International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 8, Issue 1, pp 45-54, January-2024

https://doi.org/10.47001/IRJIET/2024.801006

An In-Depth Analysis of Steganography Techniques: From Classical Edge Detection to Adaptive Approaches

[1]Noor Gh. Abdullah, [2]Shahd A. Hasso

[1,2]Software Department, College of Computer Science and Mathematics, University of Mosul, Mosul – Iraq

***Abstract* - This paper delves into the realm of steganography, focusing on the evolution of techniques employed to conceal data within digital images. Beginning with an exploration of the motivations behind information security and the role of cryptography, the paper introduces adaptive steganography as a discreet means of incorporating private data into a cover medium. The discussion then shifts to the three key factors in image steganography - resilience, capacity, and imperceptibility - forming the foundation of effective data hiding. The spatial and frequency domain methods are compared, with specific emphasis on the classical Least Significant Bit insertion and more advanced adaptive steganography techniques. The paper further introduces edge-based steganography, highlighting the advantage of manipulating edge areas for increased imperceptibility. Moving beyond definitions and types, the paper provides a comprehensive analysis of notable research works in the field, elucidating their objectives, methodologies, results, strengths, and limitations. The conclusion reflects on the dynamic landscape of steganography, acknowledging both achievements and areas for improvement.**

Keywords: Steganography, Adaptive Steganography, Image Encryption, Edge-based Steganography, Data Hiding, Spatial Domain, Frequency Domain, Capacity, Imperceptibility, Resilience.

I. INTRODUCTION

Any organization's first priority is information protection, which is why information security has been the subject of much research. Historically, the preferred technique for guaranteeing dependable and secure communication has been cryptography. On the other hand, malevolent attackers may be suspicious of encrypted data. Adaptive steganography [1]. has therefore been proposed as a way to solve this issue by discreetly incorporating private data into a cover medium without drawing undue attention from adversaries. Steganography is distinguished from cryptography by its concealing characteristic, which makes sure that the hidden data is invisible to eavesdroppers. Steganography techniques have multiple applications such as digital signatures, fingerprinting, access control systems, and covert communication [2]. Their ultimate goal is to preserve data privacy and prevent unauthorized duplication of intellectual property[3].

The three main factors for image steganography methods are resilience, capacity, and imperceptibility. These factors together make up the "magic triangle" that Johnson et al. [4] postulated. Peak signal-to-noise ratio (PSNR) is used to measure imperceptibility; robustness indicates protection against manipulation or eavesdropping; and capacity refers to the amount of data hidden in the cover image. The two primary kinds of picture encryption methods are spatial domain and frequency domain. Secret information is directly added to the intensity of the image pixels in the spatial domain, as opposed to cover pictures, which are altered in the frequency domain and have secret data embedded in the transform coefficients [5].

Least Significant Bit insertion [6] is a traditional spatial domain approach that offers a high payload and minimal processing complexity but is not resistant to statistical attacks. Techniques in the transform domain, including the Discrete Cosine Transform (DCT) [6] and Wavelet Transform (DWT) [7], are made to be more resilient to eavesdropper manipulation and attacks. One notable example of a hybrid technique is adaptive steganography [8], often referred to as "Statistics-aware embedding," "Masking," or "Model-Based embedding." Using statistical global properties of the cover picture, this method finds the best places to incorporate LSB/DCT coefficients. It uses an adaptive random selection of pixels, frequently omitting smooth or homogeneous colour regions. Interestingly, using edge regions to hide the secret message improves the stego image's visual appeal. When information is buried in edge locations, stego pictures are highly imperceptible because human visual systems are less sensitive to alterations in edge sites than in smooth areas[9].

II. STEGANOGRAPHY DEFINITION AND TYPES AND APPLICATIONS

Steganography is the term for the technique of secret communication between a source and a destination. It comes from the Greek terms "stegos," which means covered, and "grafia," which means writing. Steganography's main goal is to covertly insert confidential data into a carrier media such that it seems to be the original medium[10]. In the past,

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 8, Issue 1, pp 45-54, January-2024

https://doi.org/10.47001/IRJIET/2024.801006

steganography methods involved the use of razor heads, wax tablets, and invisible ink. Secret messages were written on wood and covered with wax in the instance of wax tablets. Messages were written with invisible ink, which only showed up when the paper heated up[11]. Sometimes masters would write messages in code on the scalps of their slaves, which they would then mail to the designated recipients as the captives' hair came back. When the slave reached its destination, the receiver would shave him or her to reveal the secret message[12].

Germany invented the Microdot technology during World War II, which involves embedding photographic data into a cover image at a size no larger than a written period. The Prisoner's dilemma serves as an example of the basic idea of steganography. Knowing the warden is keeping an eye out for such activity, two prisoners who are preparing an escape speak to each other in secret[3].

They conceal their signals inside other objects that appear harmless in order to avoid being discovered. Stego picture, cover image, secure message, and stego analysis are some of the key words used in steganography. The carrier carrying the concealed message is called the cover picture; the embedded secret message is called the stego image; and the information meant to remain private is called the secure message[3].

