Reference-Free Detection of Steganography: A Spectral-Entropic Measure in the Differential Histogram-Correlative Domain

[1]Natiq M. Abdali, [2]Zahir M. Hussain

[1]College of Arts, University of Babylon, Iraq.

[2]Faculty of Computer Science and Mathematics, University of Kufa, Najaf, Iraq.

ABSTRACT: A recent study has shown that using neural networks to identify tampering in images is successful. However, reference-free steganalysis has gained popularity due to the complexity of getting a database, which is needed in the classification operation to identify tampering. A technique for the least significant bit (LSB) steganalysis based on studying the derivatives of the histogram correlation was recently published in a paper. This paper presents a novel blind steganalysis approach using the entropy and Fourier transform of derivatives of the image histogram autocorrelation. It examines its method successfully to unknown image steganography techniques to detect tampering images in the spatial domain. The technique is applied to three types of image data, the first of which is a gray-scale image, the second of which is true-color image data, and the third of which is color (256) image data, employing a MATLAB application.

KEYWORDS: Steganalysis, steganography, signal processing, entropy, Fourier transform.

---***---

1. INTRODUCTION

Rapid technological advancements in recent years have made multimedia widely used for data transport, especially in the context of the internet of things (IoT) [1]. The Internet is a common medium for the interchange of digital material among individuals, private enterprises, institutions, and governments [2]. Nevertheless, the transfer of data frequently happens across unsecured network routes. This data interchange mechanism has several advantages, but one major disadvantage is the risk to data security and privacy. The risk of hostile attacks, eavesdropping, and other subversive operations has increased due to the availability of easily accessible technologies that can exploit weaknesses in data transmission routes [3]. A new area of covert communication is hiding information [4]. We can cover or carry hidden messages using digital photos, movies, sound files, and other computer files that include redundant or perceptually irrelevant information. Many steganography methods that conceal messages within multimedia items have been proposed in the last few years. One common steganography technique is LSB embedding in an image. A stego image can be created by enclosing a confidential message within a carrier image. The main objective of steganalysis is to determine if the hidden message is present or not.

There really is a threat from science and technology to community safety. In order to prevent and evaluate this threat to our community, a variety of research projects and articles have been carried out to explore and create novel image steganalysis techniques. There haven't been many articles written regarding how hard it is to obtain a database, nevertheless. Image steganography—the technique of hiding information in an image—is one of the most popular covert communication strategies [5].

Thus, similar to cryptanalysis, which focuses on cryptography, steganalysis is the study of discovering concealed information in a digital carrier and differentiating between stego items and cover material with little to no understanding of steganography techniques. Gathering data that may indicate the existence of an encoded message is the aim of steganalysis [6–7].

Below are the study's primary contributions.

- A new detection technique for various image steganography is described, based on the image's entropy and Fourier transform differential histogram-correlative.
- The technology is used to discover image steganography in various image formats. The suggested system findings proved the efficiency of the strategy.
- Opposite neural network approaches, the proposed system does not depend on authentic images.
- The proposed system is a novel blind steganalysis in the spatial domain.

The rest of the paper is organized as follows:

Section two analyzes similar jobs in several fields, then Section three studies the suggested system's entropy and Fourier transform effects. Experimental testing outcomes are discussed in Section four. Section five provides conclusions based on the truth presented in this work.

2. RELATED WORKS

In this section, several researchers' works are discussed steganalysis system techniques.

RS (Regular/Singular) steganalysis, a novel approach for identifying the least significant bit encoding in grayscale and color images, was presented by Fridrich et al. [8]. Using this technique, the image is divided into groups, and the noise inside each group is then measured. Each group's LSBs of a predetermined set of pixels are reversed (using a mask, or the pixel scheme to be flipped). Depending on whether there is an increase or reduction in pixel clutter, each group is classified as either regular or single. A dual sort of flipping involves repeating the classification. Because of this, the RS steganalysis method is more reliable than the Chi-square method.

