1-1-2022

Reference-free differential histogram-correlative detection of steganography: Performance analysis

Natiq M. Abdali

Zahir M. Hussain
Edith Cowan University, z.hussain@ecu.edu.au

10.11591/ijeecs.v25.i1.pp329-338
Abdali, N. M., & Hussain, Z. M. (2022). Reference-free differential histogram-correlative detection of steganography: Performance analysis. Indonesian Journal of Electrical Engineering and Computer Science, 25(1), 329-338. https://doi.org/10.11591/ijeecs.v25.i1.pp329-338

Indonesian Journal of Electrical Engineering and Computer Science
Vol. 25, No. 1, January 2022, pp. 329~338
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v25.i1.pp329-338

Reference-free differential histogram-correlative detection of steganography: performance analysis

Natiq M. Abdali[1], Zahir M. Hussain[2,3]
[1]Department of Software, College of Information Technology, University of Babylon, Babylon, Iraq
[2]Faculty of Computer Science and Mathematics, University of Kufa, Najaf, Iraq
[3]School of Engineering, Edith Cowan University, Joondalup, Australia

Article Info

Article history:

Received Jul 14, 2021
Revised Nov 24, 2021
Accepted Dec 2, 2021

Keywords:

Computer security
Image processing
Image tampering
Signal processing
Steganalysis

ABSTRACT

Recent research has demonstrated the effectiveness of utilizing neural networks for detect tampering in images. However, because accessing a database is complex, which is needed in the classification process to detect tampering, reference-free steganalysis attracted attention. In recent work, an approach for least significant bit (LSB) steganalysis has been presented based on analyzing the derivatives of the histogram correlation. In this paper, we further examine this strategy for other steganographic methods. Detecting image tampering in the spatial domain, such as image steganography. It is found that the above approach could be applied successfully to other kinds of steganography with different orders of histogram-correlation derivatives. Also, the limits of the ratio stego-image to cover are considered, where very small ratios can escape this detection method unless modified.

Corresponding Author:

Zahir M. Hussain
Faculty of Computer Science and Mathematics, University of Kufa
Najaf, Iraq
Email: zmhussain@ieee.org

1. INTRODUCTION

Currently, billions of images may be found online. Images are used to capture real-life events, communicate information, and pursue other kinds of interests. Regrettably, due to notable advances in image steganography and its related software, terrorist gangs may now communicate messages using normal image communication with great efficiency. Since these steganographic softwares aim to disguise the payload as a random image-noise process produced by the electronic systems of the camera, identification of images related to illegal activity is difficult using the human eye alone. This technological threat to public security is a real-world problem. As a result, studies explored and created novel image steganalysis methods to prevent plus analyze this danger. One of the most popular secret communication approaches is image steganography, which involves concealing data in an image [1].

The goal of image steganography techniques is to introduce a difficult-to-detect alteration in order to hide a coded important message in a carrier image (cover object). Even in case a non-autorized entity notices the stego, concerns about the data contained in the cover image are almost unlikely since it appears to be a standard image. The most prevalent image steganography techniques fall into three categories: naive steganography [2], [3], adaptive steganography [4]-[8], and deep learning-based embedding [9]-[16].

As a result, in a manner similar to cryptanalysis, it is focused on cryptography. Steganalysis means the art and practice of detecting secret material or messages in a digital image (cover) and distinguishing between stego-object and the clean-cover object with little or no understanding of the steganography

techniques. The aim of steganalysis is to gather some evidence indicating the existence of an encoded message and it is the inverse of the process of steganography [17], [18]. Steganalysis may be classified into two principal categories: passive steganalysis and active steganalysis. Passive steganalysis attempts to detect the steganographic encoding technique and categorize a cover medium as stego, whereas active steganalysis attempts to find an estimation of the secret message length then, eventually, recover this secret information from the cover object [19], [20].

The following points are the main contributions of this study.

- The analysis of a novel detection approach for least significant bit (LSB) image steganography is presented, which is based on deriving the image histogram's auto-correlation property.
- The study of the system involved the detection of different methods of LSB image steganography.
- The system is used to detect other image steganography that uses different image formats. The proposed system findings demonstrated the method's effectiveness.
- The presented steganalysis does not rely on the availability of original images as neural network methods.

The rest of this paper is presented as follows: section 2 is concerned with reviewing related studies in a variety of areas; while section 3 presents correlation effects, investigation of the proposed system and performance measures. Section 4 presents extensive experimental (simulation) results. Based on the facts reported in this study, section 5 makes the conclusions.

2. RELATED WORKS

Fridrich *et al.* [21] suggested the RS steganalysis algorithm to detect LSB-embedding in color-images (24-bits) and grayscale-images (8-bits). During the level, each image pixel is split into 4 separate groups of four pixels (22 blocks), and the discriminating function f (.) is applied to each of these groups to detect their smoothness. Westfeld and Pfitzmann [22] suggested a framework that relies on analyzing pairs of values (PoVs) that are transmitted during the message-embedding process using the chi-square attack. The expected frequency-distribution of steganograms (which represents the arithmetic mean of two frequencies in a pair (PoV) because of the absence of the cover medium) with any sample distribution of stego medium.