Steganography encompasses various types, each contingent on the chosen carrier medium. Optimal choices often revolve around carrier mediums with high redundancy. Several commonly utilized mediums include as shown in Figure (1)[13]:

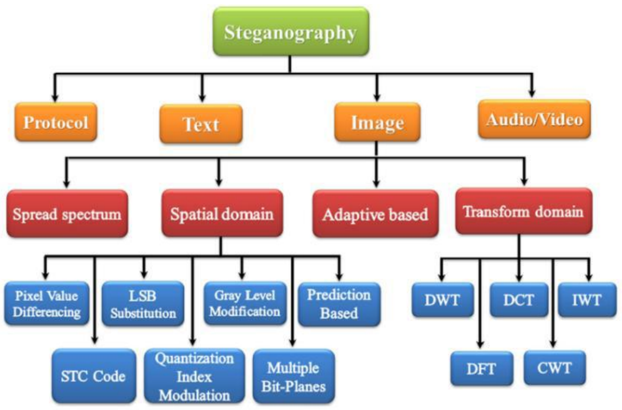

Figure 1: Steganography According to Medium [14]

Steganography is a method of concealing data for various purposes, primarily to prevent unauthorized access or awareness of a message. It finds applications in radio monitoring, automatic systems for detecting specific stego messages, and modern technologies like web hosting for secret information transfer. Medical imaging systems use steganography to maintain confidentiality in patient data. Fujitsu is developing technology to encode invisible data in printed pictures for quick retrieval by mobile phones. Other applications include intelligence services, protecting trade secrets, government limitations due to criminal use concerns, military communication, and corporate espionage. Steganography is employed in both business and non-commercial sectors to hide sensitive information[14].

Table (1) provides a comprehensive overview of various steganography types, elucidating their distinct characteristics, techniques employed, applicable file formats, and inherent challenges. Steganography, the art of covert communication, manifests through diverse forms such as Image Steganography, where data is concealed within pixel intensities of digital images. Video Steganography extends this concept to multimedia files, utilizing techniques from both image and audio steganography. Text Steganography involves hiding information within text files using formatting elements like tabs and capital letters.Protocol Steganography ventures into the realm of network protocols, embedding covert data within headers and trailers of network packets. Audio Steganography manipulates digital sound, embedding information through binary sequence modifications. DNA Steganography, a unique frontier, explores embedding data within DNA sequences, leveraging their chaotic nature and numerical mapping tables.

Each steganography type poses specific challenges, ranging from the limited capacity of text files to the potential perceptual distortions in audio steganography. The table aims to facilitate a comparative understanding of these steganography types, aiding users in selecting the most suitable method based on their requirements and considerations.

III. EDGE BASED STEGANOGRAPHY

Edge-based Steganography makes use of the fact those changes in edge areas are harder for the human visual system to notice, which helps it stay hidden. When manipulating edge regions, there is an advantage over smoother sections inside an image: more secret bits can be accommodated[20]. Edges are essential for interpreting images because they separate the image from its background and define surrounding elements. They offer the area, perimeter, and shape of the image, among other crucial details. One of the core functions of image processing is edge detection, which is the identification of distinct variations in intensity between neighboring pixels[21]. We refer to the location of such discontinuity as an edge. Many methods are used for edge detection and are categorized into different groups in the field of image processing as shown in Figure (2) [6].

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 8, Issue 1, pp 45-54, January-2024

https://doi.org/10.47001/IRJIET/2024.801006

Table 1: Techniques, File Formats, and Challenges

Steganography Type	Description	Techniques	File Formats	Challenges and Considerations
Image Steganography [15]	Covert information is embedded within digital images using pixel intensities. The algorithm, with a secret key, produces a stego image.	Pixel intensities manipulation	JPEG, PNG, BMP, etc.	Limited to the capacity of image space; susceptibility to certain attacks; requires careful selection of embedding locations to avoid detection.
Video Steganography [13]	Concealing covert information in video files (H.264, Mp4, MPEG, AVI). Utilizes techniques from image and audio steganography due to the multimedia nature of videos .	Techniques from image and audio steganography; manipulation of video frames and audio tracks	H.264, Mp4, MPEG, AVI, etc.	Exploits the vast space in video formats; potential for blending into the continuous stream of information; may require synchronization between video and audio data; detection challenges due to diverse formats.
Text Steganography [16]	Using capital letters, tabs, and white spaces to hide information inside a text document.	Format manipulation using tabs, capital letters, and white spaces	Text files	Limited to text size; potential redundancy in text data; not widely used due to limited capacity and redundancy.
Protocol Steganography [17]	Embedding covert information in network protocols (IP, TCP, ICMP, UDP) within network packet headers and trailers.	Data manipulation within network protocols; utilization of protocol layers	IP, TCP, ICMP, UDP, etc.	Requires in-depth knowledge of network protocols; may impact network performance; potential for detection in sophisticated network analysis.
Audio Steganography [18]	Embedding covert information in digital sound (WAV, AU, MP3) by modifying binary sequences.	Binary sequence modification; signal noise introduction; algorithmic methods	WAV, AU, MP3, etc.	Challenges in embedding due to sequential arrangement of binary in sound; diverse techniques from simple to advanced; potential perceptual distortions.
DNA Steganography [19]	Embedding covert information in DNA sequences, utilizing the chaotic nature of DNA. Numerical mapping tables are employed for enciphering.	Utilization of DNA's chaotic nature; numerical mapping tables for enciphering	DNA sequences	Limited practical applications; challenges in DNA manipulation; potential ethical considerations; advanced techniques required for effective data hiding.

