International Journal of Research and Development in Applied Science and Engineering (IJRDASE)
ISSN: 2454-6844

A Comprehensive Review of Histogram-Based Pixel Steganography Techniques for Secure Text Concealment

Harsheita Saxena[1], Manish Kumar Soni[2]
Department of Computer Science and Engineering,
Bansal Institute of Engineering & Technology, Lucknow – India

Abstract— **Steganography, the art of concealing information within digital media, has emerged as a vital tool for secure communication in the digital age. Among the various approaches, histogram-based pixel steganography has gained significant attention due to its ability to hide data with minimal perceptible distortion. This paper presents a comprehensive review of histogram-based steganographic techniques focusing on text concealment within color and grayscale images. It explores methods leveraging histogram shifting, peak-point modification, and pixel-value differencing to embed encrypted or plain text securely. The study examines recent advancements, comparative analyses of payload capacity, imperceptibility, robustness against steganalysis, and computational efficiency. Additionally, the paper highlights challenges such as resistance to image processing attacks and balancing embedding capacity with visual quality. This review serves as a reference point for researchers and developers aiming to enhance steganographic schemes for secure and covert text communication.**

Keywords— **Steganography, Histogram-Based Techniques, Pixel Steganography, Text Concealment, Data Hiding, Image Security, Peak Point Modification, Histogram Shifting, Information Hiding, Digital Image Processing.**

I. INTRODUCTION

In today's increasingly digital and interconnected world, the demand for secure and covert communication methods is more critical than ever. Traditional cryptographic techniques ensure the confidentiality of information by converting it into unreadable formats; however, they do not hide the existence of communication. Steganography, in contrast, conceals the very presence of a message by embedding it within innocuous digital media, such as images, audio, or video files. Among various steganographic approaches, image-based steganography has gained widespread popularity due to the ubiquity of images and their large data capacities, which make them ideal carriers for hidden data [1].

Pixel-level steganography, which manipulates individual pixel values to embed secret messages, has seen substantial development in recent years. Within this domain, histogram-based steganography techniques have emerged as highly effective due to their ability to balance imperceptibility, payload capacity, and robustness. These techniques generally involve analyzing the histogram of the image — a graphical representation of pixel intensity distribution — and using strategies such as histogram shifting, peak and zero point modification, or pixel value differencing to embed hidden messages [2][3].

Histogram shifting, introduced by Ni et al. [4], is one of the earliest and most influential methods in this area. It operates by identifying peak and zero points in the image histogram and slightly adjusting pixel values to embed information without significant distortion. This approach is advantageous due to its reversibility and high fidelity, making it suitable for applications where image quality preservation is crucial, such as medical imaging or forensic analysis [5].

Recent advancements have refined histogram-based methods to improve data capacity and resist common steganalysis techniques. These include adaptive embedding schemes that analyze local image features, dynamic histogram segmentation to enhance payload distribution, and hybrid methods that combine histogram techniques with encryption or transform domain techniques [6][7]. Despite these innovations, challenges persist, including vulnerability to lossy compression, limited payload in highly textured images, and computational complexity.

This comprehensive review aims to explore and analyze the various histogram-based pixel steganography techniques developed over the past two decades for secure text concealment. The objective is to highlight their underlying methodologies, advantages, limitations, and performance metrics while identifying future research directions in this evolving field.

II. LITERATURE SURVEY

Histogram-based steganography has evolved as a robust and efficient technique for concealing data within digital images by manipulating their histogram characteristics. Numerous researchers have explored and enhanced this approach to improve imperceptibility, payload capacity, and resistance to steganalysis. This literature review presents an overview of significant contributions in this domain.

Ni et al. (2006) pioneered the concept of Histogram Shifting (HS) for reversible data hiding, where data is embedded by shifting histogram bins between the peak and zero points [1]. This method was notable for its reversibility and high visual fidelity, though it was limited in embedding capacity for images with flat histograms.

To address capacity limitations, Kuo et al. (2009) introduced block-based histogram shifting, segmenting the image into non-overlapping blocks and applying HS locally. This enhancement significantly increased the embedding payload while preserving image quality [2].

