Pakistan Journal of Engineering and Technology, PakJET
Multidisciplinary & Peer Reviewed
Volume: 5, Number: 2, Pages: 183- 187, Year: 2022

A Binary Pattern Based Secure Data Hiding in Digital Images

Mareena Karim, and Sahib Khan*

Department of Telecommunication Engineering, University of Engineering and Technology Mardan, 23200 Mardan, Pakistan
Corresponding author: Sahib Khan (e-mail: sahib@uetmardan.edu.pk).

Received: 10/05/2022, Revised: 11/07/2022, Accepted: 25/08/2022

Abstract- **Information security is one of the most challenging tasks in the recent era of advanced technologies and communication. It is important to ensure the secure exchange of confidential data. Data hiding techniques have a key role in ensuring security. The proposed technique is one such technique to enhance the security of secret information by many folds. The proposed technique detects a binary pattern to classify the cover image pixels into two groups of pixels, i.e., the group of pixels used for information hiding and the group of pixels that remains unaffected. The secret information is hidden in the selected pixels using LSB substitution without creating any detectable modifications. The results show that the technique creates a high-quality stego image with a PSNR larger than the threshold level of 30*dB* and SSIM higher than 0.9999. Along with the good quality of the stego images, the binary pattern enhances the security of the hidden information twofold.**

***Index Terms*—Data hiding, Kirsch edge detector, LSB substitution, PSNR, SSIM.**

I. INTRODUCTION

The internet has brought convenience and advancement in digital communication technologies, with some risks regarding security like intercepting and stealing information [1, 2]. Securing information from hacking and unauthorized access, cryptography, and data hiding techniques are used [3]. Data hiding is the method of placing secret information in cover media in such a way that its presence is kept undetectable, and the secret information remains inaccessible to an authorized person. Due to the imperceptibility of secret information, data hiding techniques attracted the attention of forensics experts [4, 5].

The data hiding can be done using different types of cover media, e.g., image, text, audio, and video [6], as a medium for hiding secret data. However, the high redundancy level of the digital image makes than the most suitable media to be used as a cover medium. Secret data has usually hidden the elements of cover media by replacing the contents of cover media with the contents of secret data. The least significant bits (LSB) of cover image pixels are used for secret data substitution in the spatial domain or the least significant portion of the coefficients of a transformation of the cover image. The spatial domain technique hides secret data in the LSBs of the cover image. The spatial domain techniques include Hussain, Mehdi, et al [7], Least Significant Bit (LSB) [8], PVD-based data hiding [9], EMD-based technique [10] and others. While the transform domain technique, the hiding process uses the transform coefficients for information hiding; these include PMM-based data hiding [11] and other techniques given in [6, 10].

The techniques, as mentioned earlier, hide information in both complex and flat regions of the cover image. However, the human visual system (HVS) has a natural tendency to be more sensitive to the changes made in the flat region of an image in comparison with the complex part. Therefore, to keep the presence of the secret information innocent, the information is hidden in complex part's pixels rather than the pixel belonging to the flat region. The complex region can be detected using various techniques including Canny edge detector [12], Sobel edge detector [13], Prewitt edge detector [14], ACO-based edge detection [15], and others. The data hiding technique targeting complex region for data hiding include BEASS [16], 2LSB substitution [17], ACO-based hiding [18], and other techniques.

The Kirsch edge detector has also been used in [19] for data hiding. However, the technique has exploited both smooth and complex regions for information hiding which increases hiding capacity and decreases the PSNR. At the same time, the proposed technique explores only the complex region for information hiding and leaves the smooth region unaffected. The proposed technique, therefore, results in much higher quality stego images. Alon with high quality, the binary pattern and different possible threshold τ, further enhance the security of the proposed technique by many folds.

II. PROPOSED ALGORITHM

KED-DH technique is intended to hide confidential bits in the LSB of the selected pixels, i.e., the pixels part of the complex

This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

region within the cover image. The hiding in the cover image's complex region keeps the existence of the secret information innocent and undetectable to an intruder. KED-DH technique consists of the following stages:

- Edge Detection
- LSB Substitution
- Information Retrieval

The edge detection process enables the algorithm to isolate the complex region pixels from the flat region pixels of the cover image. As discussed in Section 1, several techniques exist to perform this task. KED-DH technique uses the Kirsch edge detector for this purpose due to the high efficiency and stable results Kirsch edge detector. While applied to a cover image, the Kirsch edge detector results in an image having edges only, and the complex region of the cover image is completely isolated from the flat region. The Kirsch edge detector process is given in (1).

$$EI = KE(I) \tag{1}$$

where I, KE, and EI represent the cover image, Kirsch edge detector, and edges detected by the Kirsch edge detector, respectively.

