21	16	25	39	56	78	102	120	129
28	25	24	26	25	22	21	24	16	18	23	33	52	79	106	123
22	20	21	23	22	19	20	24	19	18	18	21	33	55	83	104
21	20	22	26	26	22	23	26	22	21	19	18	23	38	64	85

Figure 1. General blockiness illustration on a 16×16 block of greyscale values [22]

4. EVALUATE SYSTEM PROPOSE

Peak signal noise ratio (PSNR), mean square error (MSE), histogram, correlation coefficient, and information entropy are some measurements that can be used to evaluate the proposed system. Any new algorithms are evaluated using these measurements. Therefore, any new algorithm can be considered good when it exceeds these measurements.

4.1 Mean square error

By comparing the bytes of two images, the MSE is calculated. Eight bits make up a pixel. As a result, multiple grey levels can be represented by 256 levels. MSES are helpful for comparing an image's bytes with the comparable bytes of another image. It is utilized in Eq. (2) to determine MSE as below:

$$\mathrm{MSE} = \frac{\sum \mathrm{m} \times \mathrm{n}[\mathrm{I1}(\mathrm{m} \times \mathrm{n}) - \mathrm{I2}(\mathrm{m} \times \mathrm{n})]}{2\mathrm{m} \times \mathrm{n}} \tag{2}$$

4.2 Peak signal to noise ratio

The PSNR parameter that is utilized to compute the imperceptibility in dB. It calculates the quality of two compared images. High PSNR values proposed that there is not much difference between the two images. If not, a low PSNR value indicates that a significant amount of distortion between two images. Using the formula below in Eq. (3) can get PSNR:

$$PSNR = 1 - Log_{10}\frac{R^2}{MES} \tag{3}$$

4.3 Correlation coefficient

The correlation coefficient (r) is determined by calculating the trend and the linear set of two random variables range. The correlation coefficient (r) is near to one when two variables are close to one another. They are irrelevant if the correlation coefficient (r) value is near zero. The bellow formula can be used to get the value of (r) in Eq. (4):

$$\mathrm{r} = \frac{\sum_i (x_i - \mathrm{x}_m)(\mathrm{y}_i - \mathrm{y}_m)}{\sum_i \sqrt{\sum_i (x_i - \mathrm{x}_m)^2}\sqrt{\sum_i (\mathrm{y}_i - \mathrm{y}_m)}^{\,2}} \tag{4}$$

4.4 Histogram

An image's computed histogram is a diagram that displays the number of pixels in each indicator or degree measure on the indexed color image. When an image's pixels are lengthy, the histogram holds the information needed to normalize the image and provide a reasonable degree of dissimilarity. This histogram normalizing technique might be changing. In order to increase the image's dissimilarity, normalization developed the pixel levels measure domain to its full measure. In order to implement this method, Eq. (5) redefines the equalization of the new pixel value:

$$p(m,n) = \frac{number\ of\ pixels\ with\ scale\ level \leq (m,n)}{Total\ number\ of\ pixels} \times (maximum\ scale\ level) \tag{5}$$

4.5 Information entropy

Statistical inference, lossless data compression, cryptography, and machine learning are among the many fields that use information entropy (IE), an essential randomization feature. The gray value distribution inside the image can be quantified using this criterion. The distribution of gray values is uniform when the information entropy is high. The security of a steganographic system is measured using information entropy. Let e1, e2, ..., em be m possible elements with probabilities P (e1), P (e2), ..., P (em) [23]. The following is the entropy Eq. (6):

$$H(e) = \sum_{i=0}^{m-1} P(e_i) log\ _2 P(e_i) \tag{6}$$

5. PROPOSED SYSTEM

The proposed system involves a set of steps to steganalysis secret message from color image (Figure 2). A flowchart of the proposed system is shown.

