International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 07 July 2024
Page No: 1986- 1996
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0271

A Review on Image Steganography Techniques

Avantika Bisht[1], Annu Singla[2], Kamaldeep Joshi[3]
[1,2]M.Tech. student, CSE, UIET, M.D. University, Rohtak, India.
[3]Assistant Professor, CSE, UIET, M.D. University, Rohtak, India.
Email id: *avantikabisht910@gmail.com[1] ,annusingla59@gmail.com[2] , kamalmintwal@gmail.com[3]*

Abstract
In contemporary times, the exploration of digital multimedia has transformed it into a reliable medium for secure communication. Steganography, the art of concealed communication through mediums like images, has emerged as a pivotal approach, countered by the opposing method of steganalysis for detecting embedded data. This review delves into diverse methodologies examined by researchers, elucidating the primary objective of image steganography—to safeguard data messages from illicit access. The essence lies in discreetly transferring embedded secure data to the target destination without detection by unauthorized users. While various carrier file formats can be employed, digital images, owing to their widespread use on the global Internet, become the preferred medium. The realm of steganographic methodologies encompasses a broad spectrum, varying in complexity, each with its distinct strengths and weaknesses. This exploration underscores the dynamic landscape of image steganography, affirming the ongoing pursuit of effective methods to protect information from unauthorized access through covert channels. The review article provides an overview of various methodologies employed by researchers in the field of image steganography. It emphasizes the significance of using digital images as carrier files due to their prevalence on the worldwide Internet. The content acknowledges the complexity of steganographic methods and highlights that each method has its own strengths and weaknesses. Overall, the discussion underscores the importance of exploring and analyzing these methodologies to enhance the effectiveness of image steganography in secure communication.
Keywords: *Cover image, Stego image, Image Steganography, Image Enhancement, Image Processing, Steganalysis, Steganographic Scheme.*

1. Introduction

1.1 An Introduction to Concealed Data Within Images

Image steganography captivates with its exploration of concealing data within digital images, imperceptible to human observation. This technique, rooted in the art of secret communication, enables individuals to embed messages or data discreetly within images, ensuring that the presence of the hidden information remains hidden to those who are not intended recipients. Unlike cryptography, which focuses on securing the content of a message, steganography prioritizes the concealment of the message itself, making it a subtle and covert method of communication.

1.2 Steganography Techniques

Several techniques are employed in image steganography, each with its own set of strengths and limitations. From basic methods like Least Significant Bit (LSB) substitution to more advanced approaches such as frequency domain transformations, steganography offers a diverse toolkit for hiding information within images. These techniques manipulate pixel values, alter color information, or transform images in ways that are imperceptible to human observers. the human eye's limited sensitivity to subtle changes, makes it a powerful tool in various applications, ranging from secure communication to digital.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 07 July 2024
Page No: 1986- 1996
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0271

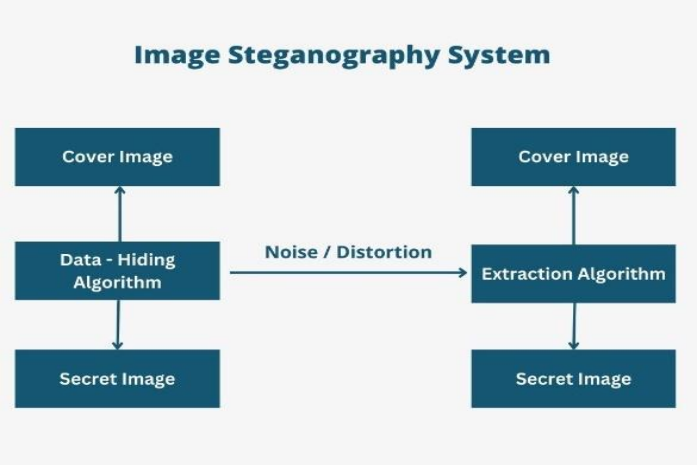

Figure 1 Stenography System

1.3 Why Image Steganography is a Better Approach

Image steganography holds several advantages over other forms of steganography, making it a preferred approach in certain scenarios:

a. Inconspicuousness:

Embedding information within the pixels of an image, especially using LSB substitution or frequency domain techniques, allows for a high level of inconspicuousness. The alterations made are often subtle and escape casual visual inspection.

b. Wide Applicability:

Images are ubiquitous in digital communication, and image steganography can be applied across various formats like JPEG, PNG, and GIF. This universality makes it a versatile choice for hiding information.

c. Human Perception Tolerance:

The human visual system is less sensitive to small changes in images, especially when those changes occur in less critical components like the least significant bits or certain frequency domains. This tolerance allows for effective concealment.

d. Robustness:

Image steganography techniques can be robust against common image processing operations, compression, and other transformations. The hidden information often survives these processes, maintaining its integrity.

e. Plausible Deniability:

Since the alterations made to the carrier image are subtle, it becomes challenging for adversaries to prove the existence of hidden information. This plausible deniability is a valuable feature in scenarios where secrecy is crucial.