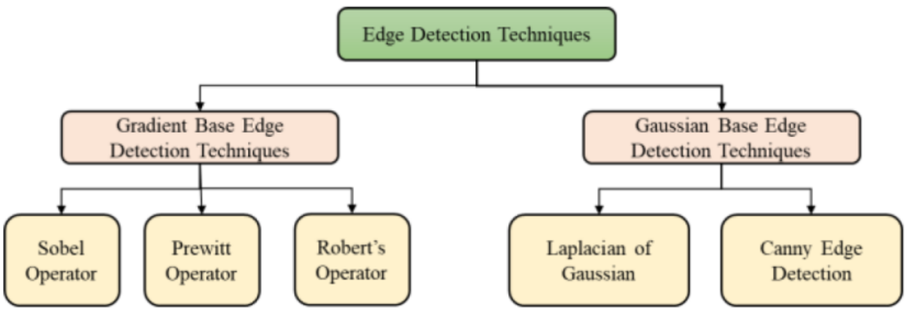

Figure 2: Classification of Edge Detection Techniques

3.1 Gradient Based Edge Detection

Gradient-based edge detection methods rely on analyzing the maxima and minima in the first derivative of an image, where the gradient is a vector indicating edge strength and direction. This process hinges on identifying changes in pixel intensities, with

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 8, Issue 1, pp 45-54, January-2024

https://doi.org/10.47001/IRJIET/2024.801006

a set threshold determining which pixels are classified as edges. The gradient magnitude (G(x,y)) is computed as the square root of the sum of squared differences in pixel intensities $(\Delta x^2 + \Delta y^2)^{1/2}$, while the gradient direction (θ(x,y)) is determined using the tangent of the ratio of changes in y and x $(\tan(\Delta y/\Delta x))$. Notable operators for gradient estimation include the Sobel, Prewitt, and Roberts operators[21].

The Sobel operator utilizes a 3x3 mask for discrete differentiation in horizontal and vertical directions. Prewitt calculates edge magnitude and orientation using convolution with different kernels, limited to 8 orientations[22]. Roberts operator computes the 2-D spatial gradient, identifying high spatial frequency pixels as edges through specific masks for convolution in horizontal and vertical directions. The final step involves applying a threshold to the gradient magnitude, classifying pixels exceeding this threshold as edge pixels[23].

3.2 Gaussian Based Edge Detection

Gaussian-based edge detection encompasses two prominent methods: Laplacian of Gaussian (LoG) and Canny Edge Detection[24].

1. **Laplacian of Gaussian (LoG):** The Laplace method for edge detection is characterized by its utilization of the second derivative and zero crossings to identify edges. However, its sensitivity to noise necessitates the application of Laplacian of Gaussian (LoG) for refinement. In this process, the image undergoes initial smoothing through a Gaussian filter to mitigate noise effects. Subsequently, the smoothed image is subjected to Laplace application, enhancing the second derivative. The final step in edge detection entailsidentifying zero crossings in this enhanced second derivative, aligning with corresponding high peaks in the first derivative. This combined approach in LoG effectively addresses noise-related challenges in the edge detection process[25].
2. **Canny Edge Detection:**Canny edge detection employs a finite difference approximation of the partial derivative to achieve precise edge identification. The process begins with initial image smoothing facilitated by a Gaussian filter, effectively minimizing noise interference[26]. Following this, the computation of gradient magnitude and orientation is executed through partial derivatives. Subsequent stages in the Canny edge detection method encompass non-maxima suppression and the application of threshold techniques. These measures collectively refine and enhance the accuracy of edge detection, ensuring the identification of edges in a robust and effective manner[27].

IV. ANALYSIS OF STEGANOGRAPHIC TECHNIQUES IN EDGES

Table (2) provides an insightful overview of three distinct steganography schemes, each employing unique techniques to conceal information within digital images. These schemes, namely "Hiding Behind Corners," "Hiding Secret Message in Edges," and "High Payload Steganography Mechanism," utilize diverse methodologies, aiming for effective information hiding while addressing specific challenges. The table outlines key aspects of each scheme, shedding light on their strengths, weaknesses, and the underlying principles driving their implementation.

Table 2: Steganography Scheme Comparison

Scheme Introduction	Description
Hiding Behind Corners [28]	By employing the y (where y=8-x) most significant bits for edge identification, this approach makes use of the Filter First concept to choose and detect edge locations for embedding. It is successful at concealing information in picture elements like edges and seeks to ensure information retrieval without additional data. But it has flaws like vulnerability and information retrieval ease after the stego-image is recognized.
Hiding Secret Message in Edges [29]	With this approach, messages are embedded according to edges found by a Laplacian filter. It corrects the imbalance between adjacent pixels and flips grayscale values to guarantee uniformity in the D value. Its restrictions include limiting the length of the secret message and only using edge detection in non-overlapping windows, which lessens its suspicion by attackers.
High Payload Steganography Mechanism [30]	In order to enhance embedding positions, this approach uses two edge detectors on the same image and combines their results. It separates the image into raster pieces that do not overlap and prioritises large payload capacity over image quality. Nevertheless, it has disadvantages such as limiting the use of all edge pixels, altering some cover pixels for information storage, and perhaps affecting image quality because of block size changes.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 8, Issue 1, pp 45-54, January-2024

https://doi.org/10.47001/IRJIET/2024.801006

V. RELATED WORKS

Table (1) below presents a compilation of notable research papers in the field of steganography, showcasing diverse methodologies employed by researchers to achieve effective data hiding. Each entry details the objectives, methods utilized, obtained results, strengths, and limitations of the respective approaches. This comprehensive overview provides valuable insights into the evolving landscape of steganographic techniques, offering a comparative perspective on the advancements made in the field.

