Blind Steganalysis Method Using Image Spectral Density and Differential Histogram Correlative Power Spectral Density

Hafedh Ali Shabat *, Khamael Raqim Raheem, and Wafaa Mohammed Ridha Shakir

Technical Institute of Babylon, AL-Furat AL-Awsat Technical University (ATU), Kufa, Iraq
Email: h.ali@atu.edu.iq (H.A.S.); khmrakrah@atu.edu.iq (K.R.R.); inb.wfa@atu.edu.iq (W.M.R.S.)
*Corresponding author

***Abstract*—Recent research has demonstrated the success of employing neural networks for the purpose of detecting image tampering. Nevertheless, the utilization of reference-free steganalysis has become increasingly popular as a result of the challenges associated with obtaining an annotated dataset. This dataset is crucial for the classification process using neural networks, which aims to detect and identify instances of tampering. This paper introduces a robust approach to blind steganalysis, utilizing image spectral density and differential histogram correlative power spectral density. The proposed method employed two distinct forms of image data, namely a gray-scale image and true-color image data. The results indicate that the proposed methodology successfully achieved the anticipated outcomes in identifying manipulated images as evidenced by its successful application on the two distinct datasets. In the experiment results, the proposed technique succeeded quite well in terms of accuracy at low embedding ratios. Also, it successfully recognized sequential and random least significant bit steganography.**

***Keywords*—steganalysis, steganography, signal processing, entropy, spectral density**

I. Introduction

Digital music, podcasts, online and recorded webinars, video chats, and movies have altered the way we interact today and are found in practically every company. These techniques are used to communicate ideas, develop personnel, build strong customer relationships, and amuse. Therefore, digital media became poses a real threat, thus, using these pathways to exchange information discreetly, remove copyrights, provide insider knowledge, transmit command and control information, or offer the technology needed to combat advanced threats became difficulty [1].

This science and technology danger to community security is a genuine one. As a result, many kinds of research or papers have been conducted to investigate and develop innovative image steganalysis approaches to avoid and assess this threat to the community. However, only some articles were done about the difficulty of receiving a database. Image steganography is the technique of concealing information within an image, and is one of the most prevalent covert communication strategies [2]. There are three common types of image steganography which are naive approaches [2, 3], adaptive approaches [4–8], and deep learning-based encoding [9–16].

Steganalysis is the discipline of finding hidden information in a digital carrier and discriminating among stego items and cover material with little or no knowledge of steganography techniques, identical to cryptanalysis, which concentrates on cryptography. The goal of steganalysis is to collect information that could lead to the presence of an encoded message [17, 18].

The contribution of study, a new detection technique for various image steganography is described based on the image's entropy and differential histogram-correlative power spectral density. The method is used to discover image steganography in various image formats. The proposed system discovered stego images created by sequential and random LSB steganography methods.

In contrast to the neural networks approach, the proposed system does not depend on authentic images. Additionally, a novel blind steganalysis in the frequency domain is presented. The rest of the paper is organized as follows:

Section II analyzes similar jobs in several fields, then, section III presents the theoretical basis of the autocorrelation function, entropy, and Fourier transform effects. Section IV renders the methodology of the proposed system. Experimental outcomes are discussed in Section V. Lastly, Section VI provides conclusions based on the truth presented in this work.

II. Literature Review

In this section, several works discussed steganalysis system techniques. Westfeld and Pfitzmann [19] presented the 1st statistical steganalysis approach. This method identifies Pairs of Values (POVs) transferred during secret data covering. Values of the pixel, quantized coefficients of the Discrete Cosine Transform (DCT), and palette indices that vary in the least significant bit are examples of POVs. According to the

Manuscript received July 11, 2023; revised July 25, 2023; accepted September 27, 2023; published January 4, 2024.

Chi-squared method, the frequencies of each of the two-pixel values in each POV tip are distant from a POV's mean. A chi-squared process is an approach that finds close-equal POVs in images and, as a result, encoded data. This approach consistently recognizes successively embedded information but fails when the information is random.

Abdali and Hussain [20] suggested a method for detecting secret messages in images in the spatial domain using differential histogram-correlative. Differential histogram-correlative examines gray-scale and color images with different orders of derivatives. It is found that the first and second derivatives are insufficient in some examine, then need to third derivative when small the ratio stego to cover images to discover the hidden message. The system is failed, and a tiny secret message can escape this method.