For non-colored images, another method was proposed in [9]. The various image histograms serve as the foundation for the system. The least significant bit (LSB) plane and the other bit planes have a weak correlation, which was found using translation coefficients using difference image histograms. The classifier that could differentiate between the tampered and the clear images was then constructed using this measure. The maximum detection ratio was 96.03%, while the encoding capacity varied from 0% to 100% in 10% increments. The proposed method outperforms RS analysis in terms of computing speed and performance for both sequential and random LSB substitution.

Abdali and Hussain [10] proposed a differential histogram-correlative approach for accurately identifying secret information in images. Grayscale and color images with varying orders of derivatives are examined using the differential histogram-correlative method. It is discovered that, in some cases, the first and second derivatives are not enough to uncover the concealed message; in these cases, the third derivative is required when the ratio of the stego to the covered images is small. A tiny secret message may be able to escape through this approach, and the system fails.

Three different identifying feature types were employed by Avcibas et al. [11] to distinguish between embedded and non-embedded images. They employed features such as histogram and entropy-related features, similarity differences, and other measures that relied on a spatial neighborhood-weighting mask. Indeed, correlation between consecutive bit planes—particularly the seven- and eight-bit planes—was employed by the authors as a criteria for distinguishing embedded images from cover images.

In order to recognize binary image steganography, Jialiang Chen et al. [12] created a steganalysis pattern based on local texture pattern (LTP). Taking into consideration the curse of dimensionality while extending LTPs, they employed the Manhattan distance for evaluating the correlation between pixels in a block of pixels in order to exclude those LTPs that weren't interesting. The binary image's pixel correlation changed the steganography process even though the stego image was able to retain its superior visual quality. The stego images and the original images were categorized using the ensemble classifier.

3. THE PROPOSED METHOD

This section proposed a method depending on the entropy and Fourier transform of autocorrelation derivative applied to image histogram. It can discover any tampering of the tested image.

3.1 Autocorrelation function

The autocorrelation function (ACF) is a useful diagnostic tool for time series analysis in the time domain. xt, t = 1... N is a time series of length N. A scatterplot of the latest N-k observations versus the initial N-k observations is a lagged scatterplot for lag k [13]. Equation (1) may be refined to yield a correlation between observations split by k time steps, where $x` = \sum_{i=1}^{N} (x_t)$ is the mean. The autocorrelation coefficient at lag k is denoted by the value R_K.

$$R_k = \frac{\sum_{t=1}^{N-k} (x_t - x`)(x_{t+k} - x`)}{\sum_{t=1}^{N-k} (x_t - x`)^2} \qquad (1)$$

When analyzing stationarity and picking from a variety of non-stationary models, the ACF comes in handy. Lag is a time interval that separates the required data and computes the coefficients in autocorrelation. When calculated, the range resultant numeral can be from +1 to-1. The autocorrelation of -1, +1 means an excellent positive and negative correlation, and it is symmetric about the x=0 line. The likelihood of a link between data values split by a certain number of time stages is used in autocorrelation plots, also known as correlo grams, to supply a more helpful understanding of the development of a strategy via time (lags). The correlogram shows autocorrelation coefficients on the vertical and the horizontal axis, lag values. The correlogram illustrates the time series' key characteristics, such as randomization, rising or falling trend, oscillation, and so on [14].

3.2 Entropy Measure

The digital world has been developing practically daily. In particular, the capabilities of technological devices and their use in almost all aspects of life have grown dramatically during the last ten years (i.e., mobile, digital players, robot machines, digital readers, etc.). These technologies demonstrate how modern technologies' computational and storage capabilities quickly increase. Numerous cryptographic techniques are still used today, like the cryptography Data Encryption System (DES), the Blowfish cipher, the Two fish cipher, and the advanced encryption standard (AES), despite the fast growth of electronic and computational machines abilities. Although flaws in these approaches have been identified for bulk data such as digital images and electronic media, the ancient algorithms predominate cryptographic algorithms at all classes (people, institutions, businesses, and governments) [15].