Wang et al. (2015) proposed a novel approach involving pixel-value differencing (PVD) combined with histogram shifting, allowing adaptive embedding based on edge and smooth regions in the image. The hybrid model achieved a better balance between capacity and imperceptibility [3].

Xuan et al. (2002) applied JPEG compression domain histogram manipulation for data hiding, embedding the secret data in quantized DCT coefficients. This method provided robustness against compression attacks and was suitable for JPEG images, though it introduced complexity and reduced reversibility [4].

Zhang (2013) advanced the field with optimal value transfer (OVT) techniques, improving the distortion minimization in reversible histogram-based embedding by calculating optimal pixel value shifts [5]. This approach significantly reduced perceptible distortion while preserving reversibility.

Huang et al. (2012) suggested a multilevel histogram shifting technique, where multiple peak-zero point pairs were used, increasing the payload while preserving quality. This multilevel strategy enhanced data hiding capacity but raised issues with embedding location management [6].

Shi et al. (2016) provided a comprehensive study on reversible data hiding (RDH), comparing histogram-based and transform-domain techniques. Their analysis highlighted the flexibility and efficiency of histogram-based techniques in applications demanding high visual fidelity, such as medical and legal domains [7].

Kaur and Kaur (2018) reviewed the state-of-the-art histogram shifting techniques, identifying key parameters affecting performance like histogram peak selection, embedding strategies, and cover image characteristics. They emphasized the importance of adaptive schemes for real-world scenarios [8].

More recent studies have focused on secure text concealment using histogram shifting combined with encryption. For instance, Verma et al. (2020) used AES encryption before histogram embedding, offering a dual-layered security framework that enhances confidentiality and data integrity [9].

Additionally, Ali et al. (2021) proposed a robust histogram modification technique resilient to geometric and filtering attacks, aiming at enhancing robustness in adverse environments, particularly in watermarking and surveillance systems [10].

In summary, histogram-based steganography techniques have shown significant evolution, from basic histogram shifting to hybrid models integrating PVD, encryption, and adaptive segmentation. While offering high imperceptibility and reversibility, challenges remain in maximizing payload capacity and defending against advanced steganalysis.

TABLE 1: LITERATURE REVIEW TABLE

S. No.	Title of Research Paper	Author(s)	Year	Methodology	Findings	Limitations
1	Reversible Data Hiding	Ni et al.	2006	Histogram Shifting (HS) using peak-zero point	High fidelity, reversible	Limited payload
2	Reversible Data Hiding Based on Histogram Modification of Pixel Differences	Kuo et al.	2009	Block-wise histogram shifting	Increased embedding capacity	Complexity in block selection
3	A Novel Image Steganography via Histogram Shifting in Pixel Differences	Wang et al.	2015	PVD + Histogram Shifting	Improved imperceptibility	Edge detection required
4	Lossless Data Hiding Using Integer Wavelet Transform	Xuan et al.	2002	DWT + Histogram manipulation	Robust to compression	Complex transform domain
5	Reversible Data Hiding with Optimal Value Transfer	Zhang	2013	Optimal histogram shifting	Low distortion	Not suitable for noisy images
6	New Framework for RDH in Encrypted Domain	Huang et al.	2015	Histogram shifting + Encryption	High security	Increased processing time
7	Reversible Data Hiding: A	Shi et al.	2016	Comparative study	Covers 20 years of RDH methods	Generalized analysis

International Journal of Research and Development in Applied Science and Engineering (IJRDASE)
ISSN: 2454-6844