Zang *et al.* [23] suggested an LSB Matching steganography system based on the detection of increasing and decreasing local minima and maxima in the stego histogram. The amplitude of the histogram is specified by using this tool. Given that embedding positions are evenly spread and, regardless of the pixel amount, the embedding degree(σ) is applied to just half of the LSB cost because the remainder already has the necessary content. As a result, 1-σ/2 of the pixel values have remained unchanged. The stego image histogram is also defined. This state (for both local extremum and local minimum) aids in image steganography detection.

Harmsen and Pearlman [24] used the histogram characteristic function (HCF) to recognize stego color images. Viswanatham and Manikonda [25] proposed an efficient and stable LSB insertion process. The strategy utilized the generation of random numbers as well as the selection of a relevant region (a region-of-interest, ROI) in which the appropriate message is to be encoded and placed in randomly-located pixels with previously generated addresses. The approach also includes a secret-key (which is the password necessary to decrypt the message), and this password must be provided by the receiver in order for the message (information) to be decoded from the carrier (cover image).

Yadav *et al.* [26] enhanced LSB strategy by using the final pair of bits of the pixels in the cover-image for the purpose of secret message-embedding and retrieval. In the process of embedding, in case the final pair of bits at the value of the pixel are either 00 or 10, the process embeds the secret-message as bit 0. If the final pair of bits of the pixel value are neither 00 nor 10, it tries to equal them to 00 or 10 by subtracting or adding 1 from the value of the pixel to embed 0. On the other hand, it embeds the secret-message as bit 1 at a pixel value if the final pair of bits of the pixel value are 01 or 11. If the final pair of bits are neither 01 or 11, we attempt to convert them to 01 or 11 by subtracting or adding 1 from that pixel value to embed 1. The message bit is 0 if the final pair of bits of a pixel in the retrieval process are 00 or 10. The opposite of that is 1.

Kadhim and Hussain [27] suggested and used a method based on a chaotic map to disguise a hidden-message (either text or smaller image) inside the larger cover-image by shuffling of the address bits. The proposed scheme employs a chaotic-map to produce an integer-valued chaotic series (represents the secret key), which are then used to choose the addresses of the cover-image pixels for the purpose of embedding the secret information (message). The parameters used by the chaotic-map are the secret-keys that should be known only to the sender and the receiver. Without recognizing these secret keys, the observer cannot sense the presence of a hidden message.

Janabi *et al.* [28] suggest a safe system for concealing a single or more extra images within a cover image of equal size. It employed a genetic algorithm strategy to produce the secret key and choose the best values for the mixing matrix. The key would be exchanged between the sender and the recipient to ensure that

special data remains secure and difficult for the untrustworthy to discover. Furthermore, the suggested technique improves the effectiveness of hiding capability, security level, and resistance to specific attacks.

3. RESEARCH METHOD

In this section, the main theory of the proposed research method is presented. Basically, it is found that variations in the derivatives of the autocorrelation function as applied to the cover-image histogram can be sensitive to any kind of tampering or steganographic content. In most cases, especially when the ratio of the message to the cover image sizes is not very small, the first-order derivative will be sufficient to discover tampering. However, when the ratio is very small, there is a challenge that may not be resolved by the first-order derivative, and higher orders would be necessary. Details will be presented in the next sub-sections.

3.1. Correlation effects

Correlation is a quatitative measure that indicats the degree of the relationship between two vectors or variables, in its widest definition. If the statistics of two variables are correlated, a modification in the amplitude of one variable can be affected by a change in the amplitude of another variable in the same direction (called positive correlation) or inverse direction (called negative correlation). The word correlation usually refers to a linear relation (association) between two continuous-valued variables, which is normally expressed using Pearson formula for product-moment correlation.

For combined normally-distributed variables (data that follows a bivariate normal distribution), the Pearson correlation-coefficient is generally the most relevant. For continuous data that is not ordinarily transferred, ordinary data, or for data including outliers, the Spearman-rank correlation formula could be utilized as a measure of the monotonic relation. All formulas for correlation-coefficients have a range from –1 to +1, with 0 indicating that there is no linear (i.e., monotonic) relation, and as the coefficient absolute-value approaches 1, the relationship between the variables becomes stronger and eventually reaches a straight line (Pearson correlation) or becomes a continuously-expanding or continuously-decreasing curve (Spearman correlation). Theory analyses and trust periods can be applied to evaluate the statistical validity of the decisions and estimate the intensity of the association in the society from which the data is sampled [29]. The cross-correlation of two waveforms was used to determine their similarity as a function of a time-lag applied to one of them. The cross-correlation of a signal with itself is known as autocorrelation. It is a time domain analysis that can be used to determine a signal's periodicity or repeated patterns. The autocorrelation function (ACF) is a popular metric for detecting whether or not there is a serial relationship. Because it provides a more detailed representation of the basic process, the autocorrelation function is more useful than the cross-coefficient test. In (1) calculates the autocorrelation for a real-valued signal x(n) with a length of N samples [30].

$$R_x(k) = \frac{1}{N}\sum_{n=0}^{N} x(n)x(n+k) \quad (1)$$

While image correlation changes when the image is loaded with stego-information, the changes in its pixel correlations are not significant enough to be detected. Hence, direct correlative analysis of stego image may fail to detect tampering. However, much stronger changes have been detected in the derivatives of histogram correlation [31]. In [31], we found that the first derivative of the histogram correlation can detect LSB-steganography. However, we didn't study other stego methods. In this work, we will show that higher-order derivatives could be necessary for other types of steganography or tampering.