Shannon entropy was initially suggested in 1948. Shannon entropy has been employed extensively in the information sciences ever since. An indicator of the degree of uncertainty around a random variable is the Shannon entropy. Shannon entropy, in particular, measures the anticipated value of the data in a message. Equation (2) defines the Shannon entropy of a random variable X [16].

$$H(X) = -\sum_{i=1}^{n} p_i \, log_2 p_i \qquad (2)$$

$$\text{Where} \quad p_i = \Pr(X = x_i)$$

3.3 Fourier Transforms Measure

Fourier transformations and frequency domain analysis are key components of signal and system analysis. Electrical engineering is based on some of these ideas as well. These ideas are so basic that they are used in many other fields, such as electrical engineering, nearly all engineering and scientific departments, and several math departments.

A wonderful mathematical method is the Fourier transform. Any function may be broken down into a sum of sinusoidal basis functions using the Fourier transform. These fundamental functions are each distinct frequency complex exponential. Because of this, the Fourier transform gives us a distinctive viewpoint on all functions, viewing them as the sum of simple sinusoids.

Despite being a fantastic mathematical tool, the Fourier transform is frequently utilized in engineering and research due to its useful applications. Understanding why the Fourier transform is so important is not simple. However, I can assure you that it makes complex problems easier to understand. In addition, the Fourier transform offers a fresh perspective on reality that is perfect for developing a more intuitive comprehension of our surroundings [17]. A mathematical method called the Fourier transform converts a function of time, x(t), to a function of frequency, X(ω). Equation (3) defines the Fourier transform of a function g(t).

$$\mathcal{F}\{g(t)\} = G(f) = \int_{-\infty}^{\infty} g(t)\mathrm{e}^{-2\pi i f t}\, dt. \qquad (3)$$

The result is contingent upon the frequency, or function off. As a result, G(f) gives the power g(t) at frequency f. Another name for G (f) is the g spectrum. Furthermore, g from G may be extracted using the inverse Fourier transform.

$$\mathcal{F}^{-1}\,\{\mathrm{G(f)}\}=\mathrm{g(t)} = \int_{-\infty}^{\infty} \mathrm{G}(f\ ) e^{2\pi i f t}\, df. \qquad (4)$$

3.4 The entropy and Fourier transform of differential histogram-correlative method

According to the correlation analysis, the universal steganalysis approach is recommended in this study. Blind-steganalysis can be used to identify the existence of a concealed message in the cover image. The proposed system was expanded to detect image tampering using the entropy and Fourier transform measures. To distinguish image manipulation, the suggested technique calculated the image's Histogram-Correlative and took the first three derivatives. The derivatives of the Histogram-Correlation of the image will have evident vibrations when tampering is present. Then, the entropy or Fourier transform measures as a criterion would lead to a decision. Fig. 1 shows the suggested technique diagram.

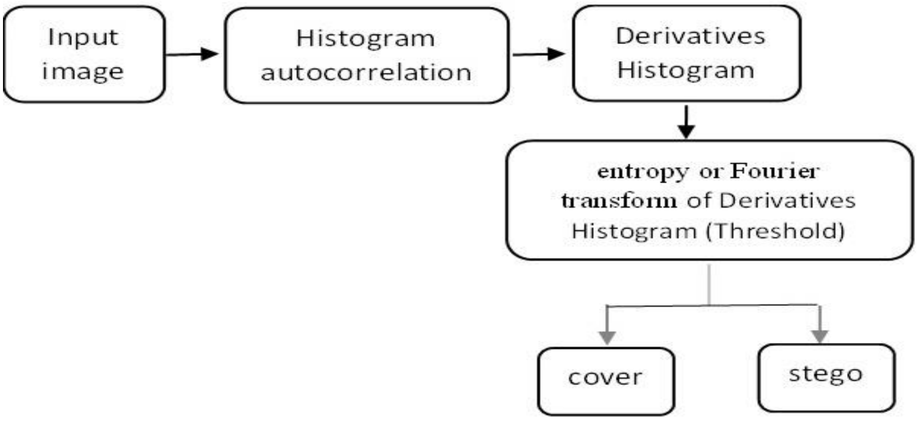
Input image
Histogram autocorrelation
Derivatives Histogram
entropy or Fourier transform of Derivatives Histogram (Threshold)
cover
stego

Fig-1. Architecture of the suggested method.