Fridrich *et al.* [21] introduced Regular/Singular (RS) steganalysis, a novel technique for detecting the Least Significant Bit encoding in grayscale and color photos. This method separates the image into groups and then measures the noise in each group. The LSBs of a defined set of pixels within each group are flipped (by employing a mask, i.e., the scheme of pixels to flip). Each group is categorized as regular or singular depending on whether the pixel clutter is decreased or increased. For a dual kind of flipping, the categorization is repeated. As a result, the RS steganalysis approach is additionally trustworthy from the Chi-square technique.

In Ref. [22], an approach for non-colored photos was suggested. The system is based on the histogram of different images. Translation coefficients through difference photo histograms were used to detect the poor correlation between the Least Significant Bit (LSB) plane and the other bit planes. This metric was then utilized to build a classifier to distinguish between the tampered and the clear images. The encoding capacity ranged from 0% to 100% in 10% increments, with the highest detection ratio at 96.03%. The suggested approach performs well for random and sequential LSB substitution, with improved performance and computation speed than RS analysis.

Malekmohamadi and Ghaemmaghami [23] provided a grayscale image steganalysis approach based on spatial and Gabor features. They looked at spatial correlations across pixels in unclean and clear images for feature selection. Gabor filter coefficients were utilized to produce input data for a training model, and those characteristics were used to train a Support Vector Machine (SVM) classifier. The entire image's first and higher-order statistics, as well as its DCT transform, were used. After that, the trained model was applied to unseen changes and clear photos. According to the findings, the algorithm had an extremely accurate detection rate of 93% for changed pictures and 96% for pure images, with an encoding ratio of 14.1%.

Lin *et al.* [24] suggested a method for successfully recognizing Modified Pixel-Value Differencing (MPVD) steganography. They presented a way for MPVD steganalysis based on the chi-square fit of the model since relevant works on Pixel-Value Differencing (PVD) steganography has mostly highlighted embedding capacity and image quality and concentrated on preventing attacks by RS and Pixel Difference Histogram (PDH) study. They tested the suggested technique with 1,000 images and discovered that it outperformed state-of-the-art techniques across various image datasets, embedding ratios, and classification methods. This technique performed substantially better in terms of accurate results at low insertion ratios in the trials. As a result, this approach may be utilized for the steganalysis of MPVD steganography and is a viable alternative to the regularly used RS and PDH analysis methods.

In summary, attempted models of detection of the secret message discussed above use networks or popular statistical methods, but they are unsuitable for detecting image tampering without an image database. This paper provides a solution to the problem of difficulty in obtaining a database of images, where the proposed system can decide on the tested image and classify it as a cover or a stego image without relying on an original image. Furthermore, the suggested method discovers tiny messages in LSB steganography.

Experiments indicated that the suggested model obtained up to 0.934 average accuracy, which is much higher than the accuracies of other popular techniques [24–26].

III. Theoretical Basis

A. Autocorrelation Function

The Autocorrelation Function (ACF) is a useful diagnostic tool for time series analysis in the time domain. x_t, 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 [27]. Eq. (1) may be refined to yield a correlation between observations split by k time steps, where $x` = \sum_{i=1}^{N} (x_t)$ is mean. The autocorrelation coefficient at lag k is denoted by the value R_K.

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

The ACF is handy when analyzing stationarity and picking from various non-stationary models. Lag is a time interval that separates the required data and computes the coefficients in autocorrelation. When calculated, the resultant range numeral can be from +1 to −1. The autocorrelation of −1, +1 means an excellent positive and negative correlation and 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 correlograms, to supply a more helpful understanding of developing a strategy via time (lags). The correlogram shows autocorrelation coefficients on the vertical and horizontal axes and lag values. The correlogram illustrates the time series' key characteristics, such as randomization, rising or falling trends, oscillation, and so on [28].

B. Entropy Function

Histogram analysis, global Shannon entropy measure, and neighboring pixel correlations are all ways to determine image randomness. The Shannon entropy, named after Claude Shannon, was developed for the first time in 1948, and Shannon entropy has been primarily applied in the information sciences since then. The Shannon entropy of a random variable measures its uncertainty, and Shannon entropy, in particular, measures the anticipated value of the information in a letter. Eq. (2) defines the Shannon entropy of a random variable X [29].