3.2. The histogram-correlative detection system

According to the correlation examination discussed in the previous section, the extended framework of the LSB steganalysis method in this work is advised. The appearance of a hidden-message in the cover-image can be detected using LSB-steganalysis. The suggested system was extended to detect three different LSB image-steganography and discover image-steganography using other different approaches. The proposed scheme computed the histogram-correlative of the image and took the first three derivatives to detect image tampering. When tampering is present, the derivatives of the histogram-correlation of the image will have noticeable vibrations. Using a filter as a threshold would result in a decision. The general architecture of the proposed approach for tampering detection is shown in Figure 1.

3.3. Measures of performance evaluation

The examination of steganographic methods is required to see if one is superior to another. Therefore, various criteria are used to examine steganographic approaches. The visual quality of steganography may be measured using a variety of methods (e.g., MSE, PSNR) [32].

Mean-squared error (MSE) indicates the sum of squares of pixelwise-error between the original cover image and the modified cover image, and MSE evaluates the amount of image distortion. Peak signa-to-noise ratio (PSNR) is the ratio of the maximum pixel-value to the noise power (MSE between the modified and the original images). PSNR is used to measure image quality. The following (2) and (3) may be used to compute MSE and PSNR.

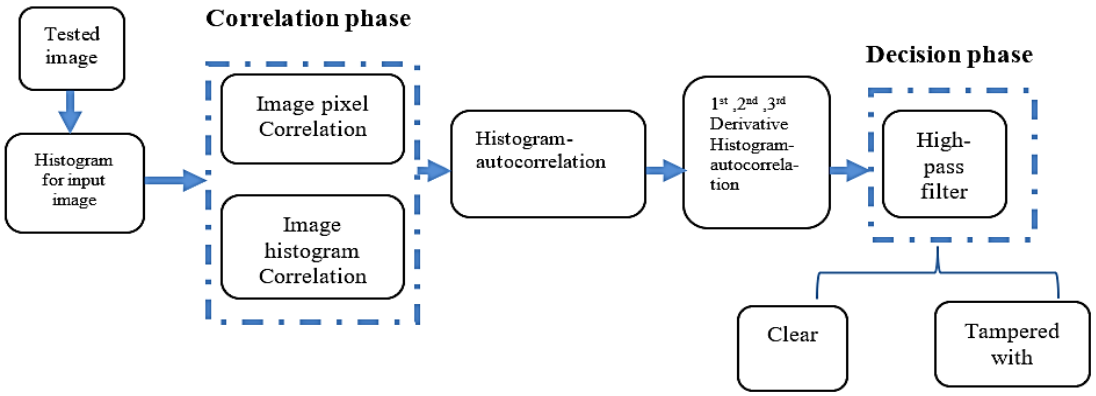


Figure 1. The block diagram of the proposed system

$$\text{MSE} = \frac{1}{H \times W} \sum_{r=0}^{H-1} \sum_{c=0}^{W-1} [I'(r,c) - I(r,c)]^2 \quad (2)$$

$$\text{PSNR} = 10 \times \log_{10} \frac{{I_{max}}^2}{\text{MSE}} \quad (3)$$

where $I(r,c)$ is the cover-image pixel-value, $I'(r,c)$ is the modified pixel-value, $H \times W$ represents the size (height by width) of the carrier (cover-image), I_{max} = maximum pixel-value, that is, 255 (if the system uses 0-255 range; otherwise 1 for 0-1 systems).

Different sizes of the secret image (cell.tif from MATLAB, under Academic License 40635944, is used as a secret message image, resized to 5*5, 10*10, 20*20, and 30*30). The size ratio R_m between message size and cover size may be computed by the following formula:

$$R_m = \frac{\text{Message Size}}{\text{Cover Image Size}} \quad (4)$$

where this ratio has a decisive role in the steganalysis process.

4. EXPERIMENTAL RESULTS AND DISCUSSION

The suggested system was tested on three different LSB steganography techniques to conceal the message in the grey-scale image, and it tested the suggested system on another different steganography approach with a color image. The proposed method should be able to detect tampered images. Figure 2 describes the grey-scale images used in these experiments, with the message modified to achieve various message-to-cover ratios (R_m). As the histogram-correlative of the image is derivation, LSB-stego introduces major ripples. As a result, the HP (high-pass) filtering applied to this derivative would be a useful method for detecting these ripples, where a threshold can be used [31].

Figures 3-5 depict the effect of the first, second and third derivatives on the histogram-correlation of the cover-image and K-LSB, Chaotic-LSB stego images. If the message is small compared to the cover (R_m), we should use the second and third derivatives, since the first is unclear. The effect of the first, second, and third derivatives on the histogram-correlation of the cover-image and K-LSB-image, enhanced-LSB stego-images, is seen in Figures 6(a)-(c). The method fails if the message size is very small ($R_m < 0.01$). Higher derivatives are almost certainly required (and will be handled in future work).

K_m represents the number of different hidden message sizes in the system. K_m=[5 10 20 30 50 100 150]. As a result, Chaotic-LBS is not appropriate for large $R_m > 0.1$and $K_m > 65$, so only K-LSB and enhanced-LSB are compared. The proposed system in the following experiment tested a different image steganography approach, this time using a color image format (BMP) [28].