Table 3: Related works analysis

Researchers	Objectives	Method	Results	Strength Points	Limitations
Wu et al., 2005 [31]	Histogram analysis method	PVD method; Provide high embedding capacity	Range of PSNR around 50%, high embedding capacity	Utilizes histogram analysis to enhance embedding capacity	PSNR range around 50% might indicate potential perceptual distortions; Limited comparison metric
Hempstalk, 2006 [28]	Eliminate the need for the original cover image in Steganography	Battle Steg method combining Hide seek and Filter first	Successful Steganalysis using WEKA's Support Vector Machine	Filter first showed the best performance	Hide seek method open to Laplace magnitude count Steganalysis
Motameni et al., 2007 [32]	Pixel Value Differencing (PVD) method	Determine the concealed data bit size by dividing the cover image's consecutive pixel difference.	High embedding capacity through histogram analysis	offering higher embedding capacities	approach relies on pixel differences,
Parvez & Gutub, 2008 [33]	Enhance pixel indicator technique	Use a variable amount of bits from the RGB (chosen pixel channel); Boost the embedding capacity by using the pixel value difference approach, 2x2 block division, and LSB substitution.	Increased capacity compared to method	Enhanced scheme allows for higher embedding capacity	Selection still depends on the channel, which might limit versatility
Yang et al., 2008 [34]	Adaptive image Steganography based on LSB and pixel value difference	encrypt 16-pixel picture chunks using AES; Insert 1-bit data using a pseudo-random number generator into a randomly selected pixel	Higher PSNR and embedding rate compared to Wu et al.'s method	Improved concept over Wu and Tsai's scheme	Readjusting required if embedding changes the level of pixel value difference
Puech et al., 2008 [35]	Implement VRAE approach for reversible data hiding	Determine the concealed data bit size by dividing the cover image's consecutive pixel difference.	VRAE approach with AES encryption; Increased payloads	Implementation of AES encryption in VRAE approach; Embedding 1-bit data into randomly chosen pixels	Limited to 1-bit data embedding; Payloads may be restricted compared to RRBE approaches
Li et al., 2009 [36]	Sobel edge operator in R, G, or B channels	Edge identification based on intensity gradients; choosing insertion areas with highest intensity gradients	Payload not guaranteed to be high	Utilizes classical edge detection (Sobel)	High payload not guaranteed
Chen et al., 2010 [37]	Canny and fuzzy edge detection	Formation of edge image using Canny and fuzzy techniques; LSB substitution for data insertion	Unnecessary modifications in stego image	Combination of Canny and fuzzy edge detection	Unnecessary modifications in stego image
Gutub, 2010	Introduce pixel	Select one channel	Hidden capacity	Pixel indicator	Hidden capacity

ISSN (online): 2581-3048
Volume 8, Issue 1, pp 45-54, January-2024
https://doi.org/10.47001/IRJIET/2024.801006

[38]	indicator technique	from RGB; Modify data bits up to 2 LSB; Sequential selection criteria	depends on cover image channel bits	technique provides a level of sophistication, but its sequential selection limits the embedding capacity	depends on cover image channel bits; Sequential selection criteria
Luo et al., 2010 [39]	Edge adaptive LSB Matching Revisited	Vertical and horizontal edge identification through pixel divergence; LSB matching for insertion	Efficient edge identification	Adaptive LSB Matching Revisited technique for edge identification	May involve unnecessary modifications in the stego image
Chen et al., 2010 [37]	High payload Steganography using hybrid edge detector	Combining LSB technique with fuzzy and canny edge detection	High embedding capacity and better quality stego image	Resists statistical Steganalysis	Increased chances of Steganalysis due to image differences
Yu et al., 2011 [40]	Achieve data hiding in HDR RGBE images	Conceal messages based on homogeneous representations; Limited embedding rate in the range of 0.127–0.145 bpp	Data hiding without distortion; Limited embedding rate	Successful data hiding without distortion in HDR RGBE images; Consideration of homogeneous representations	Limited embedding rate in the range of 0.127–0.145 bpp
Liao et al., 2011 [41]	Adaptive LSB steganography based on PVD	Use of PVD and LSB replacement; Inserting more data into edge areas than smooth areas	Increased hiding capacity in edge areas	Adaptive steganographic technique based on PVD and LSB replacement	May not be optimal for all types of images
Hussain & Hussain, 2011 [42]	Focus on the difference of boundary pixels in cover and stego images	Use of canny edge detector and LSB technique	More secure with low computational overhead	Identical edges maintained through threshold updating	Edge detection and threshold updating may affect computational efficiency
Bassil, 2012 [43]	Canny edge location for embedding region	Canny edge location for choosing embedding region; LSB methods for hiding	Lack of properly recognized edge pixels	Utilizes Canny edge location for selecting embedding region; LSB methods for hiding information	May not properly recognize edge pixels
Mahajan & Kaur, 2012 [44]	Propose random pixel selection	Embed hidden bits using randomly selected pixels; Requires stego-key for hiding and recovering	Key management overhead; Synchronization or updating phase of stego-key is a concern	Random pixel selection adds a layer of security, but key management can be challenging	Key management overhead; Synchronization challenges for stego-key
Hussain, 2013 [45]	Introduce dark area-based data hiding	Identify dark areas, use LSB to embed in binary image; Label objects with 8-pixel connectivity schemes	Increased embedding capacity in dark areas	Utilizes dark areas to hide data, increasing capacity; Incorporates connectivity schemes for enhanced hiding	May alter the visual perception of dark areas; Connectivity schemes may limit applicability
Nagaraj et al., 2013 [46]	Improved PVD method with modulus function	Embedding based on the reminder of consecutive pixels	Better performance than Wu and Tsai's and Chang and Tseng's schemes	Higher PSNR ratio and improved edge distortion	Robust against RS detection attack
Yan et al., 2013 [47]	Apply elementary cellular automata to encrypt HDR images	Encrypt HDR RGBE images using elementary cellular automata	Encryption using elementary cellular automata	Application of elementary cellular automata for HDR image encryption	Specific to HDR RGBE images; May require additional analysis for generalizability
Ma et al., 2013 [48]	Implement RRBE approach for reversible data hiding	Reserve room by histogram shifting before encryption; Significantly increase payloads	RRBE approach with histogram shifting; Increased payloads	RRBE approach allows for higher payloads by reserving room before encryption	Histogram shifting may introduce perceptual distortions; Payload increase may not be uniform across all images