In summary, image steganography stands out as an effective and versatile approach for covert communication. Its ability to seamlessly integrate hidden information within the visual content of images, coupled with the human eye's limited sensitivity to subtle changes, makes it a powerful tool in various applications, ranging from secure communication to digital watermarking.

2. Enhancing Security through Image Steganography

Image steganography serves as an innovative and Clandestine tool to bolster security measures in digital communication. By seamlessly concealing sensitive information within seemingly innocuous images, this technique provides an additional layer of protection against unauthorized access and detection.One of the key advantages of using image steganography for security lies in its ability to obscure the existence of hidden data. Unlike traditional encryption methods that might attract attention due to the use of specific algorithms or patterns, steganography operates discreetly within the visual components of an image. This covert integration helps in maintaining a low profile and reduces the likelihood of interception.Furthermore, the inconspicuous nature of steganographically embedded data enhances the overall security posture by leveraging the human eye's limited perceptual abilities. The alterations made to the carrier image are often subtle, residing in less noticeable aspects such as the least significant bits or specific frequency domains. This ensures that even a meticulous visual inspection may not reveal the presence of hidden information.The versatility of image steganography also contributes to its role in security. As images are commonplace in digital communication, the technique can be applied across various platforms and file formats, rendering it a pragmatic and flexible option for safeguarding a variety of data types.Additionally, the robustness of image steganography against common image processing operations, compression, and transformations adds to its reliability as a security measure. The hidden information remains intact through these processes,

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 07 July 2024
Page No: 1986- 1996
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0271

maintaining its confidentiality even in dynamic digital environments.In essence, security through image steganography involves leveraging the concealment of data within the visual fabric of images to thwart potential threats and unauthorized access. Its discreet nature, coupled with the ability to integrate seamlessly into everyday digital communication, positions image steganography as an asset in enhancing the security of sensitive information. Whether applied in covert messaging or safeguarding digital assets, this technique offers a unique and effective approach to fortify.

3. Literature Review

Numerous studies have been conducted in the realm of image steganography, and this section delves into some of the research pertinent to the field.

Sriram K.V.; Havaldar R.H. [2023] The research paper under consideration covers a relevant subject that image steganography covertly embeds messages into images through pixel value alterations, guided by encryption algorithms. The contemporary challenge involves concealing entire images within cover images. Addressing this, the Variational Auto-Encoder (VAE) architecture, an artificial neural network, efficiently learns with minimal dimensions. This process minimizes loss and eliminates noise during image concealment. VAE systematically encodes a clandestine image within a cover image using the encoding network, subsequently retrieving it using the decoding network. Image Steganography using Convolutional Neural Networks (CNN) proves highly compatible, accurate, and incurs minimal loss, applicable to diverse data types like remote sensing and aerial images. The model showcases robust training, loss reduction capabilities, and versatility in handling varied datasets beyond ImageNet, ensuring a secure and effective steganographic process.

Maurya S.; Nandu N.; Patel T.; Reddy V.D.; Tiwari S.; Morampudi M.K. [2023] In conclusion, this paper introduces a robust steganography scheme, crucial for safeguarding vast amounts of sensitive data amidst insecure network communication. Effectively concealing grayscale secret images within color cover images, the scheme employs a modified quantum substitution box (S-Box) in the frequency domain. The strategic utilization of the quantum S-Box to embed confidential bits within randomly chosen channels enhances overall security. The method seamlessly integrates discrete cosine transform (DCT) alongside the adjusted quantum S-Box, optimizing DCT coefficients' placement for intelligent substitution of least significant bits. Security analyses, including key space evaluation and robustness assessments, validate the method's effectiveness. Simulation results demonstrate the scheme's superiority in visual image quality metrics, making it a notable contribution to secure data communication and covert information transmission.

Sharma V.; Mir R.N.; Rout R.K. [2023] In summary, A novel approach called dynamic concealment technique is introduced, enhances security through strategically introducing alterations to cover images, considering their complex texture details. This method utilizes adversarial example generation techniques such as the fast gradient sign method to create these alterations. A combined texture characteristic is formulated by merging local binary patterns and residual interference characteristics to represent texture. The image is divided into areas according to nearby meaning, as identified through a method known as basic linear iterative grouping. Utilizing the hybrid descriptor and segmentation results, a weighted mask is generated for optimal placement of adversarial perturbations, enhancing security without conspicuous traces. Extensive experiments on BOSSbase and BOWS2 datasets demonstrate the superiority of the proposed method in increasing steganography security with minimal observable impact.