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

where $P_i=P_r(X=x_i)$.

C. Fourier Transforms

Signal and system analysis relies heavily on frequency domain analysis and Fourier transforms. These concepts are also one of the foundations of electrical engineering. These concepts are so fundamental that they are employed in various domains, including electrical engineering, almost every engineering and science department, and multiple mathematics places.

The Fourier Transform (power spectral density) is a charming mathematical technique. Using the Fourier Transform, any function may be decomposed into a sum of sinusoidal basis functions. Each of these essential functions is a different frequency complex exponential. As a result, the Fourier Transform provides us with a unique perspective on every function: the sum of simple sinusoids. While the Fourier Transform is a mathematical tool, it is widely used in research and engineering because of its practical applications. It is challenging to comprehend why the Fourier Transform is so crucial, it simplifies the answer to complicated difficulties. Furthermore, the Fourier Transform provides a new way of experiencing the world, ideal for gaining a more intuitive understanding of our environment [30]. The Fourier Transform is a mathematical technique that transforms a function of time, $x(t)$, to a function of frequency, $X(\omega)$. Define the Fourier transform of a function $g(t)$ by Eq. (3).

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

The outcome is a function of f or frequency. Consequently, $G(f)$ indicates how much power $g(t)$ has a frequency f. $G(f)$ is also known as the g spectrum. Furthermore, the inverse Fourier Transform may be used to extract g from G:

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

When an image is injected with embedding value, the image's correlation modifications, but the modifications in its pixel correlations aren't significant sufficiently to recognize. As a result, direct correlative examination of the stego image may be ineffective in detecting manipulation. On the other hand, the derivatives of histogram correlation have shown far more substantial variations. The identification of LSB-steganography can be achieved through the utilization of the first derivative of the histogram correlation, as mentioned in [31].

IV. Proposed Method

The proposed method depends on the image entropy and power spectral density of the autocorrelation derivative applied to the image histogram in order to discover any tampering with the original image. Fig. 1 illustrates the diagram of the proposed method.

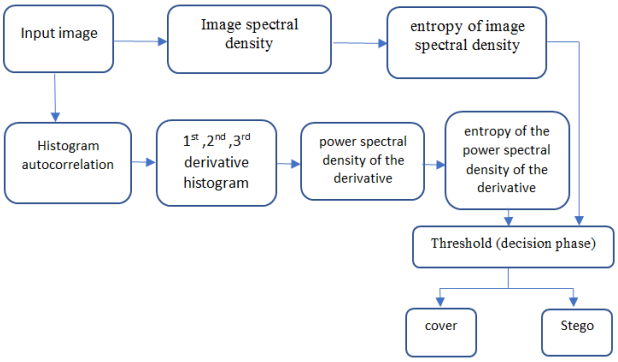


Fig. 1. Architecture of the proposed method.

According to the correlation analysis, the universal steganalysis approach is recommended in this study. Blind steganalysis can be used to identify a concealed message in the cover image. The proposed system was expanded to detect image tampering using the entropy and differential histogram correlative power-spectral density measure. The suggested technique calculated the image's Histogram-Correlative to distinguish image manipulation and took the first three derivatives. Then, the entropy of power-spectral density measure as a criterion would lead to a decision.

The Fourier transform (power spectral density) is applied to the input image's derivatives histogram autocorrelation by Eq. (5).

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

where $1 \leq k \leq$ N and d_1 is the first derivative of the image's Histogram-Correlative, d_2 and d_3 are the second and third derivative of the image's Histogram-Correlative. Then, calculate the entropy of the power spectral density of the derivative by Eq. (6).

$$enp = f_1 \times -\sum_{i=1}^{n} p_i \, log_2 p_i \tag{6}$$

The spectral density of the image is determined by utilizing Eq. (7).

$$Sp = \sum_{n=1}^{N} w(n) \times \exp\left(-j2\pi kn/N\right) \tag{7}$$

where $1 \leq k \leq N$ and w is the image.