3.5 Performance Evaluation Tools

Fourier transform correlation derivative is the first way of determining a threshold that may be used in a decision.

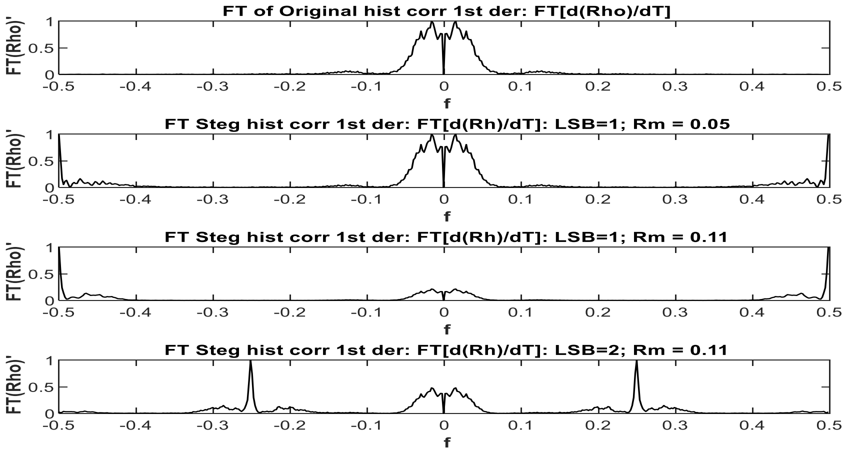

Fig- 2.

The Fourier Transform of histogram correlation 1st derivative of cover and three stego images

Firstly, the Fourier transform is applied on the input tested image's derivatives histogram autocorrelation by equation (5).

$$f_1 = \sum_{n=1}^{N} d_1(n) \times \exp(-j2\pi kn/N) \qquad (5)$$

where 1 <= k <= N and d_1 is the first derivative of the image's Histogram-Correlative.

Secondly, we take the border of the Low-Pass and High-Pass of the Fourier transform image histogram correlation derivative as a 0.1 value as a positive range, including f = 0, as follows:

$$no = fo \times Ln \qquad (6)$$

Where fo=0.1 is the border of the high-pass and low-pass of the Fourier transform image histogram correlation derivative, *Ln* =255 is the positive range including f=0, and *no* is the index of fo.

Then find the max High -pass region and max Low-pass region of Fourier transform (see Figure 2), as follows:

$$mL1 = \max(f_1(1{:}\, no)) \qquad (7)$$

$$mH1 = \max(f_1(no + 1: Ln) \qquad (8)$$

$$r1o = mH1/mL1 \qquad (9)$$

Where $r1o$ is the max High-pass region /max Low -pass region of Fourier transform of the first derivative of the image's Histogram-Correlative for the original image.

Finally, we apply the equations (5-9) to find $r2o, r3o$ are the max High-pass region /max Low -pass region of Fourier transform of the second, third derivative of the image's Histogram-Correlative for the original image and in the same way apply the equations (5-9) for the stego images.

The following equation may be used to calculate the size rate R_m between payload size and carrier size:

$$R_m = \frac{Message\ Size}{Cover\ Image\ Size} \qquad (10)$$

The second threshold is entropy of autocorrelation derivative of the image histogram utilized in this work was created as follows:

$$d_1 = d_1{}^2 \qquad (11)$$

$$\text{entropy threshold} = -\sum d_1\ log_2(\ d_1\ ) \qquad (12)$$

where $\boldsymbol{d_1}$ is the first derivative of the image's Histogram-Correlative.

The entropy of the autocorrelation derivative of the image histogram will be low since the image is original. It will be high if the tested image is tampered. However, the entropy criterion is more accurate for color images than other thresholds to discover image tampering.

4. EXPERIMENTAL RESULTS AND DISCUSSION

The suggested system should recognize images that have been tampered. The gray-scale images utilized in these tests are depicted in Figure (3).