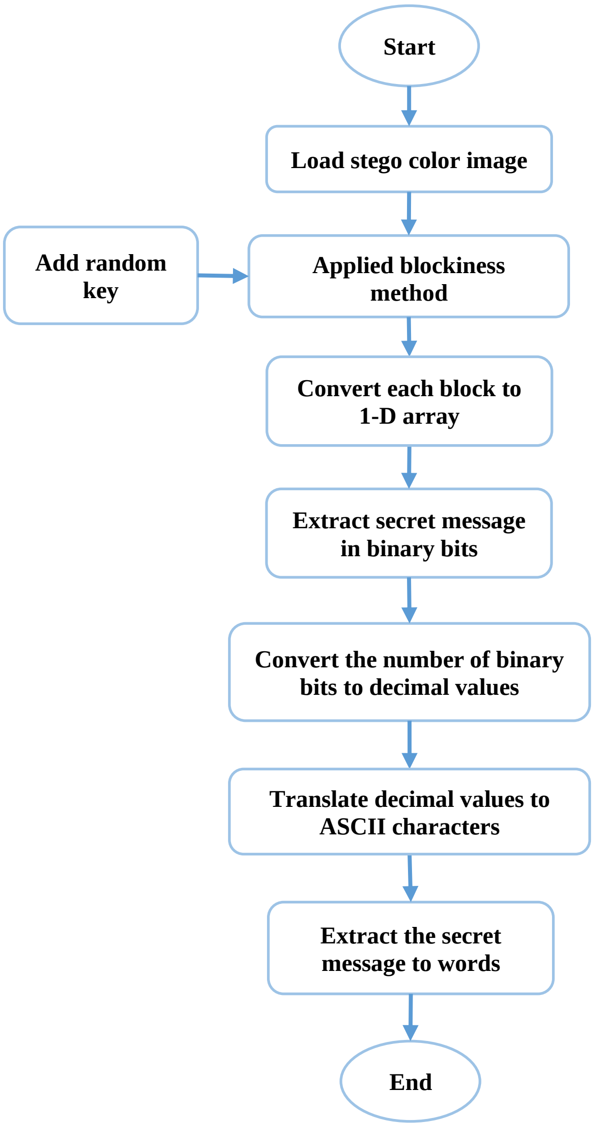

Start
Load stego color image
Add random key
Applied blockiness method
Convert each block to 1-D array
Extract secret message in binary bits
Convert the number of binary bits to decimal values
Translate decimal values to ASCII characters
Extract the secret message to words
End

Figure 2. The flowchart of proposed system

1. **First step: stego-color image**

Load a set of stego-color images in the system to detect a secret message in the image using the key attack, as shown in Figure 3. The attacker searches each pixel in the color image for the pixel of RGB to find a secret message and then exist it.

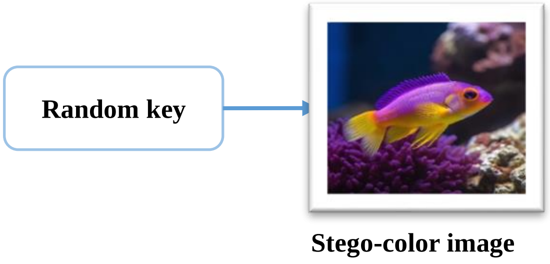
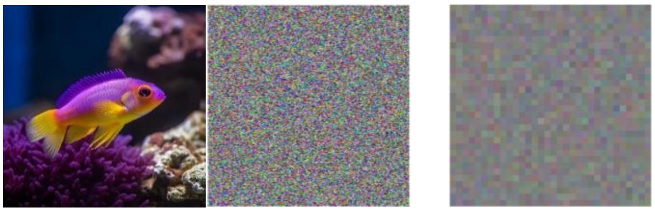


Figure 3. Detection secret message in stego-image using key

2. **Second step: applied blockiness method**

In this step, the blockiness method was applied on the stego-color image, then divided the image into 8×8 blocks by using Eq. (7), as shown in Figure 4. Applied blockiness with RGB in each pixel in color-image. Repeat the step to access eight blockiness in the steganography image.



(a) Original stego-color image (b) 8×8 block

Figure 4. Divide stego-color image into 8×8 blocks

$$\begin{gathered} Block\ size\ of\ image = 8bit \\ image = 0 \\ image = block\ size + 1 \end{gathered} \tag{7}$$

3. **Third step: extract binary secret message**

In this step, convert each block into a 1-D array whose size varies depending on the stego-color image size. Then, using try key attack for each block for stego-color image blockiness to extract the number of bits from LSB comparing with MSB in RGB in each pixel to obtain bits of secret message in binary.