The entropy is applied on the spectral density of the tested image by Eq. (8).

$$eni \; = \; Sp \times -\sum_{i=1}^{n} p_i \, log_2 p_i \tag{8}$$

Finally, the threshold that locates whether an image is clear or tampered with can be determined by employing Eq. (9).

$$Threshold = 10 \log 10 \times enp \times eni \quad (9)$$

Eq. (10) is used to calculate the size rate R_m between payload size and carrier size [32]:

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

The entropy of power spectral density of the autocorrelation derivative of the image histogram will be less than 0 since the image is original. It will be high if the tested image is tampered with. However, the entropy criterion is more accurate for color images to discover image tampering.

V. Experiment Results and Discussion

Various indicators were used to assess the efficiency of the blind proposed steganalysis approach. There are four possible results if suspicious images are embedded:

(1) True positive (TP): a stego image is accurately classified as a stego image.
(2) False negative (FN): a stego image is incorrectly classified as a carrier image.
(3) True negative (TN): a cover image is correctly classified as a carrier image.
(4) False positive (FP): a cover image is wrongly classified as a stego image.

Metrics such as accuracy are used to evaluate the success of the suggested strategy. The fraction of all accurately predicted classes is referred to as accuracy. The accuracy should be as high as possible [24]. Eq. (11) is used to calculate accuracy.

$$\text{Accuracy} = \frac{TP+TN}{TP+FP+FN+TN} \quad (11)$$

In the first experiment, the suggested system was evaluated for detecting the embedding image by the Modified Pixel-Value Differencing steganography method (MPVD) [24]. The grayscale cover images with PNG extension, which obtained from the BOSS database [33]. The testing was run on 10,00 with 512×512-pixel images chosen randomly from 10,000 images. For the embedding ratios of 10% and 100%, we conducted the tests and determined the threshold's value as Eq. (9) to classify the tested image which is shown in Table I.

TABLE I: Results Using a Threshold Value of 0 for the Suggested Technique

Embedding ratio (%)	TP	FN	TN	FP	Accuracy
10	934	66	996	4	0.934
20	975	25	996	4	0.975
30	984	16	996	4	0.984
40	996	4	996	4	0.996
50	998	2	996	4	0.998
100	1000	0	996	4	0.999

The result in Table I exhibit that the suggested method has high accuracy.

Fig. 2 represents the carrier and stego images. The threshold criteria for original images is less than 0. Powerful entropy appears after steganography, making the threshold bigger than 0 in the first derivative. Fig. 3 shows Case 1 which represents the original image, and Cases 2, 3 and 4 are the stego images with three different embedding ratios.

(a) (b)

Fig. 2. PNG images, (a) carrier image, and (b) stego image.

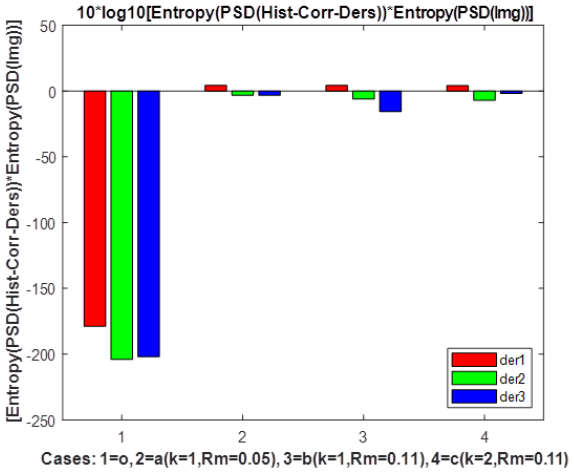
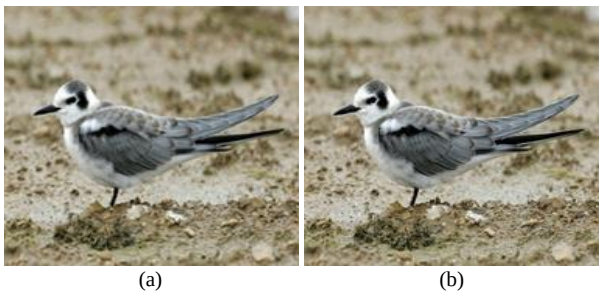


Fig. 3. Entropy power spectral (Histogram correlation Derivatives) × entropy power spectral of cover and three stego images.