ISSN (online): 2581-3048
Volume 8, Issue 1, pp 45-54, January-2024
https://doi.org/10.47001/IRJIET/2024.801006

Singla & Juneja, 2014 [49]	Adaptive and secure steganographic algorithm	PDHist table, Candidate table, and Takefill adjusting Algorithm	Secure against Steganalysis and histogram-based attacks	Preserves histogram with the help of PDHist table	Performance compared with previously PVD-based methods
Al-Dmour & Al-Ani, 2015 [50]	Edge detection and XOR coding	Image steganography based on edge detection and XOR coding	Message hiding in spatial or transform domain	Novel technique using edge detection and XOR coding	Effectiveness may vary depending on the image content and coding approach
Lin et al., 2017 [51]	Conceal messages based on pixel luminance	Partition pixels based on luminance; Select low luminance pixels for greater message concealment; Embedding rates of 2.433 to 20.002 bpp	Greater message concealment with low luminance pixels	Partitioning based on luminance allows for effective message concealment; Offers a wide range of embedding rates	Specific parameters may impact results; Larger embedding rates may increase the risk of steganalytic attacks
Puteaux & Puech, 2018 [52]	Utilize error prediction and LOCO-I in JPEG-LS for RRAE	Achieve average embedding rate of 2.46 bpp	Error prediction and LOCO-I in JPEG-LS for RRAE	Successful use of error prediction and LOCO-I for RRAE approach; Achieving average embedding rate	Limited to JPEG-LS compression standard; May not be applicable to other compression methods
Gao et al., 2020 [53]	Decrease distortion in data hiding	Utilize a two-dimensional prediction-error histogram; Provide embedding rates between 1.202 and 2.85 bpp	Decreased distortion; Variable embedding rates	Two-dimensional prediction-error histogram to decrease distortion; Offers variable embedding rates	Limited to the specified embedding rates; Distortion reduction may still be perceptible
Lan et al., 2022 [54]	Carry secret message in RGBE images	Adaptive method considering exponent channel distribution; Embedding rates from 7.30 to 9.29 bpp	Retains exponent channel during message concealment	Adaptive method considers exponent channel distribution; Wide range of embedding rates	Dependent on specific parameters; Higher embedding rates may lead to perceptual distortions
Wang et al., 2022 [55]	Employ block-level approach for reversible data hiding	Achieve a maximum embedding rate of 2.5 bpp	Block-level approach for reversible data hiding	Block-level approach allows for a high maximum embedding rate; Provides flexibility in payload selection	Maximum embedding rate may not be achievable in all scenarios; Limited security evaluation
Tsai et al., 2022 [56]	Employ random binary digits to encrypt images	Encryption using random binary digits	Secure encryption using random binary digits	Utilization of random binary digits for image encryption	May not provide advanced cryptographic features; Security evaluation may depend on encryption algorithm used
Hsieh & Wang, 2023 [57]	Evaluate EC-MV steganalysis using WCTCIS algorithm	Use constructive image steganography (CIS) approach; Resist steganalysis attack; Linear ROC curve with AUC around 0.50	Resistance to steganalysis; Linear ROC curve	Constructive image steganography resists steganalysis attacks; Linear ROC curve indicates resilience to detection	AUC around 0.50 may limit robustness against some steganalytic attacks; Effectiveness may vary with different datasets

The analysis of the presented steganography research works reveals a dynamic landscape of methodologies employed to address the complexities of data hiding within digital images. Researchers, spanning from Wu et al. in 2005 to more recent contributions by Wang et al. and Hsieh & Wang, have explored a wide array of techniques such as histogram analysis, adaptive image steganography, and block-level approaches. Noteworthy strengths include increased embedding capacity, resistance to steganalysis, and distortion reduction. However, limitations, such as potential perceptual distortions, susceptibility to specific steganalysis methods, and challenges in key management or synchronization, highlight areas for improvement. The progression from classical edge detection methods to the integration of advanced encryption and prediction-error histograms reflects an ongoing quest for innovation in achieving both robust data hiding and security. As the field continues to evolve, these analyses offer valuable

ISSN (online): 2581-3048
Volume 8, Issue 1, pp 45-54, January-2024
https://doi.org/10.47001/IRJIET/2024.801006

insights for researchers seeking to further enhance the effectiveness and versatility of steganographic techniques.