4. **Fourth step: extraction secret message**

In this step, convert every binary bit's number to decimal, then convert each 8-bit by ASCII to a character and convert the set of characters to a word; apply this operation on all bits to obtain many words of secret message, such as in Figure 5.

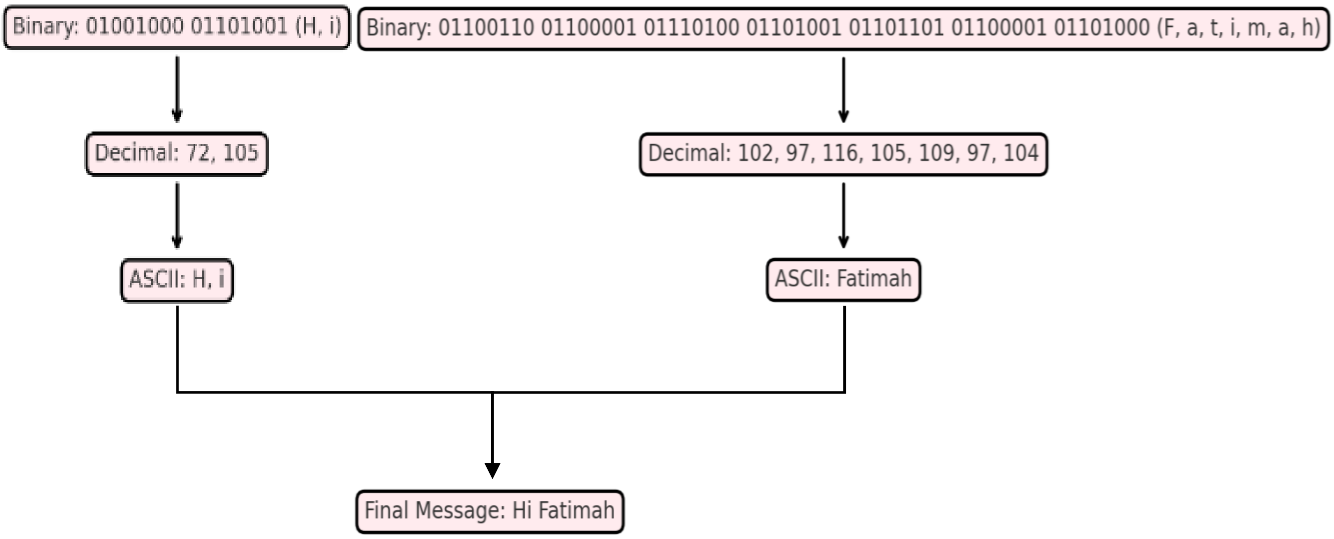

Binary: 01001000 01101001 (H, i)
Binary: 01100110 01100001 01110100 01101001 01101101 01100001 01101000 (F, a, t, i, m, a, h)
Decimal: 72, 105
Decimal: 102, 97, 116, 105, 109, 97, 104
ASCII: H, i
ASCII: Fatimah
Final Message: Hi Fatimah

Figure 5. Process of convert binary bits into word and extract the secret message

Extraction algorithm

```
Process:
Input: stego color image
Output: extraction secret message
Initial;
A= Load stego color image
B= Applied blockiness
C= key attack
D= extraction number of bits
E= extraction secret message
Step1: Load stego-color image in A.
Step2: Applied blockiness to divide stego-color image to set of blocks 8×8 in B.
Step3: Load key attack in C.
Step4: Extraction no. of bits from LSB in RGB of pixels by using key attack on each block in D.
Step5: Extraction number of binary bits for secret message by convert number of bits in ASCII to convert each 8 bits to word in E.
Step6: Put (this results secret message) in E.
End
```

6. TEST OF THE RESULT

This part shows all tests in stego-color and extraction secret message, whereas Table 1 indicates stego-color images and images without stego. Table 2 indicates the measurements between stego-color images and images without stego in mean square error (MSE), Peak signal-to-noise ratio (PSNR), Information entropy (IE), and Correlation coefficient, and Table 3 illustrates the histogram of stego-color images and images without stego.