In the second experiment, the suggested system was evaluated for detecting the embedding image by the method of the Least Significant Bit (LSB). For the cover images, which were True Color Images (RGB), each channel of each pixel was embedded with 2 bits or 4 bits by changing the least significant bits for the 3-channel embedding, which successively inserted secret data into each image pixel [34]. The color images taken from the Mendeley Data [35]. Fig. 4 display the cover image and stego image.



(a) (b)

Fig. 4. RGB images, (a) carrier image, (b) stego image.

The testing data involved 150 images with 512×512 pixels, chosen randomly from 1500 images. It was found that the threshold criterion for the first, second, and third derivatives of natural images is smaller than 0. After steganography, powerful entropy arises, raising the threshold for the first derivative above zero. This can be seen in Figs. 5 and 6.

In Fig. 5, Cases 1, 2, 3 are the entropy value for the first, second, and third derivatives of the original image R, G, and B, respectively. In Fig. 6, Cases 1, 2, and 3 are the entropy value for the first, second, and third derivatives of the stego image R, G, and B, respectively.

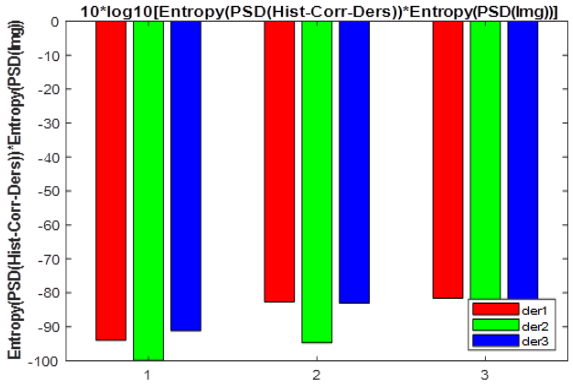


Fig. 5. Entropy power spectral (Histogram correlation Derivatives) × entropy power spectral of the cover image (RGB).

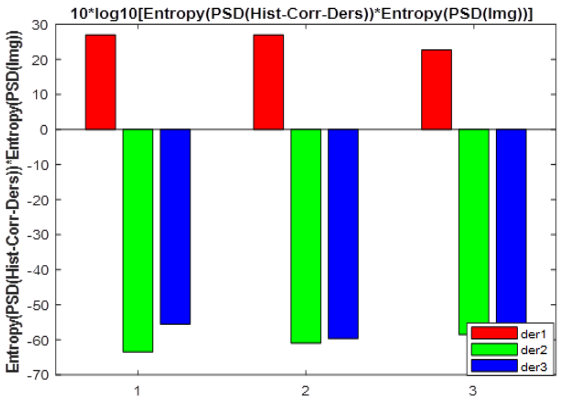


Fig. 6. Entropy power (Histogram correlation Derivatives) × entropy power spectral of stego image (RGB) spectral.

The method under consideration successfully detected tampered images with embedding ratios of 0.05 and 0.11, where the stego image based on Chaotic-LSB method [36] as illustrated in Fig. 3. Where the variations in the entropy value of the first derivative were noticed is the location where the powerful entropy emerges, which raises the threshold for the first derivative above zero. Furthermore, the method under consideration was implemented on embedding ratios of 10%, 20%, 30% and 40% of the BOSS image dataset. The results were compared with multiple prior studies utilizing the identical BOSS dataset, as depicted in Table II.

Table II provides a comparison of the outcomes based on their accuracy. The data presented in the table indicates that the proposed approach exhibited superior performance compared to alternative strategies when applied to the BOSS database. It is possible in the future to add improvements to the proposed system via new tools such as thresholds that are more suitable for modern steganography methods to detect tiny messages that are difficult to discover in the current proposed way.