VI. CONCLUSIONS

In conclusion, this paper offers a thorough exploration of steganography techniques, tracing their evolution from classical methods to the adaptive approaches of the present. The analysis of notable research works provides a panoramic view of the field, emphasizing the strengths and limitations of diverse methodologies. While advancements have been made in terms of increased embedding capacity, resistance to steganalysis, and reduced perceptual distortions, challenges such as key management and uniform payload increase across all images persist. The shift from classical edge detection to more sophisticated techniques, incorporating encryption and prediction-error histograms, reflects the continuous quest for innovation in achieving robust data hiding and heightened security. As technology evolves, further research is encouraged to address existing limitations and propel steganography towards enhanced effectiveness and versatility.

ACKNOWLEDGEMENT

The authors would like to thank University of Mosul for Support.

REFERENCES

[1] R. D. Rashid and T. F. Majeed, "Edge based image steganography: Problems and solution," *2019 3rd Int. Conf. Commun. Signal Process. their Appl. ICCSPA 2019*, no. May, 2019, doi: 10.1109/ICCSPA.2019.8713712.

[2] R. Mohamad, "Data hiding by using AES Algorithm," *Wasit J. Comput. Math. Sci.*, vol. 1, no. 4, pp. 112–119, 2022, doi: 10.31185/wjcm.82.

[3] D. Dongre and R. Mishra, "A Review on Edge Based Image Steganography," *Int. J. Recent Innov. Trends Comput. Commun.*, vol. 2, no. 9, pp. 2862–2866, 2014.

[4] N. Johnson, Z. Duric, S. Jajodia, and N. Memon, "Information Hiding: Steganography and Watermarking—Attacks and Countermeasures," *J. Electron. Imaging*, vol. 10, p. 825, Jan. 2001, doi: 10.1117/1.1388610.

[5] H. Kolivand, T. C. Wee, S. Asadianfam, M. S. Rahim, and G. Sulong, *High imperceptibility and robustness watermarking scheme for brain MRI using Slantlet transform coupled with enhanced knight tour algorithm*, no. 0123456789. Springer US, 2023. doi: 10.1007/s11042-023-16459-7.

[6] N. Akhtar, "An LSB Substitution with Bit Inversion Steganography Method," 2016, pp. 515–521. doi: 10.1007/978-81-322-2538-6_53.

[7] D. Baby, J. Thomas, G. Augustine, E. George, and N. R. Michael, "A novel DWT based image securing method using steganography," *Procedia Comput. Sci.*, vol. 46, no. Icict 2014, pp. 612–618, 2015, doi: 10.1016/j.procs.2015.02.105.

[8] H.-D. Yuan, "Secret sharing with multi-cover adaptive steganography," *Inf. Sci. an Int. J.*, vol. 254, pp. 197–212, Jan. 2014, doi: 10.1016/j.ins.2013.08.012.

[9] 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, 2010, doi: 10.1016/j.sigpro.2009.08.010.

[10] N. Rabade and Y. S. Thakur, "Different Steganography Techniques and Stego Keys Used in Digital Image Processing-a Review," *Int. Res. J. Mod. Eng. Technol. Sci.*, no. 02, pp. 852–859, 2023.

[11] N. Hamid, A. Yahya, R. B. Ahmad, and O. M. Al-Qershi, "Image steganography techniques: an overview," *Int. J. Comput. Sci. Secur.*, vol. 6, no. 3, pp. 168–187, 2012.

[12] Shikha and V. K. Dutt, "Steganography : The Art of Hiding Text in Image using Matlab," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 4, no. 9, pp. 822–828, 2014.

[13] M. S. Abuali, C. B. M. Rashidi, M. H. Salih, R. A. A. Raof, and S. S. Hussein, "Digital image steganography in spatial domain a comprehensive review," *J. Theor. Appl. Inf. Technol.*, vol. 97, no. 19, pp. 5081–5102, 2019.

[14] M. Hassaballah, M. A. Hameed, and M. H. Alkinani, "Introduction to digital image steganography," *Digit. Media Steganography Princ. Algorithms, Adv.*, pp. 1–15, 2020, doi: 10.1016/B978-0-12-819438-6.00009-8.

[15] G. Yadav and A. Ojha, "Improved security in the genetic algorithm-based image steganography scheme using Hilbert space-filling curve," *Imaging Sci. J.*, vol. 67, pp. 1–11, Feb. 2019, doi: 10.1080/13682199.2019.1570678.

[16] R. Din *et al.*, "Evaluating the Feature-Based Technique of Text Steganography Based on Capacity and Time Processing Parameters," *Adv. Sci. Lett.*, vol. 24, pp. 7355–7359, Oct. 2018, doi: 10.1166/asl.2018.12941.

[17] S. Bobade and R. Goudar, "Secure Data Communication Using Protocol Steganography in IPv6," in *2015 International Conference on Computing Communication Control and Automation*, 2015, pp. 275–279. doi: 10.1109/ICCUBEA.2015.59.

[18] C. Han, R. Xue, R. Zhang, and X. Wang, "A new audio steganalysis method based on linear prediction," *Multimed. Tools Appl.*, vol. 77, pp. 1–25, Jun. 2018, doi: 10.1007/s11042-017-5123-x.

[19] P. Malathi, M. Manoaj, R. Manoj, V. Raghavan, and R. E. Vinodhini, "Highly Improved DNA Based Steganography," *Procedia Comput. Sci.*, vol. 115, pp. 651–659, 2017, doi: 10.1016/j.procs.2017.09.151.

[20] M. Kasthuri, "Performance analysis of gradient based image edge detection," *Int. J. Health Sci. (Qassim).*, vol. 6, no. June, pp. 2272–2278, 2022, doi: 10.53730/ijhs.v6ns5.9134.