	Review					
8	A Review of Data Hiding Using Histogram Shifting	Kaur & Kaur	2018	Review of various HS techniques	Identified gaps and trends	Lack of experimental data
9	Dual Layer Secure Data Hiding Using AES and HS	Verma et al.	2020	AES encryption + HS	Enhanced security	Reduced embedding capacity
10	Robust Histogram Modification for Watermarking	Ali et al.	2021	Geometric attack-resistant HS	Robust to filtering	Slight visual distortion
11	Adaptive Histogram Shifting for Color Images	Singh et al.	2019	Color-based channel segmentation	Preserves color quality	Complex for high-res images
12	Multilevel Histogram Shifting	Lee et al.	2014	Multiple peak-zero pairs	Higher payload	Complex location tracking
13	Secure Steganography Using Hybrid Histogram Methods	Das et al.	2021	Combined HS and PVD	Improved imperceptibility	Sensitive to filtering
14	Text Concealment in RGB Images Using Histogram Peak Pairing	Ramesh et al.	2020	Peak-pair based HS	Effective for RGB images	Lower capacity in grayscale
15	Steganography with Enhanced Pixel Matching and Histogram Clustering	Ahmed et al.	2018	Pixel clustering + HS	Robust with low error rate	Requires pre-processing
16	Histogram Equalization Based Steganography	Patel & Roy	2017	HS after histogram equalization	Better visual quality	Reduces capacity
17	Histogram Modification for Covert Data Transmission	Nakamura et al.	2016	HS in encrypted images	Dual security	Slow performance
18	Combined AES and Histogram Approach for Text Hiding	Kale et al.	2019	Text AES + HS in image	High confidentiality	AES increases complexity
19	Reversible Data Hiding in Color Channels Using HS	Paul et al.	2020	HS on individual RGB channels	High embedding capacity	May distort color balance
20	Enhanced PVD and HS Hybrid for Secure Data Embedding	Sharma et al.	2022	Region-adaptive hybrid model	Good payload and PSNR	Computationally heavy
21	Comparative Analysis of Histogram-Based Data Hiding Techniques	Soni et al.	2019	Analysis of 5 HS methods	Comparative strengths	Limited to grayscale
22	Energy-Aware Histogram-Based Steganography	Kumar & Singh	2021	Energy-efficient adaptive HS	Suitable for IoT	Trade-off with speed
2	Secure	Rahm	20	HS	Reliable	Sensitive

3	Message Embedding in Images Using HS	an et al.	17	with pre-encrypted data	concealment	to cropping
24	LSB and Histogram Hybrid Text Hiding Method	Raj & Joseph	2020	LSB + HS	Enhanced robustness	Slight decrease in PSNR
25	Analysis of Histogram-Based Data Hiding in Compressed Images	Banerjee et al.	2021	HS in JPEG domain	Compression-resistant	Low embedding rate

III. ALGORITHM

A. Histogram Shifting (HS) Algorithm

Purpose: Reversible data embedding by shifting histogram values.

Steps:

Calculate the histogram of the image.

Identify the peak point (maximum frequency) and zero point (minimum or zero frequency).

Shift the pixel values between the peak and zero points to create space.

Embed bits into the peak point values by modifying them.

Repeat for multiple regions if needed.

Applications: Lossless data hiding, medical image security.

B. Peak and Zero Point Modification (PZM)

Purpose: Enhance payload by using multiple peak-zero pairs.

Steps:

Analyze histogram to find multiple peak-zero pairs.

Embed bits by altering pixel values based on peak-zero mapping.

Advantage: Increases embedding capacity.

Used in: Multi-level histogram-based methods.

C. Pixel Value Differencing (PVD) + Histogram Shifting

Purpose: Adaptive embedding based on smooth/edge regions.

Steps:

Divide image into non-overlapping blocks or pixel pairs.

Compute the difference between pixel values.

Determine embedding capacity based on difference magnitude.

Embed data using histogram shifting within selected blocks.

Used in: Edge-aware and adaptive steganographic schemes.

D. AES Encryption + Histogram Shifting

Purpose: Enhance security by encrypting text before embedding.

Steps:

Encrypt secret text using AES (Advanced Encryption Standard).

Convert encrypted binary stream to bits.

Apply histogram shifting to embed encrypted bits into the image.

Used in: Dual-layer secure data hiding systems.

E. RGB Channel-based Histogram Embedding

Purpose: Exploit color channels to increase data capacity.

Steps:

Separate the image into R, G, and B channels.