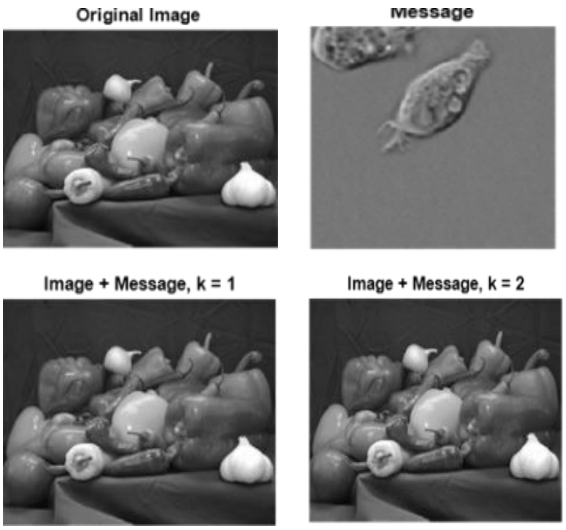


Figure 2. The grey-scale cover and stego MATLAB images

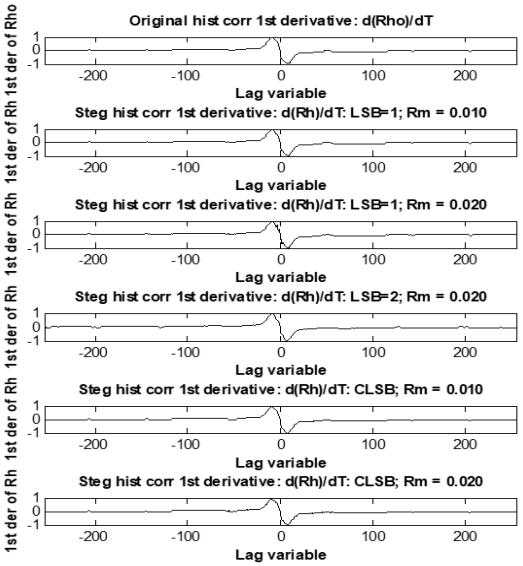


Figure 3. The 1st derivative of the histogram-correlative for Chaotic_LSB, K_LSB stego and cover images for several LSB-levels and several messages to cover-size ratios

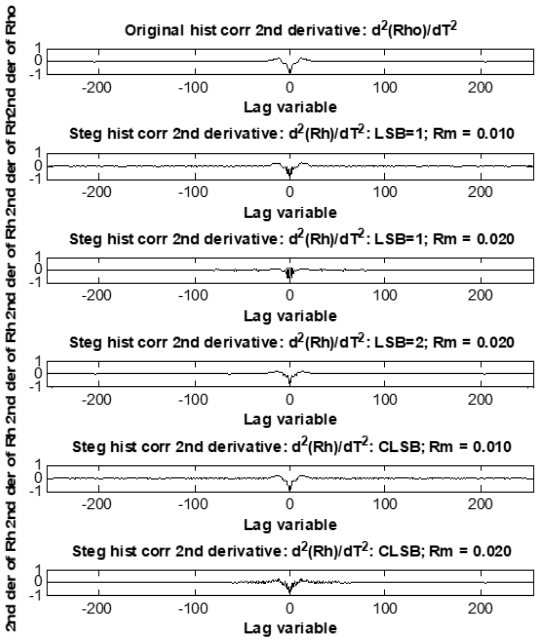


Figure 4. The 2nd derivative of the histogram-correlative for Chaotic_LSB, K_LSB stego and cover images for several LSB-levels and several messages to cover-size ratios