Ambika; Virupakshappa; Veerashetty S. [2022] In summary, addressing security challenges in Wireless Sensor Networks (WSN), this work explores Steganography as a robust encryption technique. Leveraging Generative Adversarial Networks (GAN), the method conceals aggregated data within cover images, enhancing security against steganalysis attacks. However, inherent issues, such as image fluctuations over lossy networks and potential unauthorized access to secret information, are acknowledged. The suggested advanced GAN Steganography method effectively tackles these concerns, as demonstrated by experimental results revealing heightened Peak Signal-to-Noise Ratio

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 07 July 2024
Page No: 1986- 1996
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0271

(PSNR), diminished Mean Square Error (MSE), and enhanced Structural Similarity Index (SSIM). These observations emphasize the significance of the proposed approach in bolstering security while mitigating data loss.

Agarwal S.; Jung K.-H. [2022] In conclusion, this study introduces a resilient deep neural network specifically crafted for detecting content-adaptive image steganography, crucial in combating the misuse of hiding improper data within digital images. The proposed method incorporates novel strategies, including non-trainable convolutional layers with fixed high-pass kernels, layer-specific learning rates, and ReLU with customized thresholding, demonstrating improved detection performance. Notably, the approach avoids image down-sampling, relying solely on the global average pooling layer. Experimental results, validated on BOWS2 and BOSSBase datasets using various steganography schemes, showcase the proposed scheme's superiority over recent techniques in most cases, affirming its efficacy in content-adaptive steganography detection.

Gaffar A.; Joshi A.B.; Singh S.; Srivastava K. [2022] In summary, concealing sensitive information within a host image poses a significant challenge, and recent image steganography methods have often faced limitations in embedding capacity or vulnerability. The GRNSCT model, founded on the Golden Ratio and Non-Subsampled Contourlet Transform, is introduced, addresses these concerns by offering both high embedding capacity and enhanced confidentiality. Through a mosaic process and two-level NSCT, it achieves remarkable embedding capacity, while double-layer encryption using a card shuffling method ensures confidentiality. Rigorous security evaluations, including key sensitivity, histogram analysis, and information entropy, confirm the robustness of the hidden images. Experimental results illustrate the effectiveness of the proposed approach, achieving a 300% payload at 24 bits per pixel (bpp) with a Peak Signal-to-Noise Ratio (PSNR) reaching up to 42.38 dB, surpassing current approaches.

Sharma V.K.; Sharma P.C.; Goud H.; Singh A. [2022] In conclusion, this paper introduces a robust image steganography technique, leveraging graph signal processing, for secure communication through social networks. Quantum scrambling is employed to obtain a scrambled version of the secret image, and the subsequent graph wavelet transformation enhances interpixel correlation. Applying α blending to the cover image and scrambled secret image signals ensures effective embedding. The inverse graph wavelet transformation produces the stego image, maintaining excellent visual quality. Experimental results demonstrate identical picture quality between the cover and stego images, affirming the efficacy of the proposed method in achieving secure and visually indistinguishable steganographic communication.

Seenappa V.; Krishnappa N.C.; Mallesh P.K. [2022] In conclusion, this research addresses the need for secure information handling in the medical field through Image Steganography. Existing methods suffer from image quality limitations, prompting the proposal of a novel approach employing DNA sequences from a hyperchaos system and a hybrid compression technique involving Discrete Wavelet Transform (DWT) and Neural Network. Utilizing medical images for testing, the developed method demonstrates enhanced performance, as indicated by a 57.21 PSNR value for the cover image. The hybrid compression method proves effective, significantly improving image quality in steganography, with superior PSNR values compared to individual compression components, validating its potential for secure medical data concealment.

Trivedi V.K.; Stalin S.; Joshi S.; Alkinani M.H.; Shukla P.K.; Gaur B. [2022] In summary, the widespread adoption of social media necessitates robust privacy safeguards. In response, we propose a secure "user data protection scheme" that involves encrypting data using the RC4 algorithm and embedding it within multimedia images through 3–3 least significant bits (LSB) techniques, supplemented by the Bernoulli map. This approach ensures heightened security by employing dual encryption techniques—RC4 for user data encryption and the Bernoulli map for random LSB embedding. Experimental findings demonstrate superior performance, achieving a 9 bits per pixel (bpp) embedding capacity in color images with a Peak Signal-to-Noise Ratio (PSNR) exceeding 42 dB, and

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 07 July 2024
Page No: 1986- 1996
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0271

3 bpp in grayscale images. Notably, our method results in less distortion in stego-images compared to current methodologies.