TABLE II: COMPARISON OF ACCURACIES FOR BOSS DATASET IMAGES

Embedding ratio (%)	Proposed method	Lin *et al.*'s method [24]	Sabeti *et al.*'s method [25]	Bui *et al.*'s method [26]
10	0.934	0.903	0.533	0.884
20	0.975	0.959	0.902	0.898
30	0.984	0.987	0.945	0.902
40	0.996	0.995	0.968	0.898

VI. CONCLUSION

A strategy for frequency domain image tampering detection is described. This approach is known as blind steganalysis, and it may be used with various steganography techniques. The proposed method detects whether or not an image has been modified without depending on an authentic image, where 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 entropy value of the power density spectral derivative of the image's histogram correlation will have a high amount. While if an image is clear, the entropy value will have a minus amount. This reality is explicit in testing many images. The suggested method is promising when the encrypted message is minimal. If the entropy value of the derivative of the correlation of the image's histogram is bigger than 0 in the first derivative, then the tested image is a stego. The proposed method demonstrated favourable performance in comparison to other techniques, rendering it suitable for both color and grayscale images.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

AUTHOR CONTRIBUTIONS

Hafedh A. Shabat conducted the conceptualization; Khamael R. Raheem constructed the methodology; Hafedh A. Shabat and Khamael R. Raheem carried out the software; Wafaa M. Ridha Shakir conducted formal analysis and examined the data; Wafaa M. Ridha Shakir did writing—review and editing, all authors participated in writing the paper; all authors had approved the final version.

REFERENCES

[1] F. S. Hassan and A. Gutub, "Improving data hiding within colour images using hue component of HSV colour space," *CAAI Transactions on Intelligence Technology*, vol. 7, pp. 56–68, 2022.

[2] W. You, H. Zhang, and X. Zhao, "A Siamese CNN for image steganalysis," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 291–306, 2020.

[3] R. Cogranne, C. Zitzmann, L. Fillatre, F. Retraint, I. Nikiforov, and P. Cornu, "A cover image model for reliable steganalysis," in *Proc. Information Hiding: 13th International Conference*, IH 2011, Prague, Czech Republic, May 18–20, 2011, pp. 178–192.