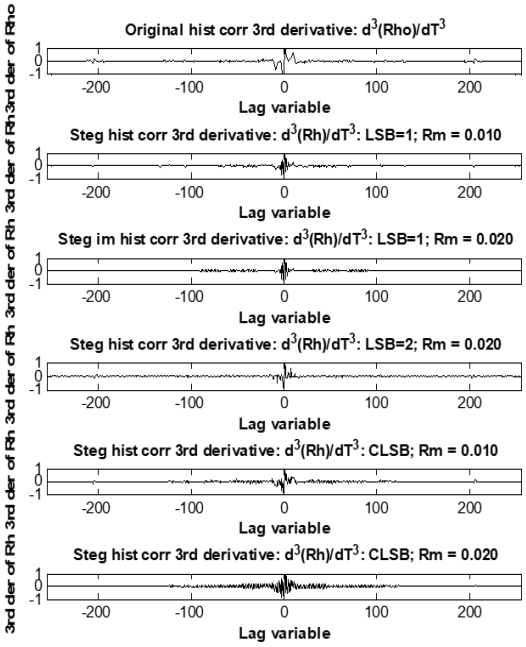
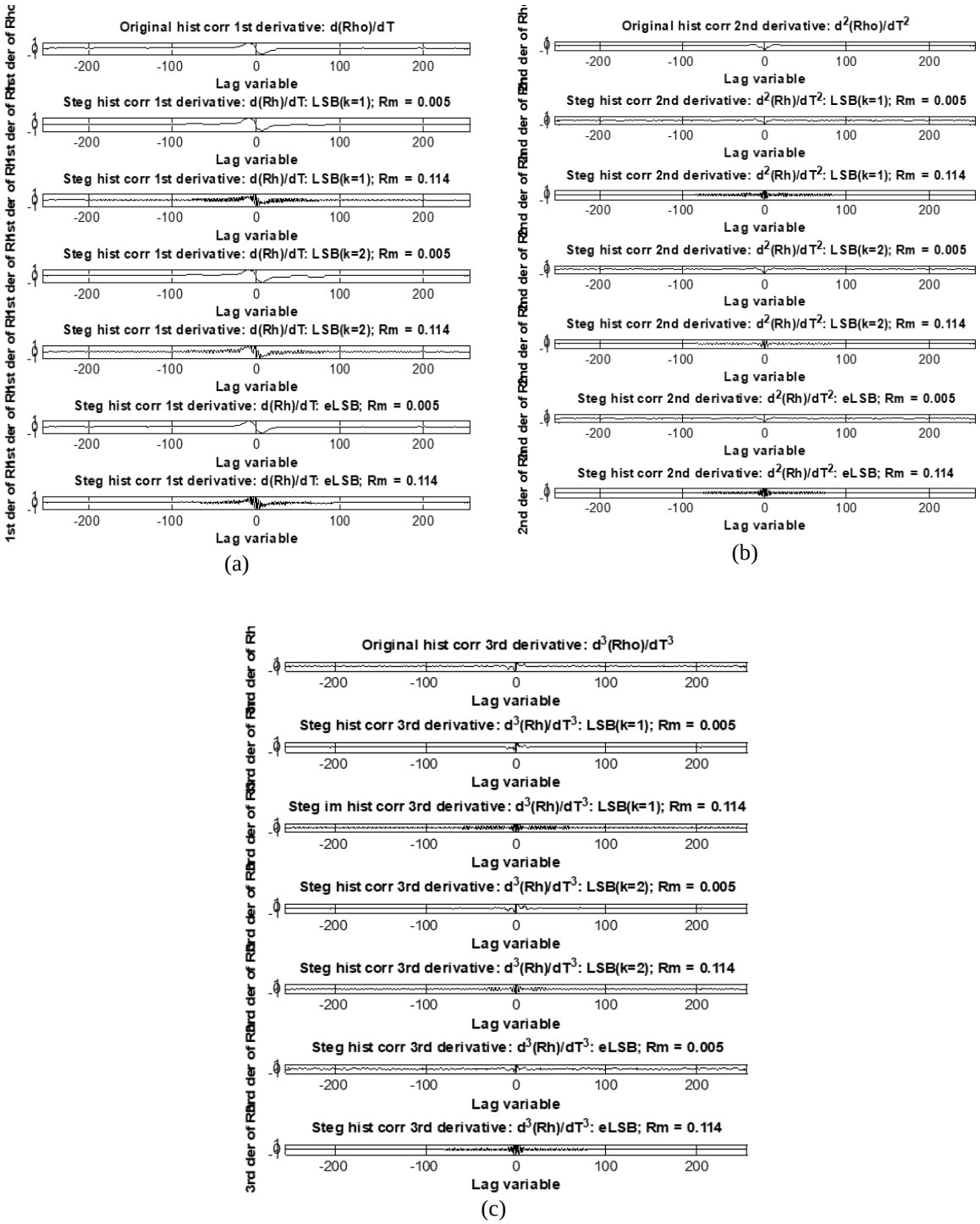


Figure 5. The 3rd derivative of the histogram-correlative for Chaotic_LSB, k_LSB stego and cover images for several LSB-levels and several messages to cover-size ratios

Figure 7 shows cover, message and stego images used for results in Figure 8 which shows the influence of the first derivative of the histogram-correlative for cover and stego color images. Figures 9 and 10 show the results for a different set of images. According to Figures 8, 10 and Tables 1 and 2, the first derivative is sufficient to detect image tampering, as evidenced by the influence of the PSNR value, image type for the cover and message images, and whether they are 256 or true color. If the PSNR is high, we should probably use the second and third derivatives instead of the first because the first is vague.

From the results, we found that the proposed system is capable of detecting the small secret message. It uses high derivatives, whether it is employed to detect the LSB or various other steganography methods. It deserves seeing since the neighboring histogram points correlation diminishes with the increase of the ratio R_m, which is the ratio measuring the message-size to cover-image size. Figure 11 demonstrates this truth. Figure 11 depicts the correlation between neighboring histogram points for cover-image and K-LSB stego-images for various K powers.



(a) (b)

(c)

Figure 6. The derivative of the histogram-correlative for enhanced_LSB, K_LSB stego and cover images for several LSB-levels and several messages to cover-size ratios: (a) first derivative, (b) second derivative, (c) third derivative

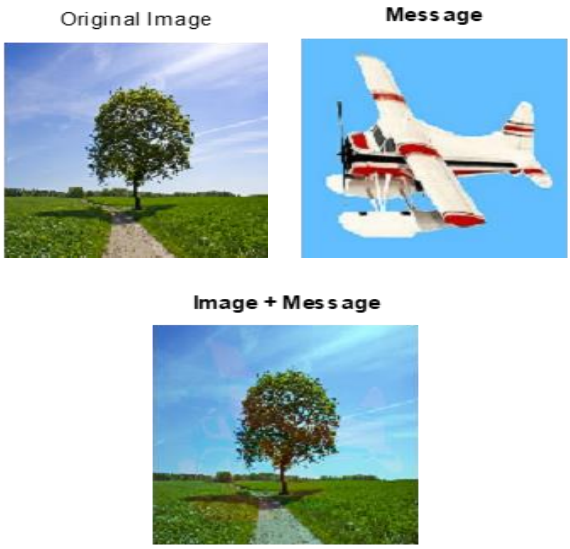


Figure 7. The images of the cover (true color), message (256 color) and stego (true color)