Mandal P.C.; Mukherjee I.; Paul G.; Chatterji B.N. [2022] In conclusion, electronic picture concealment digital images plays a pivotal role in ensuring secure communication, concealing information within cover media. The paper offers an in-depth examination and analysis of recent steganographic techniques, addressing challenges in deep learning-based approaches. The balance between embedding capacity, imperceptibility, and security remains a key challenge. With the increasing importance of security and computational power, steganography has become integral to modern applications. The discussion extends to popular steganography tools, offering insights into the evolving landscape. The article concludes by highlighting future research directions, emphasizing the continual exploration of this domain for enhanced secure communication methods.

Agrawal R.; Ahuja K.; Steinbach M.C.; Wick T. [2022] In summary, our Sparse Approximation Blind Multi-Image Steganography (SABMIS) scheme tackles the challenging task of concealing grayscale secret images within grayscale cover images. It Increases the embedding capacity while maintaining the visual fidelity of both the stego-image and the retrieved secret images. The innovative embedding method, utilizing ADMM and LASSO formulations, ensures resilience against steganographic attacks. SABMIS outperforms existing methods, particularly in hiding multiple secret images, demonstrating superior embedding capacities and minimal quality deterioration. Its security is reinforced by resistance to attacks, this renders it among the most secure methods available. Furthermore, SABMIS demonstrates effective implementation and practical utility for securely transmitting medical images online.

Krishna B.M.; Santhosh C.; Suman S.; Shireen S.S. [2022] In conclusion, ensuring highly secure communication is paramount in the digital era, necessitating robust cryptographic methods. This paper introduces a DNA-based asymmetric algorithm, comparing its performance with ElGamal, RSA, and Diffie–Hellman algorithms. Applied to image steganography for encrypting patient information, the proposed method exhibits enhanced efficiency with minimal hardware resource consumption and improved latency. Leveraging Dynamic Partial Reconfiguration (DPR) enhances security by allowing selective transformation without system shutdown. The cryptosystem, designed and simulated in Xilinx Vivado, is programmed with secure partial bit files on diverse architectures, including Basys3, Nexys4 DDR, and Zync-7000 AP SoC, fortifying resilience against vulnerable attacks in the channel.

Chinniyan K.; Samiyappan T.V.; Gopu A.; Ramasamy N. [2022] In summary, steganography, akin to cryptography, enables secret communication by concealing data within seemingly normal information. Unlike traditional cryptography, steganography focuses on hiding the very existence of the message, avoiding suspicion and attention. The developed Stacked Autoencoder model efficiently compresses, encodes, decodes, and encrypts data using Elliptic Curve Cryptography. Trained on the Flickr Image Dataset, the model integrates both cover and secret images, yielding a container image. The outcomes illustrate a secret image with a 4% degradation and a container image with a 14% degradation, highlighting the efficacy of the suggested method in ensuring secure and discreet data concealment.

Sharma H.; Mishra D.C.; Sharma R.K.; Kumar N. [2021] In summary, safeguarding digital information from cyber threats is crucial, prompting the introduction of An innovative multi-image cryptographic steganography technique utilizing the Rabin cryptosystem and Arnold transform, this approach conceals diverse data forms securely. The (n,n) secret sharing prevents impersonation attacks, employing header information for accurate data retrieval. Camouflaging randomized encrypted data in image edges ensures adaptability and security. Experimental results demonstrate high Peak Signal-to-Noise Ratio (PSNR) and minimal Mean Squared Error (MSE) values are observed across audio, image, and video signals, along with entropy metrics closely matching the original cover image. Sensitivity analysis underscores resilience, and comparative assessments position the proposed

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 07 July 2024
Page No: 1986- 1996
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0271

technique as superior or comparable to existing methods in standard evaluation metrics.

Sukumar A.; Subramaniyaswamy V.; Ravi L.; Vijayakumar V.; Indragandhi V. [2021] In conclusion, the growing vulnerability of sensitive medical images to data threats necessitates robust security measures during transmission across insecure channels. This work introduces a formidable image steganography approach, incorporating Excessive Integer Wavelet Transformation, Laplacian Pyramid Decomposition, Arnold Transformation Scrambling, and Histogram Displacement techniques. Deep learning classification ensures stego images evade detection by the Human Visual System. Comparative analysis demonstrates superior performance with average NCC values of 0.8917 and average PSNR values of 36.375, even at increased embedding rates. Security and robustness assessments further affirm the effectiveness of the proposed method, positioning it as superior to related approaches in the literature.

Swain G.; Pradhan A. [2022] In summary, this research presents a steganography technique utilizing adaptive quotient value differencing (AQVD), quotient value correlation (QVC), and remainder replacement for camouflaging and retrieving data in 3-by-3 pixel blocks. The method addresses the problem of unused pixel blocks and guarantees data integrity verification upon reception. By segmenting a pixel block into quotient (QT), middle bit (M), and remainder (R) blocks, the technique employs AQVD and QVC procedures to achieve efficient data concealment. Verification bits within the R block facilitate integrity checks, and experimental findings indicate enhanced HC and PSNR values, along with resilience to regular-singular and pixel difference histogram analyses.