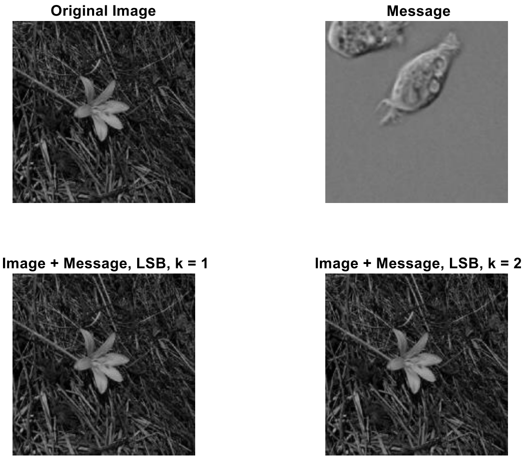

Fig-3. The carrier and stego images are in gray-scale

In the first experiment, the suggested system examined the BOSS database [18]. A random selection of 1000 with 512 x 512-pixel images was used for testing out a total of 10,000 images in grayscale format (PNG). We found that for natural images, most information is LP(Low-Pass) region. Hence, max (HP)/max (LP) is less than 1. Powerful HP(High-Pass) components appear after steganography, making max (HP) is bigger than max (LP). This truth appears in Figures (4) and (5). In Figures (4) and (5), case 1 is the original image, and cases 2,3, and 4 are the stego images with different embedding ratios.

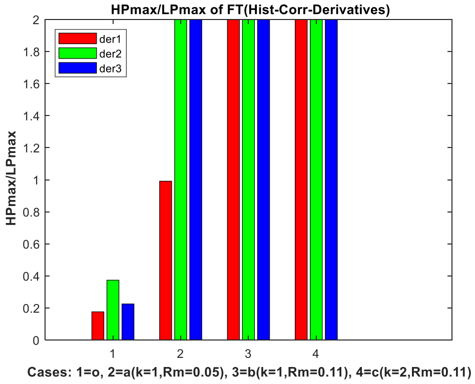

Fig-4. max High-Pass / max Low-Pass of FT(Histogram-Correlation-Derivatives) of cover and three stego images.

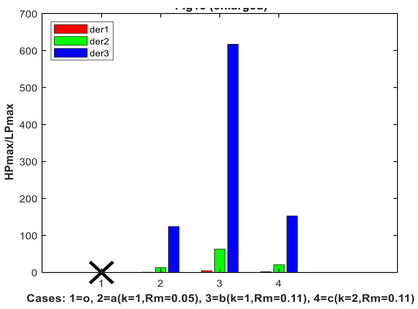

Fig-5. max High-Pass / max Low-Pass of FT(Histogram-Correlation-Derivatives) of cover and three stego images (enlarged).

The proposed method was tested using several image steganography techniques to encrypt the message in color BMP (true and 256) images. The suggested approach should be capable of detecting manipulated images by using the second threshold. As a result, using the entropy measure on this derivative would be an excellent way to detect secret message, where a criterion may be utilized.

In the second test, the least significant bit (LSB) approach was used to assess the recommended system's ability to recognize the embedded image. True-color (RGB) images were used for the cover images. By modifying the least significant bits of the 3-channel embedding, which sequentially injected secret data into each image pixel, each channel of each pixel was embedded with 2 or 4 bits [19]. The color images were obtained from [20] of the Mendeley data. The cover image and stego image are shown in Figure 6. The testing data consisted of 150 images of 512×512 pixels chosen at random from a set of 1500 images. We found that if the image is clear, then the value of the entropy of the first three derivatives of histogram correlative is tiny. When the value of the entropy of derivatives of histogram correlative is high, then the tested image is tampering. This can be seen in Figure (7). In Fig. 7, Case 1 is the entropy value for the first, second, and third derivatives of the stego image, and Case 2 is the entropy for the first derivative and the second and third derivatives, which are tiny values of the cover image.

