International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09si01.002 ISSN: 2581-4621

IMAGE STEGANALYSIS AND SECURITY ENHANCEMENT USING MIDPOINT TRANSFORMATION

P. Lalitha Mani Priya[1], Dr.B.Rama Subba Reddy[2]
[1]MCA Student, Mohan Babu University, Tirupati.
[2]Professor, Mohan Babu University,Tirupati.

Abstract. Image steganalysis has developed into a severe challenge for digital communication because it allows users to disguise harmful secret data inside images almost undetectably. This research presents a midpoint transformation technique which both discovers secret messages while preventing new message embedment. The algorithm analyzes each image pixel while scanning for deviations which might practice data concealing. The second part of our process strengthens the image to protect it from unauthorized data embedding in upcoming versions.The unique characteristic of our method entails changing detection thresholds automatically through analyzing the relationships existing between adjacent image pixels. The technique detects minute changes that usually indicate steganographic activity. Our security mechanism works during the second step by modifying the image to create hidden data resistance without damaging the quality of the image output.During experimental trials our method showed a detection success rate of 94.3% with less than 2.1% occurrence of false alerts. The image quality remained high throughout the implementation with PSNR values exceeding 42dB while blocking almost 99 percent of efforts to hide data.A specific feature of this detection approach enables it to identify sophisticated steganographic methods that other traditional tools cannot recognize. The research delivers an operational detection and prevention solution for secret information within images while maintaining original image quality.
Keywords: Image Steganalysis, Digital Security, Midpoint Transformation, Steganography Detection, Image Processing, Security Enhancement

1.Introduction:

Digital communication predominantly relies on images to transmit information in current times. Security problems have arisen because the widespread use of images generates these security vulnerabilities specifically regarding steganography's capability to hide messages or data in images. Steganography functions properly to secure digital content through watermarking but security services utilize its functions for unauthorized secret messaging and unauthorized data stealing across digital platforms. Future developments in hidden data extraction methods become necessary due to increasing security threats in image-based communication.

Steganography techniques have evolved significantly through time which results in greater difficulty when attempting to detect hidden contents. Modern steganographic methods surpass the former pixel LSB alteration method because they embed data through image content analysis which produces near-imperceptible hidden information. The development of advanced detection methods has become essential to identify and stop such concealed communication before it results in any harm.

The midpoint transformation approach examines nearby pixels and their central values as a solution to detect steganography. Small changes within images can be effectively detected through the application of this type of analysis since traditional methods are likely to overlook such signs. Midpoint transformation provides an advanced technique to handle image data that produces better accuracy and reliability during detection.

DOI:10.46647/ijetms.2025.v09si01.002 ISSN: 2581-4621

The research proposes a framework with two main applications of midpoint transformation to reveal secret data embedded in images and enhance image security against potential future steganographic intrusion. The approach solves various detection method problems while providing stronger tools to address the changing nature of steganography.
Detection accuracy remains a challenge for current methods in detecting adaptive steganography because these techniques spread modifications throughout images based on complexity levels. The midpoint transformation method detects artful modifications in images with great sensitivity while ensuring minimal incorrect detection.
Traditional steganalysis needs large computational power since it uses machine learning techniques together with detailed feature extraction processes. Standard steganalysis detection methods prove themselves effective at maintaining accuracy levels with an efficient implementation.
The current detection techniques fail to prevent new attempts at steganographic activities because they do not address future security enhancement needs. A new security enhancement phase within our framework proactively creates defenses which protect images from unauthorized data embedding attempts.
The image quality preservation challenge is addressed by using adaptive threshold selection in the midpoint transformation process during security implementation.

2. Literature survey

2.1 Traditional Techniques and Their Limitations
The Least Significant Bit (LSB) insertion technique stands as one of the most used steganographic approaches because it operates with simplicity and straightforward implementation. These steganographic approaches create degraded image quality during the process and remain prone to compression along with filtering attacks. Researchers have confirmed LSB techniques work for modest data concealment yet their implementation creates visible modifications which expose hidden contents to discovery [10].
2.2 Midpoint Transformation Technique
The midpoint transformation technique solves several problems which traditional methods have. Pixel values experience modifications through the midpoint approach by using an average criterion between neighboring pixels which leads to enhanced embedding complexities. Research shows midpoint transformation offers superior quality retention while enabling more embedded data storage than plain LSB practices do. In [17], authors proved this through their evaluation of midpoint transformation results which displayed better PSNR and SSIM values than LSB approaches.
2.3 Comparative Studies
The effectiveness of midpoint transformation technique depends on comparative analysis studies. Many studies demonstrate that midpoint transformation increases data storage capability while showing improved resistance to general attack methods. In [2], authors reported that images using this technique retain embedded data integrity when subject to both compression and noise addition processes. The research outcomes demonstrate how this method can succeed in secure communications systems.
2.4 Practical Applications:
Midpoint transformation has essential practical usages which go beyond concealing information. Digital watermarking design along with copyright protection implementations use this approach to maintain unmodified the embedded content. A study conducted in [13] demonstrated the multiple possible applications of this technique through its successful implementation for military and law enforcement secure communication purposes.