Mukherjee S.; Sarkar S.; Mukhopadhyay S. [2021] In summary, this paper presents a novel image steganography technique using a double-layered pencil-shaped shell matrix, prioritizing high embedding capacity, superior visual fidelity, and enhanced privacy and security. The proposed approach conceals an additional 2 bits within every pixel pair, resulting in a capacity of 3.0 bits per pixel (bpp) with an average signal-to-noise ratio (SNR) of 43.25 decibels. Comparative evaluations demonstrate its superiority over existing steganographic schemes based on shell matrices, validated through RS, JPEG compression, Q-index, and normalized absolute error assessments. The method offers significant advantages for various sectors in both private and government organizations, showcasing resilience and security.

Krishnaveni N.; Sudhakar P. [2022] In conclusion, this paper addresses the growing the necessity of safeguarding data in digital communication, highlighting the importance of cryptography and steganography. Steganography, focusing on data concealment, is particularly significant for multimedia data. The proposed image steganography algorithms, spanning spatial, frequency, and wavelet domains, showcase improved performance compared to traditional methods. Experimentation on the USC-SIPI image database reveals higher PSNR values close to 53 after secret data embedding, surpassing existing algorithms with an average PSNR around 50. The proposed methods contribute to enhanced data security in visual content transmission, catering to the increasing demands of digital communication and large datasets.

Chaudhary S.; Hiranwal S.; Gupta C.P. [2021] In summary, this study introduces an innovative image steganography method employing graph signal processing (GSP). The approach incorporates Arnold cat map transform, Spectral graph wavelet, and singular vector decomposition (SVD) to enhance security. The alpha blending process and GSP-based synthesis contribute to creating a robust stego image with improved visual quality. Evaluation metrics, including PSNR, NCC, SC, and AD, affirm the efficacy of the proposed scheme. The scheme proves resilient against image processing attacks, highlighting its efficiency and robustness in concealing sensitive information within cover media while maintaining high-quality stego images.

Mehta D.; Bhatti D. [2022] In conclusion, This paper presents an innovative method for digital image steganography aimed at countering JPEG compression attacks, a notable challenge in secure data transmission over public networks. The proposed method utilizes DC coefficients of Discrete Cosine Transform (DCT), ensuring robustness against lossy JPEG compression while maintaining a

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 07 July 2024
Page No: 1986- 1996
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0271

100% retrieval rate for concealed information, with payloads of up to 8192 bits, while remaining imperceptible. The approach involves embedding a key, derived from a fusion of the hidden message and cover image, into the most significant bits (MSBs) of the DC values within selected DCT blocks. Extensive simulation experiments validate the effectiveness of the algorithm, demonstrating its resilience under various quality factors and highlighting superior performance through metrics such as Peak Signal-to-Noise Ratio (PSNR), Payload, Bits Per Pixel (BPP), Structural Similarity Index (SSIM), and Normalized Cross-Correlation (NCC).

Ravikumar K.P.; Reddy H.S.M. [2021] In conclusion, the proposed Crow Search Algorithm-based Deep Belief Network (CSA-DBN) emerges as an effective solution for securing patient information through image steganography. By strategically analyzing pixel attributes such as pixel distribution, wavelet strength, edge features, and texture attributes (Local Binary Patterns (LBP) and Local Directional Patterns (LDP)), CSA-DBN identifies appropriate pixels for data embedding. Utilizing embedding intensity and Discrete Wavelet Transform (DWT) coefficient, medical data is seamlessly integrated and later extracted. Performance assessment, incorporating metrics such as correlation coefficient, PSNR, and SSIM, demonstrates the resilience of CSA-DBN. Even when confronted with salt and pepper noise, the technique achieves mean values of 0.9471, 24.836 decibels, and 0.4916, respectively. Without such noise, these metrics notably rise to 0.9741, 57.832 decibels, and 0.9766, respectively.

Sharma N.; Batra U. [2021] In conclusion, this study concentrates on enhancing image steganography by introducing a tool that utilizes Huffman Encoding and Particle Swarm Optimization (HPSO). The key objectives include preserving image quality and maximizing data-carrying capacity. The HPSO scheme not only achieves higher information embedding capacity while preserving image quality effectively. Experimental results, using metrics such as Peak Signal-to-Noise Ratio (PSNR), Mean Square Error (MSE), Bit Error Rate (BER), and Structural Similarity Index (SSIM) underscore the outstanding efficacy of the proposed HPSO approach. Furthermore, its robustness against statistical attacks enhances the overall efficiency of the information hiding scheme.