The detected edges EI are further processed to get a binary pattern E. The process is called thresholding as given in (2).

$$E(i,j) = \begin{cases} 1, if EI(i,j) \geq \tau \\ 0, if EI(i,j) < \tau \end{cases} \tag{2}$$

where, τ is the threshold value.

The binary pattern E is then used to identify the pixels belonging to the complex region and to hide secret information in the complex region. The secret information is hidden in the complex region using the 4LSB substitution mechanism. The cover image is processed pixel by pixel, and each pixel belonging to the complex region is subjected to the hiding process. The 4 LSB of the pixel is substituted with 4 bits of secret message. While the pixel belonging to a flat region remains unaffected. The process of data hiding is completed when all pixels are processed for 4LSB substitution, or all the secret message bits are hidden in the cover image. The process results in a stego image with embedded confidential data.

The stego image is shared with the intended party using any communication link or system. At the same time, the secure binary pattern is shared with the known party via a third trusted party. On the receiver side, the intended user will attempt to retrieve the hidden information using the binary pattern. The pattern identifies the pixels used for hiding information. The information is retrieved by reading the 4 LSB of the pixels identified by the binary pattern. The complete process of edge detection, hiding, sharing, and retrieving the hidden information is shown in Fig. 1.

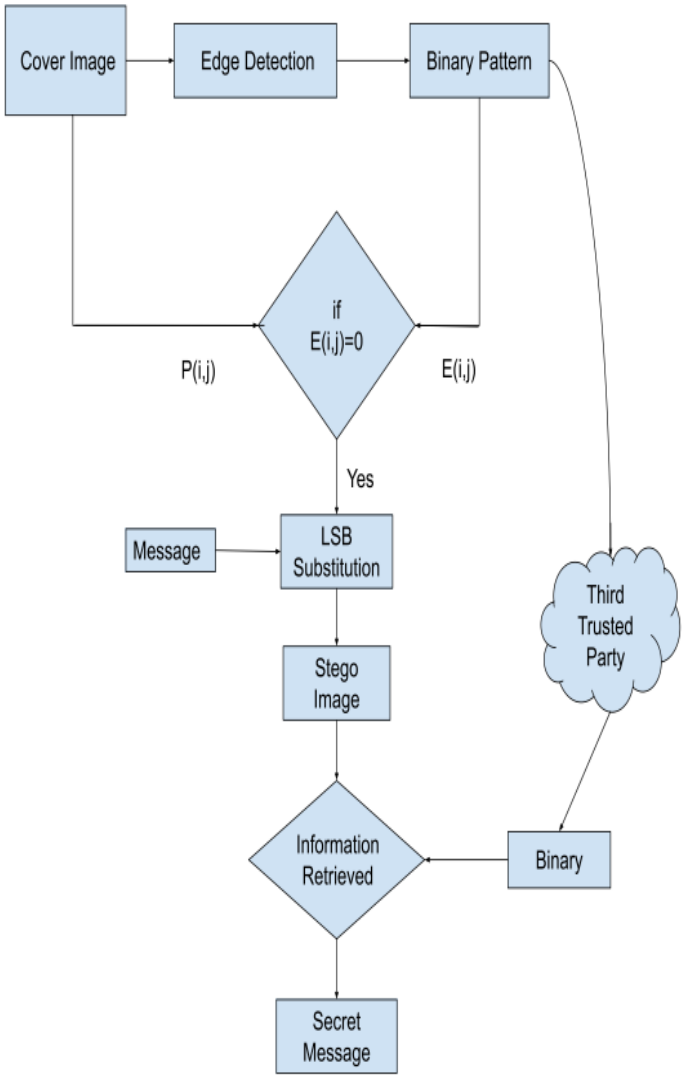


FIGURE 1: Process of edge detection

(a) Lena Cover (b) Lena Edge

FIGURE 2. Lena cover image and the edge pattern

III. EXPERIMENTAL RESULTS AND ANALYSIS

The effectiveness of the KED-DH clustering algorithm is analyzed for different values of τ using a single cover image of Lena given in Fig. 2(a). The cover image is processed with a Kirsch edge detector, and the resulting image, with edge information only, is shown in Fig. 2(b).