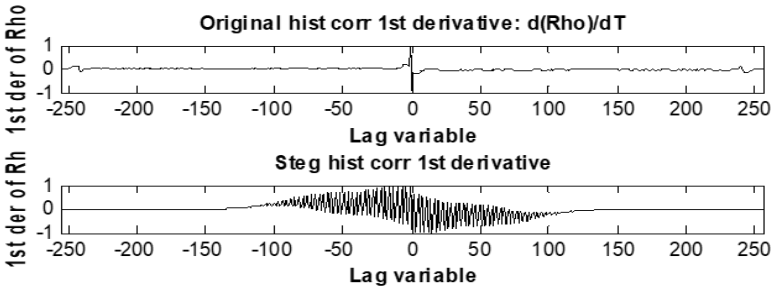


Figure 8. The 1st derivative of the histogram-correlative for cover and stego color images

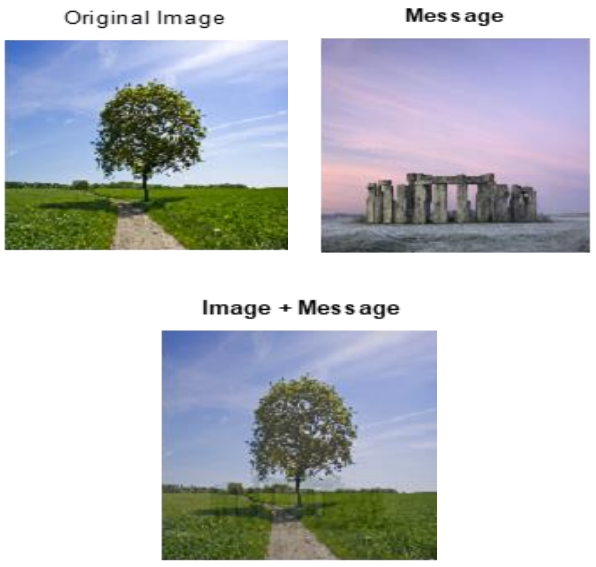


Figure 9. The cover, the message and the stego images are all in true color

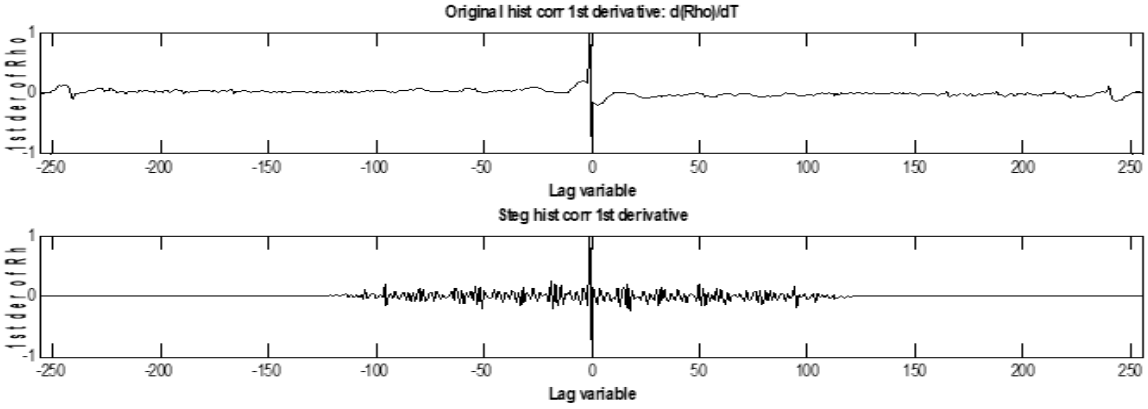


Figure 10. The 1st derivative of the histogram-correlative for cover and stego color images

Table 1. Details of hiding an image in a cover image as in Figure 7

Mixing Matrix	PSNR	MSE	Cover size
[0.002 0.9 0.7 0.2]	52.603	0.598	256×256 pixels

Table 2. Details of hiding an image in a cover image as in Figure 9

Mixing Matrix	PSNR	MSE	Cover size
[0.001 0.9 0.6 0.2]	58.038	0.320	256×256 pixels

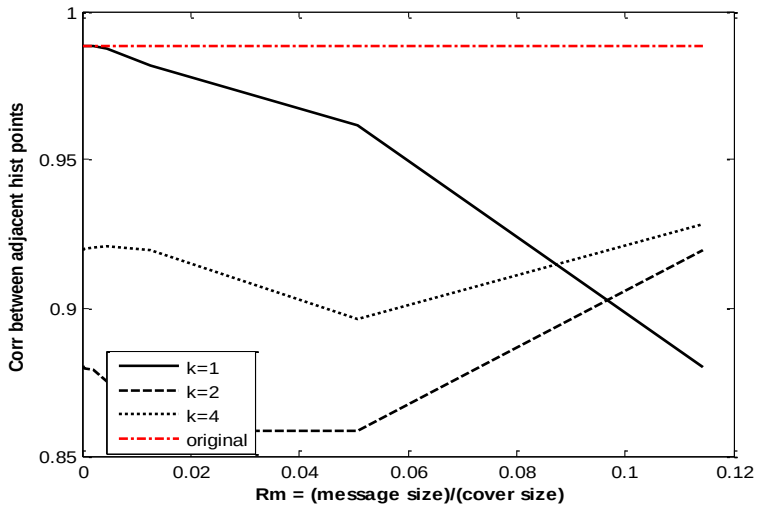


Figure 11. Correlation between adjacent histogram points for cover and K-LSB stego-images for various K