Maji G.; Mandal S.; Sen S. [2021] In conclusion, this study presents a novel method for spatial domain image steganography, employing XOR-based encoding to embed encoded confidential message bits into various higher-order pixel value bits. The approach involves block-wise encoding and Least Significant Bit (LSB) embedding to minimize distortion while increasing payload capacity. The proposed scheme achieves visual imperceptibility and enhances image quality measures such as Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Normalized Cross-Correlation (NCC), and Structural Similarity Index (SSIM). Notably, it surpasses alternative methods in resisting standard steganalysis attacks, ensuring secure communication with an average PSNR value exceeding 51dB even at 90% capacity utilization.

Ghosal S.K.; Mukhopadhyay S.; Hossain S.; Sarkar R. [2021] In summary, this study introduces a novel steganographic scheme using the Laguerre transform (LT) in the transform domain. Employing LT on non-overlapping m-pixel groups of the cover image, the scheme embeds encoding variable-length bits from secret data into the transformed components. Following incorporation, adjustments are made to reduce distortion. Findings show a growing discrepancy between cover and stego-pixels with the increment of m, suggesting improved security. The proposed approach surpasses certain state-of-the-art techniques., offering improved stego image quality and higher payload capacity. This highlights the efficacy of the Laguerre transform-based approach in achieving secure and efficient steganography in the transform domain.

Shashikiran B.S.; Shaila K.; Venugopal K.R. [2021] In conclusion, this study emphasizes the paramount importance of data security in the digital realm, addressing it through the suggested algorithm merges image encryption and steganography techniques. By utilizing the Knight's Tour Algorithm from chess, a 5x5 block pattern is created for image encryption, enhancing security measures. The ciphered image is subsequently inserted into another image, followed by additional block rearrangement to generate a cryptographic-steganographic image. The

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 07 July 2024
Page No: 1986- 1996
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0271

technique proves its effectiveness by ensuring robust data security, as evidenced by favorable Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM) metrics. This method offers a promising solution for securing digital information.

Mukherjee (Ganguly) N.; Paul G.; Saha S.K. [2021] To conclude, this study introduces an innovative steganographic technique leveraging pixel difference values in non-sequentially chosen adjacent pixel pairs. Demonstrating exceptional embedding capacity (up to 8 bits) without necessitating a seed or key, the algorithm proves robust against visual, structural, and statistical attacks. Comparative analyses against state-of-the-art methods highlight its efficacy, while successful resistance to StirMark benchmarks underscores its robustness. The proposed technique showcases high versatility and resilience, establishing itself as a promising solution in the realm of steganography with notable resistance to various testing scenarios and attacks.

Ambika; Biradar R.L. [2021] To sum up, image steganography is a vital facet in modern information technology, facilitating secure communication through covert transmission of secret information within carriers. In this study, a cutting-edge technique is presented, which integrates the Integer Wavelet Transform (IWT) of lower frequency, fractal encryption, and the L-shaped tromino theorem applied in the transform domain. This innovative approach, known as the IWT-fractal encryption method, boosts embedding capacity while keeping computational complexity low, thus guaranteeing high-quality secret image transmission. Experimental findings showcase substantial enhancements in peak signal-to-noise ratio (PSNR) and entropy metrics when compared to conventional methods. This affirms the proposed technique's efficacy, providing heightened network security with lower computational demands than contemporary approaches.

Yadav G.S. [2021] In conclusion, safeguarding information while ensuring imperceptibility remains a crucial challenge in data-hiding techniques. The conventional static key/pattern approaches, though secure, may compromise imperceptibility. Addressing this, the proposed genetic algorithm-based data-hiding scheme employs chromosomes as dynamic keys, ensuring enhanced imperceptibility and security. Comparative analysis based on imperceptibility measures, including PSNR, NC, and SSIM, reveals significant improvements, achieving a PSNR increase of up to 46.25 (over 2%) in imperceptibility. This underscores the efficiency of the genetic algorithm method in maintaining a balance between security and imperceptibility during data-hiding operations.

Mukhopadhyay S.; Hossain S.; Ghosal S.K.; Sarkar R. [2021] In summary, this study presents a successful image steganography method utilizing the Catalan Transform (CT) in the transform domain. By decomposing the cover image into non-overlapping 2×2 blocks and transforming them with CT, secret bits are embedded, allowing a payload 1 to 4 bits per pixel (bpp) range. The inverse Catalan Transform (ICT) is subsequently utilized to produce stego-pixels. Experimental findings consistently reveal superior Peak Signal to Noise Ratio (PSNR) values exceeding 30 dB, outperforming existing techniques. Additional parameters such as Mean Squared Error (MSE), Structural Similarity Index (SSIM), and Normalized Cross-Correlation (NCC) are also evaluated, confirm the effectiveness of the proposed scheme. The stego-images exhibit robustness against detection by the StegExpose tool, underscoring the method's security.