The image shown in Fig. 2(b) is processed to get a binary pattern. The binary pattern can be obtained using different threshold levels τ. The Lower the threshold value, the more pixels are assigned to

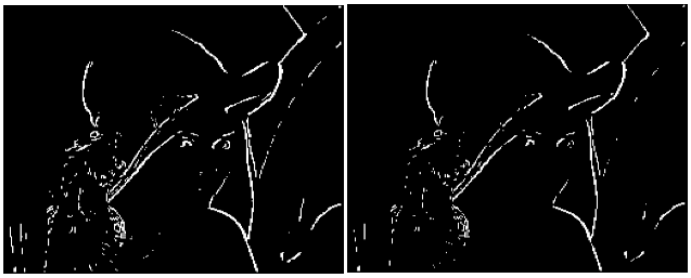
the binary pattern, and the higher the value of the τ result, the less the number of pixels in the complex region.

(a) $\tau = 200$ (b) $\tau = 400$

(c) $\tau = 600$ (d) $\tau = 800$

(e) $\tau = 1000$ (f) $\tau = 1200$

(g) $\tau = 1400$ (h) $\tau = 1600$



(i) $\tau = 1800$ (j) $\tau = 2000$

FIGURE 3. The binary pattern for different thresholds

KED-DH technique is tested for different values of τ, i.e., 200, 400, 600, 800, 1000, 1200, 1400, 1600, 1800 and 2000. The resulting binary patterns are shown in Fig. 3(a-j), respectively.

(a) $\tau = 200$ (b) $\tau = 400$

(c) $\tau = 600$ (d) $\tau = 800$

(e) $\tau = 1000$ (f) $\tau = 1200$

(g) $\tau = 1400$ (h) $\tau = 1600$

(i) $\tau = 1800$ (j) $\tau = 2000$

FIGURE 4. The stego image for different thresholds

The binary patterns shown in Fig.3(a-j) are used for hiding confidential bits in the complex part of the cover image given in Fig. 2(a), using the KED-DH data hiding technique. The stego image obtained for different values of τ, i.e., 200, 400, 600, 800, 1000, 1200, 1400, 1600, 1800 and 2000 are shown in Fig. 4(a-j), respectively. The qualitative and visual results show that the KED-DH algorithm results in good quality stego image for the different values of τ. The hidden information in each resulting stego image does not leave any visually significant traces or distortion. Hence, the KED-DH technique keeps the mere existence of confidential information innocent and undetectable to any intruder or unauthorized person.

The performance of the KED-DH technique is also measured quantitatively based on the parameters of peak signal-to-noise ratio PSNR, structural similarity index SSIM, and hiding capacity HC. The quantitative results show that the PSNR and SSIM of KED-DH increase with the value of τ, as shown in Fig. 5 and Fig. 6, respectively. While the HC of the KED-DH technique decreases with an increase in the value of τ, as presented in Fig.7.