[21] J. A. M. Saif, M. H. Hammad, and I. A. A. Alqubati, "Gradient Based Image Edge Detection," *Int. J. Eng. Technol.*, vol. 8, no. 3, pp. 153–156, 2016, doi: 10.7763/ijet.2016.v6.876.

[22] G. M. H. Amer and A. M. Abushaala, "Edge detection

ISSN (online): 2581-3048
Volume 8, Issue 1, pp 45-54, January-2024
https://doi.org/10.47001/IRJIET/2024.801006

methods," *2015 2nd World Symp. Web Appl. Networking, WSWAN 2015*, no. April, 2015, doi: 10.1109/WSWAN.2015.7210349.

[23] S. Krig, "Image Pre-Processing BT - Computer Vision Metrics: Survey, Taxonomy, and Analysis," S. Krig, Ed., Berkeley, CA: Apress, 2014, pp. 39–83. doi: 10.1007/978-1-4302-5930-5_2.

[24] S. Saluja, A. K. Singh, S. Agrawal, M. E. Scholar, I. Bhilai, and S. Asst, "A Study of Edge Detection Methods," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 2, no. 1, pp. 994–999, 2013, [Online]. Available: www.ijarcce.com

[25] A. Jan, S. A. Parah, and B. A. Malik, "A novel laplacian of gaussian (LoG) and chaotic encryption based image steganography technique," *2020 Int. Conf. Emerg. Technol. INCET 2020*, no. June, 2020, doi: 10.1109/INCET49848.2020.9154173.

[26] X. Wang and J.-Q. Jin, *An Edge Detection Algorithm Based on Improved CANNY Operator*. 2007. doi: 10.1109/ISDA.2007.6.

[27] J. Liu *et al.*, "Image Edge Recognition of Virtual Reality Scene Based on Multi-Operator Dynamic Weight Detection," *IEEE Access*, vol. 8, pp. 111289–111302, 2020, doi: 10.1109/ACCESS.2020.3001386.

[28] K. Hempstalk, "Hiding behind corners: Using edges in images for better steganography," *Researchgate.Net*, no. January 2006, 2006, [Online]. Available: https://www.researchgate.net/profile/Kathryn-Hempstalk/publication/241605558_Hiding_Behind_Corners_Using_Edges_in_Images_for_Better_Steganography/links/541fdafe0cf241a65a1acad4/Hiding-Behind-Corners-Using-Edges-in-Images-for-Better-Steganography.pdf

[29] M. R. Modi, S. Islam, and P. Gupta, "Edge Based Steganography on Colored Images BT - Intelligent Computing Theories," D.-S. Huang, V. Bevilacqua, J. C. Figueroa, and P. Premaratne, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 593–600.

[30] P. B. Chanda, S. Datta, S. Mukherjee, and J. P. Choudhury, "Comparative Study on Different Image Steganography Based Edge Detection," *Int. J. Innov. Res. Sci. Eng. Technol.*, pp. 220–226, 2016.

[31] H.-C. Wu, N.-I. Wu, C.-S. Tsai, and M.-S. Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods," *Vision, Image Signal Process. IEE Proc. -*, vol. 152, pp. 611–615, Nov. 2005, doi: 10.1049/ip-vis:20059022.

[32] H. Motameni, M. Norouzi, M. Jahandar, and A. Hatami, "Labeling Method in Steganography," *World Acad. Sci. Eng. Technol. Int. J. Comput. Electr. Autom. Control Inf. Eng.*, vol. 1, pp. 1600–1605, 2007, [Online]. Available: https://api.semanticscholar.org/CorpusID:9357037

[33] M. T. Parvez and A. A.-A. Gutub, "RGB Intensity Based Variable-Bits Image Steganography," in *2008 IEEE Asia-Pacific Services Computing Conference*, 2008, pp. 1322–1327. doi: 10.1109/APSCC.2008.105.

[34] C.-H. Yang, C.-Y. Weng, S.-J. Wang, and H.-M. Sun, "Adaptive Data Hiding in Edge Areas of Images With Spatial LSB Domain Systems," *IEEE Trans. Inf. Forensics Secur.*, vol. 3, no. 3, pp. 488–497, 2008, doi: 10.1109/TIFS.2008.926097.

[35] W. Puech, M. Chaumont, and O. Strauss, "A reversible data hiding method for encrypted images," *Secur. Forensics, Steganography, Watermarking Multimed. Contents X*, vol. 6819, no. March 2008, p. 68191E, 2008, doi: 10.1117/12.766754.

[36] L. Li, B. Luo, Q. Li, and X. Fang, "A Color Images Steganography Method by Multiple Embedding Strategy Based on Sobel Operator," in *2009 International Conference on Multimedia Information Networking and Security*, 2009, pp. 118–121. doi: 10.1109/MINES.2009.187.

[37] W.-J. Chen, C.-C. Chang, and T. Le Hoang, "High payload steganography mechanism using hybrid edge detector," *Expert Syst. Appl.*, vol. 37, pp. 3292–3301, Apr. 2010, doi: 10.1016/j.eswa.2009.09.050.

[38] A. Gutub, "Pixel Indicator Technique for RGB Image Steganography," *J. Emerg. Technol. Web Intell.*, vol. 2, Feb. 2010, doi: 10.4304/jetwi.2.1.56-64.