Agrawal R.; Ahuja K. [2021] In conclusion, this paper presents an innovative scheme for Compressed Sensing Image Steganography (CSIS) aimed at enhancing embedding capacity while preserving stego-image visual quality, particularly in compressed formats. CSIS employs sparsification of the cover image in blocks, obtaining linear measurements and selecting permissible measurements. The encrypted secret data is then embedded into these measurements, achieving embedding capacity 1.53 times higher than recent schemes. Reconstruction involves utilizing the Alternating Direction Method of Multipliers (ADMM) and the Least Absolute Shrinkage and Selection Operator (LASSO). Experimental results on standard grayscale and color images exhibit superior performance with a 37.92 dB average PSNR, and mean SSIM index and NCC coefficients close to 1, demonstrating CSIS's significant advancement

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 07 July 2024
Page No: 1986- 1996
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0271

4. Proposed

The proposed study aims to meet the following goals through comprehensive analysis.

1. Develop an image steganography algorithm.
2. Enable the embedding of any image within another image.
3. Ensure the hidden image is imperceptible to human vision.
4. Support various image formats.
5. Maintain the visual quality of the cover image.
6. Balance high payload capacity and imperceptibility.
7. Ensure robustness against image processing operations like compression and resizing.
8. Achieve computational efficiency for real-time embedding and extraction.
9. Provide functionality to display the cover image before and after embedding.Include a feature to extract and display the hidden image.

5. Scope of Research

The scope of research in image steganography remains expansive, focusing on advancing techniques for secure data concealment within images. Ongoing efforts aim to enhance the robustness and imperceptibility of hiding schemes, addressing challenges posed by evolving steganalysis methods. Researchers explore novel approaches to increase capacity, extend applicability to diverse image formats, and improve resistance against various image processing operations. Additionally, the integration of advanced cryptographic principles and exploration of innovative transform methods contribute to the continuous evolution of image steganography, making it a dynamic field with broad implications for secure communication, digital watermarking, and intellectual property protection.

Conclusion

In summary, our research has concentrated on enhancing steganalysis performance and assessing the hiding capacities of existing methods. Current state-of-the-art detectors exhibit almost flawless performance against contemporary steganographic schemes, necessitating the development of novel, robust, and secure hiding schemes capable of resisting steganalytic detection. These hiding schemes must satisfy three crucial requirements: security against steganalysis, robustness in the face of transmission channel distortions, and sufficient capacity for the embedded method. Importantly, our work demonstrates adaptability, allowing extension to diverse image formats. Furthermore, potential extensions involving alternative transform methods are also feasible. By addressing these aspects, our study contributes to the ongoing evolution of steganography, emphasizing the need for advanced hiding techniques to overcome challenges in steganalysis and maintain the effectiveness of covert information transmission.

References

[1] Jaffrin, L. C., Karthikayan, P. N., Datta, S., & Majumdar, A. (2023, June). Convolutional Neural Network Based Image Steganography. In Recent Trends in Computational Intelligence and Its Application: Proceedings of the 1st International Conference on Recent Trends in Information Technology and its Application (ICRTITA, 22) (p. 321). CRC Press.

[2] Maurya, S., Nandu, N., Patel, T., Reddy, V. D., Tiwari, S., & Morampudi, M. K. (2023). A discrete cosine transform-based intelligent image steganography scheme using quantum substitution box. Quantum Information Processing, 22(5), 206.

[3] Sharma, V. K., Mir, R. N., & Rout, R. K. (2023). Towards secured image steganography based on content-adaptive adversarial perturbation. Computers and Electrical Engineering, 105, 108484.

[4] Veerashetty, S. (2022). Secure communication over wireless sensor network using image steganography with generative adversarial networks. Measurement: Sensors, 24, 100452.

[5] Agarwal, S., & Jung, K. H. (2022). Identification of Content-Adaptive Image Steganography Using Convolutional Neural Network Guided by High-Pass Kernel. Applied Sciences, 12(22), 11869.

[6] Gaffar, A., Joshi, A. B., Singh, S., & Srivastava, K. (2022). A high capacity multi-

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 07 July 2024
Page No: 1986- 1996
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0271

image steganography technique based on golden ratio and non-subsampled contourlet transform. Multimedia Tools and Applications, 81(17), 24449-24476.

[7] Sharma, V. K., Sharma, P. C., Goud, H., & Singh, A. (2022). Hilbert quantum image scrambling and graph signal processing-based image steganography. Multimedia Tools and Applications, 81(13), 17817-17830.

[8] Seenappa, V., Krishnappa, N. C., & Mallesh, P. K. (2022). Hybrid Compression and DNA Sequence of Hyper Chaos System for Medical Image Steganography. International Journal of Intelligent Engineering & Systems, 15(3).