Fig-6. The true-color (RGB) tested images

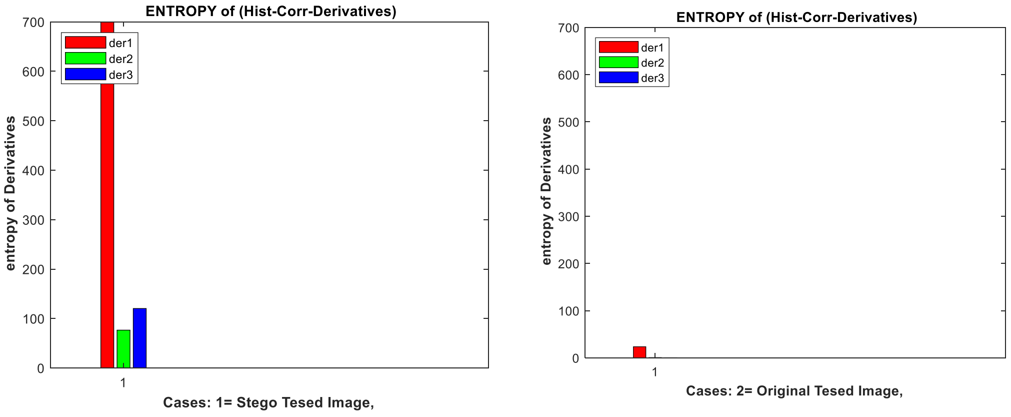

Fig-7. The histogram-correlative derivative entropy value for a clean image and tampering with an image

In the following experiment, the proposed system examined 100 images chosen at random from 1000 images using different image steganography techniques with a color image format (256). The carrier and stego images are shown in Figure 8. We found that if the image is clear, then the value of the entropy of the first three derivatives of the histogram correlative is small. When the value of the entropy of the derivatives of the histogram correlation is high, then the tested image is tampering. This can be seen in Figure 9. In Fig. 9, Case 1 is the entropy value for the first, second, and third derivatives of the stego image, and Case 2 is the entropy for the first derivative and the second and third derivatives of the carrier image, which are tiny values of the cover image.

Fig-8. The color (256) tested images.

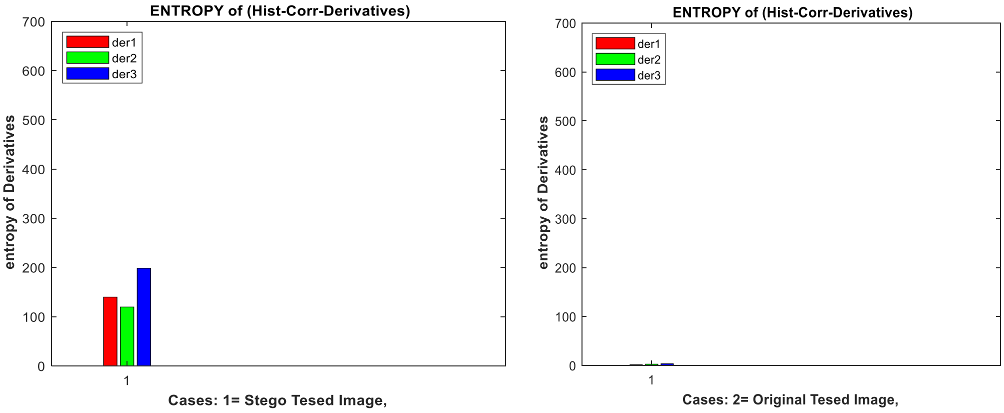

Fig-9. The histogram-correlative derivative entropy value for a clean image and tampering with an image

5. CONCLUSION

A strategy for spatial domain image tampering detection is described. This approach is known as blind steganalysis, and it may be used with a variety of steganography techniques. The proposed method detects whether or not an image has been modified without depending on an authentic image, and it uses a histogram autocorrelation way of analysis.The presented approach is based on the fact that if an image is loaded with coded data, the derivative entropy of the image's histogram correlation will have a high amount. This reality issues in different steganography methods, but the suggested method without entropy or Fourier Transform measure disappoint when the encrypted message size is minimal. These tiny messages will be unclear then the entropy or Fourier Transform measure will discover the little secret message as evident. If the derivative entropy value of the correlation of the image's histogram is a tiny amount, then the tested image is a cover. It was found that the proposed system explained above, the entropy value discussed earlier depends on the image format, whether it is color (true and 256).