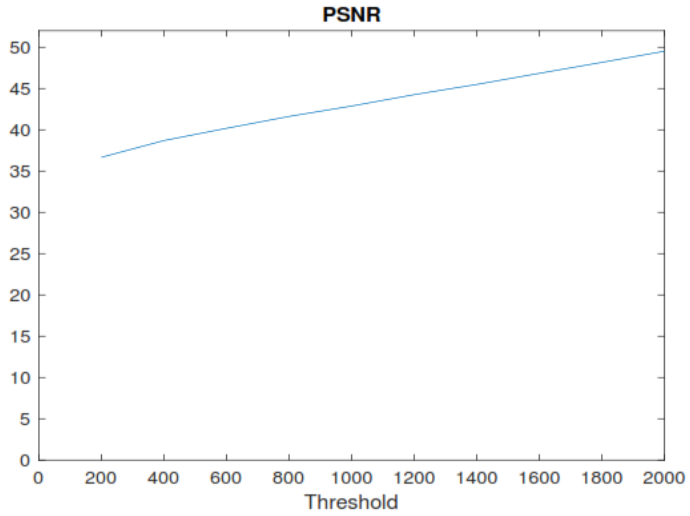


FIGURE 5. Psnr for different value of threshold

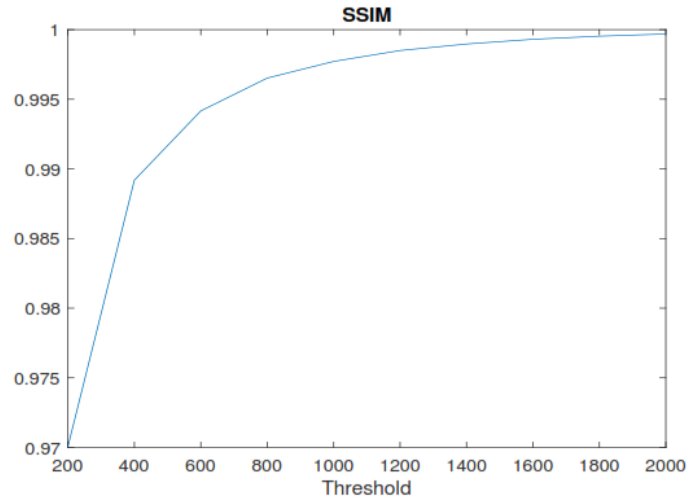


FIGURE 6. SSIM for different value of threshold

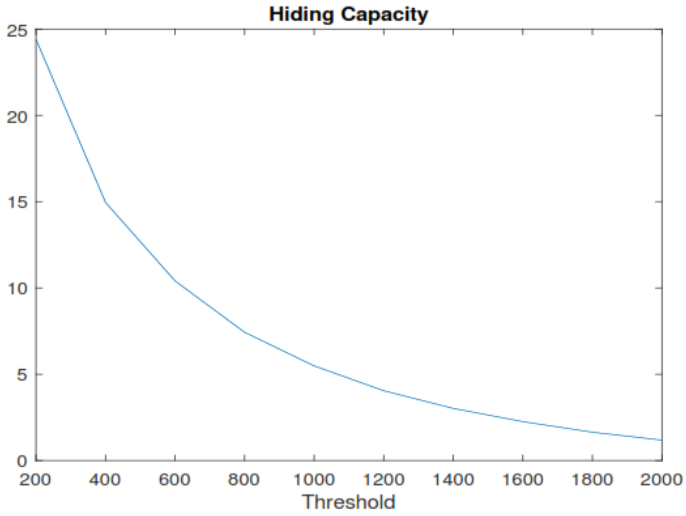


FIGURE 7. Hiding capacity for different value of threshold

IV. COMPARISON

The presented results are in Section. 3, shows that the KED-DH technique results in high-quality stego images and PSNR higher than the 30dB. In this section KED-DH technique, with τ = 1000, is compared with the state-of-the-art data hiding techniques, i.e., THMI technique [20], RDH technique [21], APSI-based data hiding technique [22], DFDE technique [23], CIHRW technique [24], STE based 4LSB hiding technique [8], Khan and Tiziano [18] and [19]. The algorithms are compared using a common cover image, i.e., Lena, and the same secret message. The comparison is made using HC, PSNR, and SSIM. The results obtained are listed in Table I.

TABLE I
COMPARATIVE ANALYSIS OF THE STATE-OF-THE-ART WITH THE KED-DH

Technique	HC (bpp)	PSNR (dB)	SSIM
Macq and Dewey	0.0325	48.45	0.9891
[21]	0.0038	52.46	0.9981
[22]	0.2630	48.7501	0.9754
[23]	0.36	39.05	0.9914
[24]	0.0156	30.00	0.8661
[8]	0.33	46.22	0.8770
[18]	0.0310	42.95	0.9975
[19]	0.60	39.58	0.9975
KED-DH	0.44	43.20	0.9999

The results are in Table I, demonstrate that the HC and SSIM of the KED-DH technique are higher than all other techniques, while the PSNR is comparable with or higher than the other techniques listed in Table I.

V. CONCLUSIONS

KED-DH technique hides secret information in the complex region of a cover image, detected with the Kirsch edge detector. The Kirsch edge detector has the capability of detecting complex regions more realistically. The important factor is τ, which can control the HC, PSNR, and SSIM. KED-DH algorithm has the

flexibility of controlling the mentioned parameters by varying the value of τ. The result shows that the KED-DH technique efficiently hides secret information in cover images without creating any visually detectable distortion. The technique also gives a significantly high value to the quality measuring parameters, i.e., PSNR and SSIM. The HC, PSNR, and SSIM of the KED-DH technique are higher than or comparable with the other state-of-the-art data hiding techniques.

FUNDING STATEMENT

The authors received no specific funding for this study.

CONFLICTS OF INTEREST

The authors declare they have no conflicts of interest to report regarding the present study.

REFERENCES

[1] R. Gupta, S. Gupta, and A. Singhal, "Importance and techniques of information hiding: A review," arXiv preprint arXiv:1404.3063, 2014.

[2] J. J. Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," Journal of Computer and System Sciences, vol. 80, no. 5, pp. 973–993, 2014.

[3] S. Nooh, "Combining encryption and preservation in information security to secure sending a message," International Journal of Computer Science & Network Security, vol. 22, no. 4, pp. 285–291, 2022.