5. CONCLUSION

A spatial domain steganalysis scheme is proposed. This method is validated with various LSB steganography approaches and is applied to other steganography approaches. The proposed method will determine whether an image was tampered with or not without relying on the original image. It employs analysis of the histogram correlative method. The suggested system is based on the reality that if the image has been modified (tampered) with a secret message, the derivative of the correlation of the histogram of the image will show noticeable vibrations. This fact appears in various steganography methods, whereas if the message size is very limited ($R_m < 0.01$), the system fails. The use of higher derivatives is almost certainly required. Since the first derivative is vague whether the message is limited in comparison to the cover (R_m), we can use the second and third derivatives. The proposed system discovered that Chaotic-LBS is not suitable for large $R_m > 0.1$ When analyzing the system, only K-LSB and enhanced-LSB are compared. As a result, examine this technique for other steganographic approaches as well. It was discovered that the method described above may be successfully applied to other types of steganography using higher orders of histogram-correlation derivatives.

ACKNOWLEDGEMENTS

The Authors would like to thank Edith Cown University, Australia for partially supporting this project via the ASPIRE Program.

REFERENCES

[1] W. You, H. Zhang, and X. Zhao, "A Siamese CNN for Image Steganalysis," *IEEE Transactions on Information Forensics and Security*, vol. 16, 2021, doi: 10.1109/TIFS.2020.3013204.
[2] R. G. Van Schyndel, A. Z. Tirkel, and C. F. Osborne, "A digital watermark," in *Proc. 1st Int. Conf. Image Process.*, pp. 86-90, Nov. 1994, doi: 10.1109/ICIP.1994.413536.
[3] R. Cogranne, C. Zitzmann, L. Fillatre, F. Retraint, I. Nikiforov, and P. Cornu, "A cover image model for reliable steganalysis," in *Proc. 13th Int. Conf. Inf. Hiding, Prague, Czech Republic*, pp. 178-192, May 2011, doi: 10.1007/978-3-642-24178-9_13.
[4] V. Holub and J. Fridrich, "Digital image steganography using universal distortion," in *Proc. 1st ACM Workshop Inf. Hiding Multimedia Secur*.IH&MMSec, pp. 17-19, 2013, doi: 10.1145/2482513.2482514.
[5] B. Li, M. Wang, J. Huang, and X. Li, "A new cost function for spatial image steganography," in *Proc. IEEE Int. Conf. Image Process. (ICIP)*, pp. 27-30, Oct. 2014, doi: 10.1109/ICIP.2014.7025854.
[6] T. Pevný, T. Filler, and P. Bas, "Using high-dimensional image models to perform highly undetectable steganography," in *Proc. 12th Int. Conf.Inf. Hiding (IH)*, Calgary, AB, Canada, Jun. 2010, pp. 28-30, doi: 10.1007/978-3-642-16435-4_13.
[7] V. Holub and J. Fridrich, "Designing steganographic distortion using directional filters," in *Proc. IEEE Int. Workshop Inf. Forensics Secur. (WIFS)*, pp. 234-239, Dec. 2012, doi: 10.1109/WIFS.2012.6412655.
[8] V. Sedighi, R. Cogranne, and J. Fridrich, "Content-adaptive steganography by minimizing statistical detectability," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 2, pp. 221-234, Feb. 2016, doi: 10.1109/TIFS.2015.2486744.
[9] H. Shi, J. Dong, W. Wang, Y. Qian, and X. Zhang, "SSGAN: Secure steganography based on generative adversarial networks," in *Proc. Pacific–Rim Conf. Multimedia (PCM)*, Harbin, China, Sep. 2017, pp. 534-544, doi: 10.1007/978-3-319-77380-3_51.
[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, doi: 10.1109/ACCESS.2018.2852771.
[11] W. Tang, S. Tan, B. Li, and J. Huang, "Automatic steganographic distortion learning using a generative adversarial network," *IEEE Signal Process. Lett.*, vol. 24, no. 10, pp. 1547-1551, Oct. 2017, doi: 10.1109/LSP.2017.2745572.
[12] J. Yang, D. Ruan, J. Huang, X. Kang, and Y.-Q. Shi, "An embedding cost learning framework using GAN," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 839-851, 2019, doi: 10.1109/TIFS.2019.2922229.
[13] S. Bernard, T. Pevný, P. Bas, and J. Klein, "Exploiting adversarial embeddings for better steganography," in *Proc. ACM Workshop Inf.Hiding Multimedia Secur.*, pp. 216-221, Jul. 2019, doi: 10.1145/3335203.3335737.
[14] 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, doi: 10.1007/978-3-030-01267-0_40.
[15] J. Hayes and G. Danezis, "Generating steganographic images via adversarial training," in *Proc. Annu. Conf. Neural Inf. Process. Syst. (NIPS)*, Long Beach, CA, USA, Dec. 2017, pp. 1954-1963.
[16] W. Tang, B. Li, S. Tan, M. Barni, and J. Huang, "CNN-based adversarial embedding for image steganography," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 8, pp. 2074-2087, Aug. 2019, doi: 10.1109/TIFS.2019.2891237.
[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* (0975 – 8887), vol. 102, no. 4, September 2014, doi: 10.5120/17802-8617.
[18] K. Karampidis, E. Kavallieratou, and G. Papadourakis, "A review of image steganalysis techniques for digital forensics," *Journal of Information Security and Applications*. Elsevier, vol. 40, pp. 217-235, 2018, doi: 10.1016/j.jisa.2018.04.005.
[19] A. Nissar and A. H. Mir, "Classification of steganalysis techniques: A study," *Digital Signal Processing*, vol. 20, no. 6, pp. 1758-1770, Elsevier, Dec. 2010, doi: 10.1016/j.dsp.2010.02.003.
[20] P. Richer, "Steganalysis: Detecting hidden information with computer forensic analysis," *SANS Institute Information Security Reading Room*, 2019, [Internet] 2019 Aug [cited 2019 Nov 5]; Available online.
[21] J. Fridrich, M. Goljan, and R. Du, "Reliable Detection of LSB Steganography in Color and Grayscale Images," *Proc. Of ACM Workshop on Multimedia and Security*, Ottawa, Oct. 5, pp. 27-30, 2001, doi: 10.1145/1232454.1232466.
[22] A. Westfeld and A. Pfitzmann, "Attacks on Steganographic Systems," in Andreas Pfitzmann (Ed.): *Information Hiding*, LNCS 1768, pp. 61-76, 1999, doi: 10.1007/10719724_5.
[23] J. Zhang, I. J. Cox, and G. Doerr, "Steganalysis for LSB Matching in Images with High frequency Noise," in: *Proc. IEEE 9th Workshop on Multimedia Signal Processing, MMSP 2007* (October 1- 3, October 19, September 16), pp. 385-388, 2007, doi: 10.1109/MMSP.2007.4412897.
[24] J. J. Harmsen and W. A. Pearlman, "Steganalysis of Additive Noise Modelable Information Hiding," in *Proc. SPIE, Security Watermarking Multimedia Contents*, pp. 131-142, 2003, doi: 10.1117/12.476813.
[25] V. M. Viswanatham and J. Manikonda, "A novel technique for embedding data in spatial domain," *Int.J. Computer Science Eng*., vol. 2, pp. 233-236, 2010.
[26] R. Yadav, R. Saini, and G. Chawla, "A novel approach for image steganography in spatial domain using last two bits of pixel value," *Int. J. Security*, vol. 5, 51-61, 2011.
[27] 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, doi: 10.3844/jcssp.2018.1247.1266.
[28] S. A.-Janabi and I. A.-Shourbaji, "A Hybrid Image Steganography Method based on Genetic Algorithm," *7th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT)*, 2016, doi: 10.1109/SETIT.2016.7939903.
[29] P. Schober, C. Bower, and L. A. Schwarte, "Correlation Coefficients: Appropriate Use and Interpretation," *Anesthesia & Analgesia*, 2018, doi: 10.1213/ANE.0000000000002864.
[30] A. Z. Sadik, Z. M. Hussain, and P. O'Shea, *Digital Signal Processing: An Introduction with MATLAB and Applications*, Springer, 2011, doi: 10.1007/978-3-642-15591-8.
[31] N. M. Abdali and Z. M. Hussain, "Reference-free Detection of LSB Steganography Using Histogram Analysis," *2020 30th International Telecommunication Networks and Applications Conference (ITNAC)*, 25-27 Nov, IEEE Xplore Press, Melbourne, VIC, Australia, 2020, pp. 1-7, doi: 10.1109/ITNAC50341.2020.9315037.