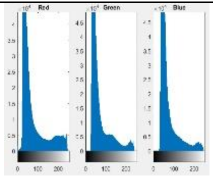
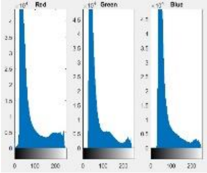
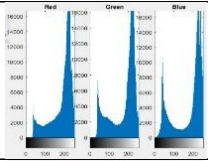
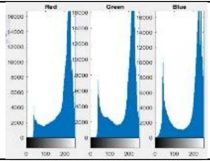
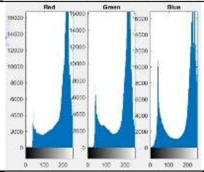
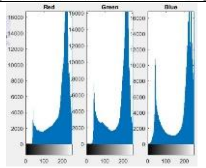
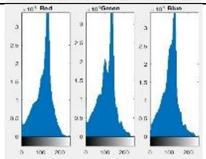
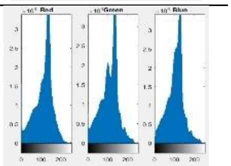
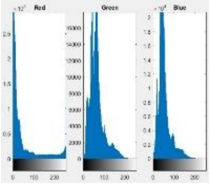
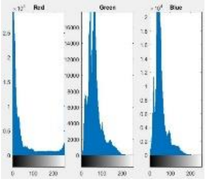
Table 1. Indicates stego-color image and color image without stego

Image Name	Stego-Color Image	Color Image without Stego
Cat		
Horse		
Parrots		
Fish		
Fox		

Table 2. Measurements of MSE, PSNR, Correlation coefficient and Information entropy

Image	MES	PSNR	Correlation Coefficient	IE
Cat	0.010776678620633763	67.80595429237161	0.9999980653950657	6.7432446
Horse	0.018259755938397286	65.5158539245143	0.9999951469719819	7.307618
Parrots	0.022328057835091834	64.64229412457709	0.9999951923022605	6.582763
Fish	0.011156005859375	67.65571627173006	0.9999983214210219	7.4034934
Fox	0.017544513081395 35	65.68939041265904	0.9999979315999405	7.188759

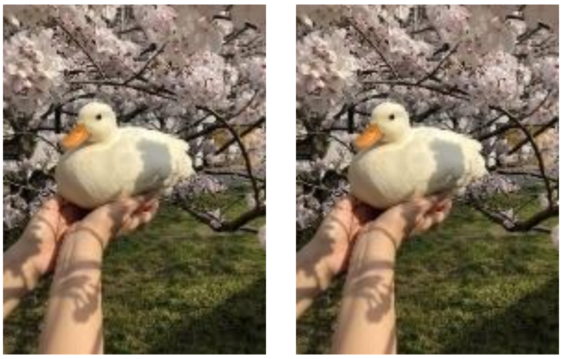
Table 3. The histogram between color image stego and color image without stego

Image	Stego-Color Image	Color Image without Stego
		
		
		
		
		

7. ANALYSIS SYSTEM

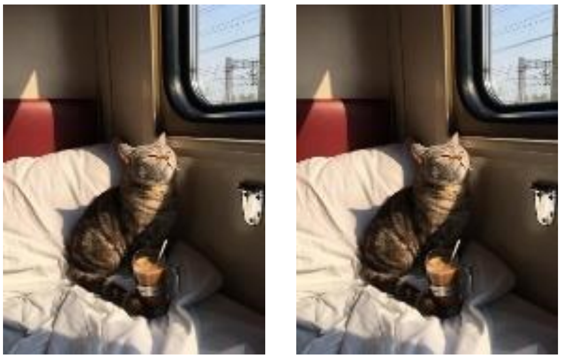
Capacity can be used as a measure of the quality of the system and can be calculated using the following equation in Eq. (8):

$$\text{capacity data stego rate} = \frac{number\ of\ secret\ message}{size\ of\ image} \qquad (8)$$