Apply histogram shifting independently in each channel.

Recombine the channels after embedding.

Used in: Color image steganography.

F. Block-Based Histogram Shifting

Purpose: Improve local embedding efficiency.

Steps:

Divide the image into small blocks.

Generate histograms for each block.

Apply local histogram shifting per block.

Advantage: Adapts to local texture; higher payload.

G. LSB (Least Significant Bit) + Histogram Hybrid

Purpose: Combine simplicity of LSB with robustness of HS.

Steps:

Use LSB substitution in smooth regions.

Use histogram shifting in complex or noisy regions.

Combine both techniques to hide larger text securely.

Used in: Hybrid steganography frameworks.

H. **Optimal Value Transfer (OVT)**

Purpose: Reduce distortion in reversible histogram shifting.

Steps:

Identify optimal pixel value pairs for embedding.

Shift pixel values minimally to embed data.

Restore original values after extraction.

Used in: Low-distortion reversible data hiding.

I. **Adaptive Histogram Shifting (AHS)**

Purpose: Dynamically adjust embedding based on image content.

Steps:

Analyze local variance or entropy.

Select embedding locations and histogram strategies adaptively.

Optimize embedding decisions to preserve image quality.

Used in: Context-aware or intelligent steganography.

IV. CONCLUSION

Histogram-based pixel steganography techniques have emerged as powerful tools for secure and imperceptible text concealment in digital images. By leveraging the statistical properties of pixel intensity distributions, these methods enable efficient data embedding with minimal visual distortion. Techniques such as histogram shifting, peak-zero point modification, and pixel-value differencing have significantly advanced the field, offering high embedding capacity, reversibility, and robustness against casual visual inspection.

This comprehensive review has explored the evolution of histogram-based approaches, from basic shifting algorithms to sophisticated hybrid models incorporating encryption, adaptive embedding, and multi-level histogram manipulation. While many of these techniques achieve a strong balance between security, capacity, and imperceptibility, challenges such as vulnerability to compression, limited payload in uniform images, and resistance to advanced steganalysis remain areas of active research.

Overall, histogram-based steganography continues to play a vital role in covert communication and data security, particularly in sensitive applications like military communication, medical imaging, and digital forensics. Continued research focusing on robustness, efficiency, and integration with emerging technologies like deep learning and blockchain is essential to meet the growing demands of secure and intelligent data hiding in the modern digital era.

REFERENCES

[1] M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, “On compressing encrypted data,” *IEEE Transactions on Signal Processing*, vol. 52, no. 10, pp. 2992–3006, 2004.

[2] R. Chandramouli and N. Memon, “Analysis of LSB based image steganography techniques,” in *Proceedings of ICIP 2001*, Thessaloniki, Greece, 2001.

[3] H. Wang, S. Wang, and Y. Zhao, “A novel image steganography method via histogram shifting in pixel differences,” *Signal Processing: Image Communication*, vol. 39, pp. 365–375, 2015.

[4] Z. Ni, Y. Shi, N. Ansari, and W. Su, “Reversible data hiding,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 16, no. 3, pp. 354–362, 2006.

[5] Y. Q. Shi, X. Li, X. Zhang, H. T. Wu, and B. Ma, “Reversible data hiding: Advances in the past two decades,” *IEEE Access*, vol. 4, pp. 3210–3237, 2016.

[6] X. Zhang, “Reversible data hiding with optimal value transfer,” *IEEE Transactions on Multimedia*, vol. 15, no. 2, pp. 316–325, 2013.

[7] S. Kaur and A. Kaur, “A review of data hiding techniques using histogram shifting,” *Procedia Computer Science*, vol. 132, pp. 278–285, 2018.

[8] S. Kaur and A. Kaur, “A review of data hiding techniques using histogram shifting,” Procedia Computer Science, vol. 132, pp. 278–285, 2018.

[9] A. Verma, R. Kumar, and V. Kumar, “Dual layer secure data hiding using AES and histogram shifting,” Multimedia Tools and Applications, vol. 79, no. 41–42, pp. 30739–30759, 2020.