[9] Trivedi, V. K., Stalin, S., Joshi, S., Alkinani, M. H., Shukla, P. K., & Gaur, B. (2022). User data privacy in multimedia domain using 3–3 LSB-based color image steganography with RC4 and Bernoulli map protection. Journal of Electronic Imaging, 31(3), 033021-033021.

[10] Mandal, P. C., Mukherjee, I., Paul, G., & Chatterji, B. N. (2022). Digital image steganography: A literature survey. Information sciences.

[11] Agrawal, R., Ahuja, K., Steinbach, M. C., & Wick, T. (2022). SABMIS: sparse approximation based blind multi-image steganography scheme. PeerJ Computer Science, 8, e1080.

[12] Krishna, B. M., Santhosh, C., Suman, S., & Shireen, S. S. (2022). Evolvable hardware-based data security system using image steganography through dynamic partial reconfiguration. Journal of Circuits, Systems and Computers, 31(01), 2250014

[13] Chinniyan, K., Samiyappan, T. V., Gopu, A., & Ramasamy, N. (2022). Image Steganography Using Deep Neural Networks. Intelligent Automation & Soft Computing, 34(3).

[14] Sharma, H., Mishra, D. C., Sharma, R. K., & Kumar, N. (2021). Multi-image steganography and authentication using crypto-stego techniques. Multimedia Tools and Applications, 80(19), 29067-29093.

[15] Sukumar, A., Subramaniyaswamy, V., Ravi, L., Vijayakumar, V., & Indragandhi, V. (2021). Robust image steganography approach based on RIWT-Laplacian pyramid and histogram shifting using deep learning. Multimedia Systems, 27, 651-666.

[16] Swain, G., & Pradhan, A. (2022). Image steganography using remainder replacement, adaptive QVD and QVC. Wireless Personal Communications, 123(1), 273-293.

[17] Mukherjee, S., Sarkar, S., & Mukhopadhyay, S. (2021). Pencil shell matrix based image steganography with elevated embedding capacity. Journal of Information Security and Applications, 62, 102955.

[18] Krishnaveni, N., & Sudhakar, P. (2022). Intricacies in image steganography and innovative directions. International Journal of Advanced Intelligence Paradigms, 23(1-2), 55-71.

[19] Chaudhary, S., Hiranwal, S., & Gupta, C. P. (2021). Spectral Graph Wavelet Based Image Steganography Using SVD and Arnold Transform. Traitement Du Signal, 38(4), 1113-1121.

[20] Mehta, D., & Bhatti, D. (2022). Blind image steganography algorithm development which resistant against JPEG compression attack. Multimedia Tools and Applications, 1-21.

[21] Ravikumar, K. P., & Reddy, H. M. (2021). Pixel Prediction-Based Image Steganography Using Crow Search Algorithm-Based Deep Belief Network Approach. International Journal of Image and Graphics, 21(01), 2150002.

[22] Sharma, N., & Batra, U. (2021). An enhanced Huffman-PSO based image

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 02 Issue: 07 July 2024
Page No: 1986- 1996
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2024.0271

optimization algorithm for image steganography. Genetic Programming and Evolvable Machines, 22, 189-205.

[23] Maji, G., Mandal, S., & Sen, S. (2021). Cover independent image steganography in spatial domain using higher order pixel bits. Multimedia Tools and Applications, 80(10), 15977-16006.

[24] Ghosal, S. K., Mukhopadhyay, S., Hossain, S., & Sarkar, R. (2021). Exploiting Laguerre transform in image steganography. Computers & Electrical Engineering, 89, 106964.

[25] Shashikiran, B. S., Shaila, K., & Venugopal, K. R. (2021). Minimal block knight's tour and edge with lsb pixel replacement based encrypted image steganography. SN Computer Science, 2(3), 139.

[26] Mukherjee, N., Paul, G., & Saha, S. K. (2021). Two-point FFT-based high capacity image steganography using calendar based message encoding. Information Sciences, 552, 278-290.

[27] Ambika, & Biradar, R. L. (2021). A robust low frequency integer wavelet transform based fractal encryption algorithm for image steganography. International Journal of Advanced Intelligence Paradigms, 19(3-4), 342-356.

[28] Yadav, G. S. (2021). A genetic algorithm based image steganography scheme with high embedding capacity and low distortion. The Imaging Science Journal, 69(1-4), 143-152.

[29] Mukhopadhyay, S., Hossain, S., Ghosal, S. K., & Sarkar, R. (2021). Secured image steganography based on Catalan transform. Multimedia Tools and Applications, 80, 14495-14520.

[30] Agrawal, R., & Ahuja, K. (2021). CSIS: Compressed sensing-based enhanced-embedding capacity image steganography scheme. IET Image Processing, 15(9), 1909-1925.