(a) stego-color image (b) image without stego

Figure 6. Big duck image



(a) stego-color image (b) stego-color image

Figure 7. Cat image

(a) stego-color image (b) stego-color image

Figure 8. Duck image

For example, the system gives several results when applying Eq. (8), as shown below. Notice that the image size will differ between the stego color image and the image without stego. In Figure 6, the image size is 653100, the secret text size is 72 bits, which is (hi fatimah), and the result of capacity is 0.00011. As for Figure 7, the hidden text was extracted, which is (Hi I am a secret message). As for the size of the image, then the message size is 160 bits, and the capacity is 0.00024. However, if the size of the message is 800 bits applied on the same image, with its size of 653100, the capacity is 0.0012, which indicates an increase in the capacity of the image. Likewise, for the Figure 8, the size of the image is 722916, the message size is 96, and the capacity is 0.00013 when the secret message hidden in the stego image is (hello message). Several factors must also be considered, the most important of which is the time consumed to extract the hidden text from the stego image. This factor depends mainly on the specifications of the computer used to implement the system. The better the computer's specifications, the less time it takes to extract the secret text from the stego image.

If the system is applied to two identical images, the value of MES will equal zero, and the value of the PSNR will equal infinity. A set of measurements was used in this paper, which was mentioned in section 4, through which close results were extracted between the stego-color image and the image without stego, which led to the sender not expecting the secret message to be discovered through the channel. In conclusion, this method is characterized by high efficiency. It was also noted that the histogram results are similar in both the stego-color image and the image without stego, which indicates the accuracy of the blockiness method and its efficiency in detecting secret texts from stego-color images and extracting them. As for the Capacity, it will not affect the size and quality of the image.

8. CONCLUSION

Steganalysis is the method of detecting hidden information within digital media (color images). It seeks to detect covert communication by analyzing patterns and anomalies that suggest the presence of steganography. The blockiness method is very efficient in extracting the secret message from the color-stego images; the attracter detects the message using the random key, which leads to knowing the contents of the secret message sent through several measurements and results mentioned in section 6. The hidden images have transparency that the human eye cannot distinguish; the proposed algorithm is written in Python to extract the secret messages from the stego-color images. It was efficient, fast, and produced the desired results.

REFERENCES

[1] Yang, C., Kang, Y., Liu, F., Song, X., Wang, J., Luo, X. (2020). Color image steganalysis based on embedding change probabilities in differential channels. International Journal of Distributed Sensor Networks, 16(5): 1550147720917826. https://doi.org/10.1177/1550147720917826

[2] Liao, X., Yu, Y., Li, B., Li, Z., Qin, Z. (2019). A new payload partition strategy in color image steganography. IEEE Transactions on Circuits and Systems for Video Technology, 30(3): 685-696. https://doi.org/10.1109/TCSVT.2019.2896270

[3] Wang, Y., Ma, Y., Jin, R., Liu, P., Ruan, N. (2020). Comprehensive criteria-based generalized steganalysis feature selection method. IEEE Access, 8: 154418-154435. https://doi.org/10.1109/ACCESS.2020.3018709

[4] Yu, X., Ma, Y., Jin, R., Xu, L., Duan, X. (2020). A multi-scale feature selection method for steganalytic feature GFR. IEEE Access, 8: 55063-55075. https://doi.org/10.1109/ACCESS.2020.2981738

[5] Ma, Y., Luo, X., Li, X., Bao, Z., Zhang, Y. (2018). Selection of rich model steganalysis features based on decision rough set α-positive region reduction. IEEE transactions on circuits and Systems for Video Technology, 29(2): 336-350. https://doi.org/10.1109/TCSVT.2018.2799243

[6] Zhou, Z., Yin, Z., Meng, R., Peng, F. (2022). Extensible steganalysis via continual learning. Fractal and Fractional, 6(12): 708. https://doi.org/10.3390/fractalfract6120708

[7] Jia, J., Luo, M., Ma, S., Wang, L., Liu, Y. (2022). Consensus-clustering-based automatic distribution matching for cross-domain image steganalysis. IEEE Transactions on Knowledge and Data Engineering, 35(6): 5665-5679. https://doi.org/10.1109/TKDE.2022.3155924