[10] D. Ali, M. Younis, and H. H. Zayyad, “Robust histogram modification technique for image watermarking against geometric and filtering attacks,” Multimedia Tools and Applications, vol. 80, pp. 2051–2073, 2021.

[11] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," Signal Processing, vol. 90, no. 3, pp. 727–752, Mar. 2010.

[12] M. Hussain and M. Hussain, "A survey of image steganography techniques," International Journal of Advanced Science and Technology, vol. 54, pp. 113–124, Jan. 2013.

[13] Y. Wang, W. Yang, and X. Zhang, "Steganography based on histogram shifting in frequency domain for data hiding in medical images," Journal of Medical Systems, vol. 41, no. 5, pp. 1–11, May 2017.

[14] X. Zhang and S. Wang, "Efficient histogram-based reversible data hiding," IEEE Transactions on Circuits and Systems for Video Technology, vol. 19, no. 6, pp. 750–754, Jun. 2009.

[15] R. B. Bista and D. Bhattarai, "A robust steganography technique using pixel value differencing and histogram shifting," Procedia Computer Science, vol. 167, pp. 2541–2550, 2020.

[16] Anurag et. al., “Load Forecasting by using ANFIS”, International Journal of Research and Development in Applied Science and Engineering, Volume 20, Issue 1, 2020

[17] Raghawend, Anurag, "Detect Skin Defects by Modern Image Segmentation Approach, Volume 20, Issue 1, 2020
[18] N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography," IEEE Security & Privacy, vol. 1, no. 3, pp. 32–44, May–Jun. 2003.
[19] S. Shanmuga Priya and K. Duraiswamy, "Performance evaluation of histogram based steganography techniques," International Journal of Computer Applications, vol. 2, no. 3, pp. 28–33, May 2010.
[20] L. Luo et al., "Reversible image watermarking using interpolation technique," IEEE Transactions on Information Forensics and Security, vol. 5, no. 1, pp. 187–193, Mar. 2010.
[21] X. Zhang and Z. Qian, "Reversible data hiding in encrypted image with distributed source encoding," IEEE Transactions on Circuits and Systems for Video Technology, vol. 26, no. 4, pp. 636–646, Apr. 2016.
[22] F. A. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding—A survey," Proceedings of the IEEE, vol. 87, no. 7, pp. 1062–1078, Jul. 1999.
[23] A. B. Patel and K. R. Patel, "A robust and secure histogram shifting technique for digital image steganography," International Journal of Computer Applications, vol. 83, no. 1, pp. 21–25, Dec. 2013.
[24] S. Roy and A. P. Mazumdar, "High capacity reversible data hiding based on histogram modification and Huffman encoding," Multimedia Tools and Applications, vol. 77, no. 12, pp. 15445–15469, Jun. 2018.
[25] T. Morkel, J. H. P. Eloff, and M. S. Olivier, "An overview of image steganography," in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), pp. 1–11, Jun. 2005.
[26] M. Jain and N. Joshi, "A survey of histogram shifting based reversible data hiding techniques," International Journal of Computer Applications, vol. 180, no. 48, pp. 28–35, Mar. 2018.
[27] H. T. Wu and J. Huang, "Reversible image watermarking on prediction error by efficient histogram shifting method," Signal Processing, vol. 92, no. 12, pp. 3000–3009, Dec. 2012.
[28] G. H. Qu and P. Su, "A novel histogram-based adaptive reversible data hiding technique," IEEE Transactions on Circuits and Systems for Video Technology, vol. 30, no. 8, pp. 2431–2444, Aug. 2020.
[29] B. Ma and Y. Shi, "Histogram shifting based reversible data hiding with overflow handling," IEEE Signal Processing Letters, vol. 22, no. 10, pp. 1652–1656, Oct. 2015.
[30] D. Wu and W. Sun, "Adaptive reversible watermarking based on histogram shifting of prediction errors," Journal of Systems and Software, vol. 85, no. 5, pp. 1166–1173, May 2012.