[32] M. Tayel, H. Shawky, and A.D. Sayed Hafez, "A new chaos steganography algorithm for hiding multimedia data," *Proceedings of the 14th International Conference on Advanced Communication Technology*, Feb. 19-22, IEEE Xplore Press, Pyeong Chang, South Korea, pp. 208-212, 2012.

BIOGRAPHIES OF AUTHORS

Natiq M. Abdali holds an MSc degree in computer science from the University of Babylon. He is currently doing his PhD in Computer Science at the University of Babylon under the supervision of Prof. Zahir M. Hussain. His interests are image processing, computer security, and signal processing. He can be contacted at email: natiq197699@gmail.com; art.natiq.mutashar@uobabylon.edu.iq.

Zahir M. Hussain got his BSc and MSc degrees from the University of Baghdad and his PhD from Queensland University of Technology (Australia) in 2002. On 1st June 2001 he moved to join the School of Electrical & Computer Engineering, RMIT, Australia, where he led a 3G communication project 2001-2002 (jointly with NEC). He has written over 300 publications. While at RMIT, he received an ARC Discovery Grant (2005-2008) with Professor Peter O'Shea to do research on the proposed short word-length systems. In 2005 he was promoted to Associate Professor of signal processing at RMIT. He got RMIT Publication Awards for 2005 and 2006, and RMIT Teaching Award for 2007. He has been a senior member of the IEEE and the Australian Computer Society (ACS); also, he got the title of Chartered Scientist from the British Science Council in 2020. He attended over 50 international conferences; worked on the TPC of many leading conferences, and served as a reviewer for leading journals, including MDPI Sensors, at which he is currently an Editor. He examined over 70 PhD Theses, and supervised 29 PhD's. In 2010 he joined the University of Kufa as a Professor of Signal Processing, while RMIT granted him Adjunct Professorship 2010-2013, then in 2014 he joined Edith Cowan University (Australia) as a Professor at the School of Engineering. He can be contacted at email: zahir.husain@uokufa.edu.iq; z.hussain@ecu.edu.au; zmhussain@ieee.org.