[8] Mustafa, E.M., Elshafey, M.A., Fouad, M.M. (2019). Accuracy enhancement of a blind image steganalysis approach using dynamic learning rate-based CNN on GPUs. In 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Metz, France, pp. 28-33. https://doi.org/10.1109/IDAACS.2019.8924265

[9] Zeng, J., Tan, S., Liu, G., Li, B., Huang, J. (2019). WISERNet: Wider separate-then-reunion network for steganalysis of color images. IEEE Transactions on Information Forensics and Security, 14(10): 2735-2748. https://doi.org/10.1109/TIFS.2019.2904413

[10] Sun, Z., Li, F., Huang, H., Wang, J. (2020). Image steganalysis based on convolutional neural network and feature selection. Concurrency and Computation: Practice and Experience, 32(5): e5469. https://doi.org/10.1002/cpe.5469

[11] Neamah, R.M., Abed, J.A., Abbood, E.A. (2020). Hide text depending on the three channels of pixels in color images using the modified LSB algorithm. International Journal of Electrical and Computer Engineering, 10(1):

809-815. https://doi.org/10.11591/ijece.v10i1.pp809-815

[12] Hashim, S.M., Alzubaydi, D.A. (2021). Steganalysis of adaptive image steganography using convolution neural network and blocks selection. In 2021 IEEE International Conference on Communication, Networks and Satellite (COMNETSAT), Purwokerto, Indonesia, pp. 162-167. https://doi.org/10.1109/COMNETSAT53002.2021.9530784

[13] Singh, B., Chhajed, M., Sur, A., Mitra, P. (2021). Steganalysis using learned denoising kernels. Multimedia Tools and Applications, 80: 4903-4917. https://doi.org/10.1007/s11042-020-09960-w

[14] Salunkhe, S., Bhosale, S. (2022). Video steganalysis for efficient cross-domain steganography detection. Ramrao Adik Institute of Technology, Navi Mumbai, and Veermata Jijabai Technological Institute, Mumbai, India.

[15] Sultana, H., Kamal, A.H.M., Apon, T.S., Alam, M.G. R. (2024). Increasing embedding capacity of stego images by exploiting edge pixels in prediction error space. Cyber Security and Applications, 2: 100028. https://doi.org/10.1016/j.csa.2023.100028

[16] Wang, Z., Chen, M., Yang, Y., Lei, M., Dong, Z. (2020). Joint multi-domain feature learning for image steganalysis based on CNN. EURASIP Journal on Image and Video Processing, 2020: 1-12. https://doi.org/10.1186/s13640-020-00513-7

[17] Jin, Z., Yang, Y., Chen, Y., Chen, Y. (2020). IAS-CNN: Image adaptive steganalysis via convolutional neural network combined with selection channel. International Journal of Distributed Sensor Networks, 16(3): 1550147720911002. https://doi.org/10.1177/1550147720911002

[18] Liao, X., Yin, J., Chen, M., Qin, Z. (2020). Adaptive payload distribution in multiple images steganography based on image texture features. IEEE Transactions on Dependable and Secure Computing, 19(2): 897-911. https://doi.org/10.1109/TDSC.2020.3004708

[19] Chaumont, M. (2020). Deep learning in steganography and steganalysis. In Digital Media Steganography, pp. 321-349. Academic Press. https://doi.org/10.1016/B978-0-12-819438-6.00022-0

[20] Hassan, M., Amin, M., Mahdi, S. (2020). Steganalysis techniques and comparison of available softwares. In Proceedings of the 1st International Multi Disciplinary Conference Theme: Sustainable Development and Smart Planning, IMDC SDSP.

[21] Liu, F., Zhou, X., Yan, X., Lu, Y., Wang, S. (2021). Image steganalysis via diverse filters and squeeze-and-excitation convolutional neural network. Mathematics, 9(2): 189. https://doi.org/10.3390/math9020189

[22] Amiruzzaman, M. (2011). Steganographic covert communication channels and their detection. Master's thesis, Kent State University, Kent, OH.

[23] 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