In conclusion, examine this method for several image steganographic approaches as well. We find the Fourier Transform measure appropriate for gray-scale images and the entropy measure suitable for color images. However, The proposed system fails when the tested image has a low correlation between an adjacent pixel.

REFERENCES

1. Sayed, Y. Himeur, A. Alsalemi, F. Bensaali, A. Amira, "Intelligent edge-based recommender system for internet of energy applications," IEEE Systems Journal 16 (3), pp. 5001–5010, 2021.
2. Y. Himeur, S. S. Sohail, F. Bensaali, A. Amira, M. Alazab, "Latest trends of security and privacy in recommender systems: a comprehensive review and future perspectives," Computers & Security, 2022.
3. Y. Himeur, A. Sayed, A. Alsalemi, F. Bensaali, A. Amira, I. Varlamis, M. Eirinaki, C. Sardianos, G. Dimitrakopoulos, "Blockchain-based recommender systems: Applications, challenges and future opportunities,", Computer Science Review,Vol. 43, 2022.
4. M. Raggo and C.Hosmer," Data hiding," *syngress*, pp. 350, Nov. 2012.
5. W. You, et al.," A Siamese CNN for Image Steganalysis," IEEE Transactions on Information Forensics and Security, Vol. 16,2021.
6. J. Zhu, R. Kaplan, J. Johnson, and L. Fei-Fei, "Hidden: Hiding data with deep networks," in Proc. Eur. Conf. Comput. Vis. (ECCV), Munich, Germany, pp. 682–697, Sep. 2018.
7. J. Hayes and G. Danezis, "Generating steganographic images via adversarial training," in Proc. Annu. Conf. Neural Inf. Process. Syst. (NIPS), Long Beach, CA, USA, pp. 1954–1963, Dec. 2017.
8. J .Fridrich, M. Goljan , R .," Du Reliable detection of LSB steganography in color and grayscale images," In: Proceedings of the 2001 workshop on multimedia and security new challenges - (MM&Sec '01), pp. 27, 2001.
9. T .Zhang, X .Ping ,"Reliable detection of LSB steganography based on the dif- ference image histogram," In: Proceedings of the IEEE international confer- ence on acoustics, speech, and signal processing, (ICASSP '03), Vol. 3III-545-8, 2003 .
10. N. M. Abdali and Z. M. Hussain, "Reference-free differential histogram-correlative detection of steganography: Performance analysis,", Indonesian Journal of Electrical Engineering and Computer Science, Vol. 25, No. 1, pp. 329-338, 2022.

I. Avcibas, M. Kharrazi, N. Memon, and B.Sankur, "Image steganalysis with binary

11. similarity measures" EURASIP J. Appl. Signal Process., 2005.
12. J. Luo, M. Yu, X. Yin, and W. Lu, "Binary image steganalysis based on symmetrical local residual patterns," Chinese Journal of Electronics, vol. 31, no. 4, pp. 752–763, 2022.
13. Chatfield," The Analysis of Time Series: An Introduction," Sixth Edition, Chapman & Hall, 1996.
14. J. Rafiee, P.W. Tse," Use of autocorrelation of wavelet coefficients for fault diagnosis," Mechanical Systems and Signal Processing Vol.23, pp.1554–1572, 2009.
15. Y .Wua, *et al.*," Local Shannon entropy measure with statistical tests for image randomness," In: Information Sciences , Vol. 222.pp. 323–342, 2013.
16.] C.E. Shannon, A mathematical theory of communication, Bell System Technical Journal, pp. 623–656, 1948.
17. L. S. Derong, " Application of Fourier Transform in Signal Processing," Signal and Information Processing, Vol.1, No. 1, pp.1-5, 2018.
18. Break Our Steganographic System Base Webpage (BossBase). Available online: http://agents.fel.cvut.cz/boss/ (accessed on 10 January 2023).
19. Z. I. Rasool, M. M. Al-Jarrah, and S. Amin, "Steganalysis of RGB images using merged statistical features of color channels," in 2018 11th International Conference on Developments in eSystems Engineering (DeSE), pp. 46-51, 2018.
20. M. Al-Jarrah, "Rgb-bmp steganalysis dataset," Mendeley Data, vol. 1, 2018.