[4] V. Holub and J. Fridrich, "Digital image steganography using universal distortion," in *Proc. the 1st ACM Workshop on Information Hiding and Multimedia Security*, 2013, pp. 59–68.
[5] B. Li, M. Wang, J. Huang, and X. Li, "A new cost function for spatial image steganography," in *Proc. 2014 IEEE International Conference on Image Processing (ICIP)*, 2014, pp. 4206–4210.
[6] T. Pevný, T. Filler, and P. Bas, "Using high-dimensional image models to perform highly undetectable steganography," in *Proc. Information Hiding: 12th International Conference*, IH 2010, Calgary, AB, Canada, June 28–30, 2010, pp. 161–177.
[7] V. Holub and J. Fridrich, "Designing steganographic distortion using directional filters," in *Proc. 2012 IEEE International Workshop on Information Forensics and Security (WIFS)*, 2012, pp. 234–239.
[8] V. Sedighi, R. Cogranne, and J. Fridrich, "Content-adaptive steganography by minimizing statistical detectability," *IEEE Transactions on Information Forensics and Security*, vol. 11, pp. 221–234, 2015.
[9] H. Shi, J. Dong, W. Wang, Y. Qian, and X. Zhang, "SSGAN: Secure steganography based on generative adversarial networks," in *Proc. Advances in Multimedia Information Processing—18th Pacific-Rim Conference on Multimedia, PCM 2017*, Harbin, China, September 28–29, 2017, Part I 18, 2018, pp. 534–544.
[10] D. Hu, L. Wang, W. Jiang, S. Zheng, and B. Li, "A novel image steganography method via deep convolutional generative adversarial networks," *IEEE Access*, vol. 6, pp. 38303–38314, 2018.
[11] W. Tang, S. Tan, B. Li, and J. Huang, "Automatic steganographic distortion learning using a generative adversarial network," *IEEE Signal Processing Letters*, vol. 24, pp. 1547–1551, 2017.
[12] J. Yang, D. Ruan, J. Huang, X. Kang, and Y.-Q. Shi, "An embedding cost learning framework using GAN," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 839–851, 2019.
[13] S. Bernard, T. Pevný, P. Bas, and J. Klein, "Exploiting adversarial embeddings for better steganography," in *Proc. the ACM Workshop on Information Hiding and Multimedia Security*, 2019, pp. 216–221.
[14] J. Zhu, R. Kaplan, J. Johnson, and L. Fei-Fei, "Hidden: Hiding data with deep networks," in *Proc. the European Conference on Computer Vision (ECCV)*, 2018, pp. 657–672.
[15] J. Hayes and G. Danezis, "Generating steganographic images via adversarial training," *Advances in Neural Information Processing Systems*, vol. 30, 2017.
[16] W. Tang, B. Li, S. Tan, M. Barni, and J. Huang, "CNN-based adversarial embedding for image steganography," *IEEE Transactions on Information Forensics and Security*, vol. 14, pp. 2074–2087, 2019.
[17] S. M. Badr, G. Ismaial, and A. H. Khalil, "A review on steganalysis techniques: From image format point of view," *International Journal of Computer Applications*, vol. 102, 2014.
[18] K. Karampidis, E. Kavallieratou, and G. Papadourakis, "A review of image steganalysis techniques for digital forensics," *Journal of Information Security and Applications*, vol. 40, pp. 217–235, 2018.
[19] A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems: Breaking the steganographic utilities EzStego, Jsteg, Steganos, and S-Tools-and some lessons learned," in *Proc. International Workshop on Information Hiding*, 1999, pp. 61–76.
[20] 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.
[21] J. Fridrich, M. Goljan, and R. Du, "Reliable detection of LSB steganography in color and grayscale images," in *Proc. the 2001 Workshop on Multimedia and Security: New Challenges*, 2001, pp. 27–30.
[22] T. Zhang and X. Ping, "Reliable detection of LSB steganography based on the difference image histogram," in *Proc. 2003 IEEE International Conference on Acoustics, Speech, and Signal Processing*, 2003, pp. 3–545.
[23] H. Malekmohamadi and S. Ghaemmaghami, "Steganalysis of LSB based image steganography using spatial and frequency domain features," in *Proc. 2009 IEEE International Conference on Multimedia and Expo*, 2009, pp. 1744–1747.
[24] W.-B. Lin, T.-H. Lai, and C.-L. Chou, "Chi-square-based steganalysis method against modified pixel-value differencing steganography," *Arabian Journal for Science and Engineering*, vol. 46, pp. 8525–8533, 2021.
[25] V. Sabeti, S. Samavi, M. Mahdavi, and S. Shirani, "Steganalysis and payload estimation of embedding in pixel differences using neural networks," *Pattern Recognition*, vol. 43, pp. 405–415, 2010.
[26] C. N. Bui, H.-Y. Lee, J.-C. Joo, and H.-K. Lee, "Steganalysis method defeating the modified pixel-value differencing steganography," *International Journal of Innovative Computing Information and Control*, vol. 6, pp. 3193–3203, 2010.
[27] C. Chatfield and H. Xing, *The Analysis of Time Series: An Introduction with R*, CRC Press, 2019.
[28] J. Rafiee and P. Tse, "Use of autocorrelation of wavelet coefficients for fault diagnosis," *Mechanical Systems and Signal Processing*, vol. 23, pp. 1554–1572, 2009.
[29] T. O. Kvålseth, "On the measurement of randomness (uncertainty): A more informative entropy," *Entropy*, vol. 18, p. 159, 2016.
[30] L. Sun, "Application of fourier transform in signal processing," *Signal and Information Processing*, vol. 1, 2018.
[31] N. M. Abdali and Z. M. Hussain, "Reference-free detection of LSB steganography using histogram analysis," in *Proc. 2020 30th International Telecommunication Networks and Applications Conference (ITNAC)*, 2020, pp. 1–7.
[32] H. Kheddar and D. Megías, "High capacity speech steganography for the G723.1 coder based on quantised line spectral pairs interpolation and CNN auto-encoding," *Applied Intelligence*, vol. 52, pp. 9441–9459, 2022.
[33] Break Our Steganographic System Base Webpage (BossBase). [Online]. Available: http://agents.fel.cvut.cz/boss/
[34] Z. I. Rasool, M. M. Al-Jarrah, and S. Amin, "Steganalysis of RGB images using merged statistical features of color channels," in *Proc. 2018 11th International Conference on Developments in eSystems Engineering (DeSE)*, 2018, pp. 46–51.
[35] M. Al-Jarrah, "Rgb-bmp steganalysis dataset," *Mendeley Data*, vol. 1, 2018.
[36] O. N. Kadhim and Z. M. Hussain, "Information hiding using chaotic-address steganography," *Journal of Computer Science*, vol. 14, no. 9, pp. 1247–1266, 2018.