[4] S. Singh and K. H. Jung, "Special issue on emerging technologies for information hiding and forensics in multimedia systems," Multimedia Tools and Applications, pp. 1–8, 2022.

[5] S. Khan, M. Ismail, T. Khan, and N. Ahmad, "Enhanced stego block chaining (esbc) for low bandwidth channels," Security and Communication Networks, vol. 9, no. 18, pp. 6239–6247, 2016.

[6] M. A. Irfan, N. Ahmad, and S. Khan, "Analysis of varying least significant bits dct and spatial domain stegnography," Sindh University Research Journal-SURJ (Science Series), vol. 46, no. 3, 2014.

[7] M. Hussain, A. W. A. Wahab, Y. I. B. Idris, A. T. S. Ho, and K. H. Jung, "Image steganography in spatial domain: A survey," Signal Processing: Image Communication, vol. 65, pp. 46–66, 2018.

[8] S. Khan, N. Ahmad, M. Ismail, N. Minallah, and T. Khan, "A secure true edge based 4 least significant bits steganography," in 2015 International Conference on Emerging Technologies (ICET). IEEE, 2015, pp. 1–4.

[9] J. Chen, "A pvd-based data hiding method with histogram preserving using pixel pair matching," Signal Processing: Image Communication, vol. 29, no. 3, pp. 375–384, 2014.

[10] C. C. Lin and P. F. Shiu, "High capacity data hiding scheme for dct-based images.," J. Inf. Hiding Multim. Signal Process., vol. 1, no. 3, pp. 220–240, 2010.

[11] S. Bhattacharyya and G. Sanyal, "Data hiding in images in discrete wavelet domain using pmm," International Journal of Electrical and Computer Engineering, vol. 5, no. 6, pp. 359–367, 2010.

[12] P. Li, "Quantum implementation of the classical canny edge detector," Multimedia Tools and Applications, vol. 81, no. 8, pp. 11665–11694, 2022.

[13] R. Joshi, M. A. Zaman, and S. Katkoori, "Fast sobel edge detection for iot edge devices," SN Computer Science, vol. 3, no. 4, pp. 1–13, 2022.

[14] S. Balochian and H. Baloochian, "Edge detection on noisy images using prewitt operator and fractional order differentiation," Multimedia Tools and Applications, vol. 81, no. 7, pp. 9759–9770, 2022.

[15] S. Balochian and H. Baloochian, "Edge detection on noisy images using prewitt operator and fractional order differentiation," Multimedia Tools and Applications, vol. 81, no. 7, pp. 9759–9770, 2022.

[16] D. Laishram and T. Tuithung, "A novel minimal distortion-based edge adaptive image steganography scheme using local complexity," Multimedia Tools and Applications, vol. 80, no. 1, pp. 831–854, 2021.

[17] S. Islam, M. R. Modi, and P. Gupta, "Edge-based image steganography," EURASIP Journal on Information Security, vol. 2014, no. 1, pp. 1–14, 2014.

[18] S. Khan and T. Bianchi, "Ant colony optimization (aco) based data hiding in image complex region," International Journal of Electrical and Computer Engineering (IJECE), vol. 8, no. 1, pp. 379–389, 2018.

[19] S. K. Ghosal, A. Chatterjee, and R. Sarkar, "Image steganography based on kirsch edge detection," Multimedia Systems, vol. 27, no. 1, pp. 73–87, 2021.

[20] B. Macq and F. Dewey, "Trusted headers for medical images," in DFG VIII-D II Watermarking Workshop. Citeseer, 1999, vol. 10.

[21] Y. C. Lin and T. S. Li, "Reversible image data hiding using quad-tree segmentation and histogram shifting.," Journal of multimedia, vol. 6, no. 4, pp. 349–358, 2011.

[22] S. P. Jaiswal, O. Au, V. Jakhetiya, A. Y. Guo, and A. K. Tiwari, "Adaptive predictor structure based interpolation for reversible data hiding," in International Workshop on Digital Watermarking. Springer, 2014, pp. 276–288.

[23] M. Goljan, J. J. Fridrich, and R. Du, "Distortion-free data embedding for images," in International Workshop on Information Hiding. Springer, 2001, pp. 27–41.

[24] C. D. Vleeschouwer, J. E. Delaigle, and B. Macq, "Circular interpretation of histogram for reversible watermarking," in 2001 IEEE Fourth Workshop on Multimedia Signal Processing. IEEE, 2001, pp. 345–350.