[39] W. Luo, F. Huang, and J. Huang, "Edge adaptive image steganography based on lsb matching revisited," *IEEE Trans. Inf. Forensics Secur.*, vol. 5, no. 2, pp. 201–214, 2010, doi: 10.1109/TIFS.2010.2041812.

[40] C.-M. Yu, K.-C. Wu, and C.-M. Wang, "A distortion-free data hiding scheme for high dynamic range images," *Displays*, vol. 32, no. 5, pp. 225–236, 2011, doi: https://doi.org/10.1016/j.displa.2011.02.004.

[41] X. Liao, Q. Y. Wen, and J. Zhang, "A steganographic method for digital images with four-pixel differencing and modified LSB substitution," *J. Vis. Commun. Image Represent.*, vol. 22, no. 1, pp. 1–8, 2011, doi: 10.1016/j.jvcir.2010.08.007.

[42] M. Hussain and M. Hussain, "Information hiding using edge boundaries of objects," *Int. J. Secur. its Appl.*, vol. 5, no. 3, pp. 1–10, 2011.

[43] Y. Bassil, "Image Steganography based on a Parameterized Canny Edge Detection Algorithm," *Int. J. Comput. Appl.*, vol. 60, no. 4, pp. 35–40, 2012, doi: 10.5120/9682-4112.

[44] M. Mahajan and N. Kaur, "Let's Play with Images and Private Data Using Stick of Randomness BT - Global Trends in Information Systems and Software Applications," P. V. Krishna, M. R. Babu, and E. Ariwa, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 619–628.

[45] M. Hussain, "A Survey of Image Steganography Techniques," *Int. J. Adv. Sci. Technol. (IJAST)*, vol. 54, pp. 113–125, May 2013.

[46] V. Nagaraj, V. Vijayalakshmi, and G. Zayaraz, "Color Image Steganography based on Pixel Value Modification Method Using Modulus Function," *IERI Procedia*, vol. 4, pp. 17–24, 2013, doi: 10.1016/j.ieri.2013.11.004.

[47] J.-Y. Yan, T.-H. Chen, and C.-H. Lin, "Encryption in High Dynamic Range Images for RGBE Format," in *2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 2013, pp. 493–496. doi: 10.1109/IIH-MSP.2013.128.

ISSN (online): 2581-3048

Volume 8, Issue 1, pp 45-54, January-2024

https://doi.org/10.47001/IRJIET/2024.801006

[48] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, "Reversible Data Hiding in Encrypted Images by Reserving Room Before Encryption," *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 3, pp. 553–562, 2013, doi: 10.1109/TIFS.2013.2248725.

[49] D. Singla and M. Juneja, "An analysis of edge based image steganography techniques in spatial domain," *2014 Recent Adv. Eng. Comput. Sci. RAECS 2014*, vol. 1, no. 2, 2014, doi: 10.1109/RAECS.2014.6799604.

[50] H. Al-Dmour and A. Al-Ani, "A Steganography Embedding Method Based on Edge Identification and XOR Coding," *Expert Syst. Appl.*, vol. 46, Oct. 2015, doi: 10.1016/j.eswa.2015.10.024.

[51] Y.-T. Lin, C.-M. Wang, W.-S. Chen, F.-P. Lin, and W. Lin, "A Novel Data Hiding Algorithm for High Dynamic Range Images," *IEEE Trans. Multimed.*, vol. 19, no. 1, pp. 196–211, 2017, doi: 10.1109/TMM.2016.2605499.

[52] P. Puteaux and W. Puech, "An Efficient MSB Prediction-Based Method for High-Capacity Reversible Data Hiding in Encrypted Images," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 7, pp. 1670–1681, 2018, doi: 10.1109/TIFS.2018.2799381.

[53] X. Gao, Z. Pan, E. Gao, and G. Fan, "Reversible data hiding for high dynamic range images using two-dimensional prediction-error histogram of the second time prediction," *Signal Processing*, vol. 173, p. 107579, 2020, doi: https://doi.org/10.1016/j.sigpro.2020.107579.

[54] C. F. Lan, C. M. Wang, and W. Lin, "XtoE: A Novel Constructive and Camouflaged Adaptive Data Hiding and Image Encryption Scheme for High Dynamic Range Images," *Appl. Sci.*, vol. 12, no. 24, 2022, doi: 10.3390/app122412856.

[55] X. Wang, C.-C. Chang, C.-C. Lin, and C.-C. Chang, "Reversal of pixel rotation: A reversible data hiding system towards cybersecurity in encrypted images," *J. Vis. Commun. Image Represent.*, vol. 82, p. 103421, 2022, doi: https://doi.org/10.1016/j.jvcir.2021.103421.

[56] Y.-Y. Tsai, H.-L. Liu, P.-L. Kuo, and C.-S. Chan, "Extending Multi-MSB Prediction and Huffman Coding for Reversible Data Hiding in Encrypted HDR Images," *IEEE Access*, vol. 10, pp. 49347–49358, 2022, doi: 10.1109/ACCESS.2022.3171578.

[57] K. S. Hsieh and C. M. Wang, "Multi-Hider Reversible Data Hiding Using a Weighted Color Transfer and Modulus Operation," *Appl. Sci.*, vol. 13, no. 2, 2023, doi: 10.3390/app13021013.

Citation of this Article:

Noor Gh. Abdullah, Shahd A. Hasso, "An In-Depth Analysis of Steganography Techniques: From Classical Edge Detection to Adaptive Approaches" Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 8, Issue 1, pp 45-54, January 2024. Article DOI https://doi.org/10.47001/IRJIET/2024.801006

****