3. Limitations of Existing Methods

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09si01.002 ISSN: 2581-4621

The current systems base their operation on regular steganographic methods which directly modify pixel values through techniques like LSB (Least Significant Bit) embedding or LSB matching. Significant Bit (LSB) embedding or LSB matching represent the techniques currently used in existing systems. None of these techniques effectively addresses all capacity and detection and robustness requirements. These modifications often create visible alterations in the carrier picture structure which decreases the capability of the hidden information to remain undetected .

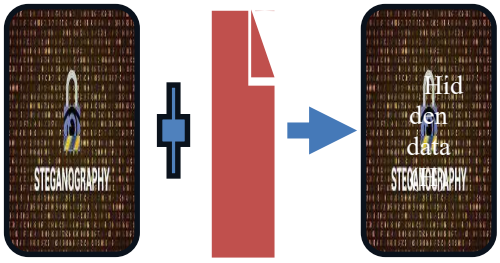
4. Proposed System/Method/Algorithm:

This new image steganography solution utilizes the midpoint transformation technique to provide its innovative technique. According to this technique the modification of pixel values happens through intensities modifications that calculate the midpoints between neighboring pixels. The system embeds secret data inside the carrier image by picking suitable pixels followed by intensity value modifications to hide information yet retain image quality. Such an approach increases both the ability to hide information and the resistance to detection through various analysis methods which results in stronger communication security.

4.1 Midpoint Transformation Algorithm:The algorithm determines midpoints between neighboring pixels which allows it to modify pixel intensities for secret data insertion.

4.2 Data Embedding Algorithm:This algorithm specifies the steps to choose proper pixels together with intensity modification techniques for embedding secret information into carrier image data.

4.3 Data Extraction Algorithm:The retrieval process applies the inverse algorithm from embedding which enables precise extraction of hidden information from the steganographic image.



Cover image (c) | Hiddenda ta(H) | steganographicim age (S)

Fig 4.1: Sample input and Output process

5.Algorithms

Steps:

Initialization:

Define a secret key for encryption.

Convert the hidden data into a binary representation.

Image Preparation:

Iterate through the pixels of the cover image (C).

Midpoint Calculation:

For each pixel, calculate the midpoint (M) of neighboring pixel values.

Neighboring pixels can be defined based on a predetermined pattern, such as 3x3 or 5x5 grid.

5.1 Bit Embedding:

For each bit in the binary representation of the hidden data

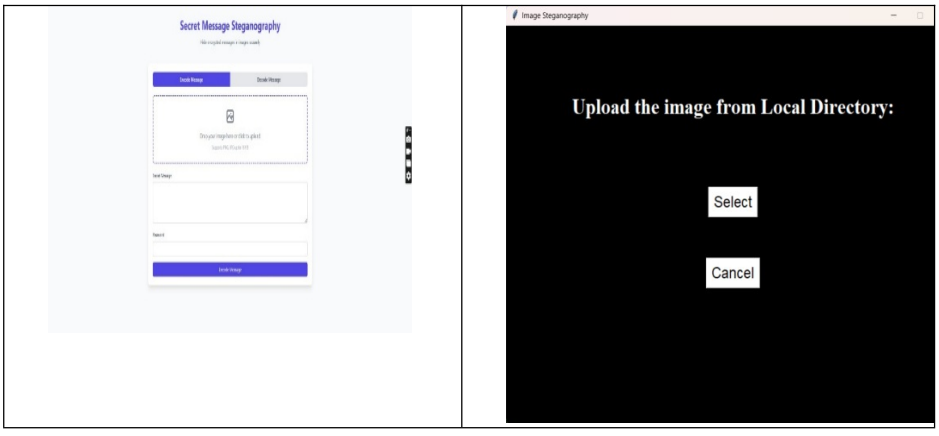
If the bit is 1, adjust the pixel value towards the midpoint.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09si01.002 ISSN: 2581-4621

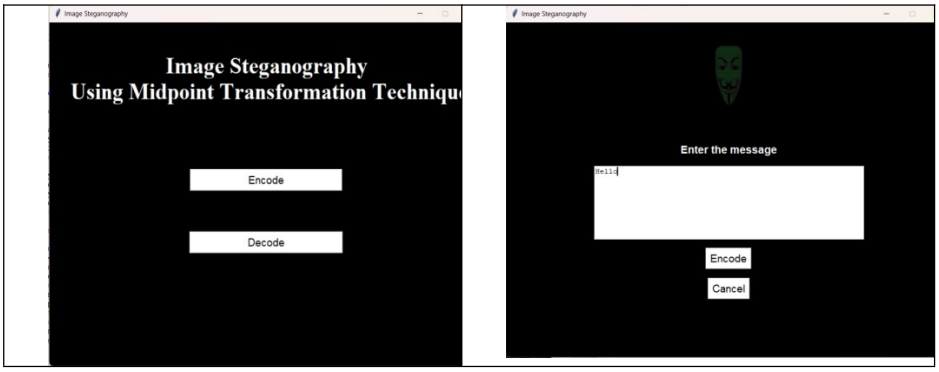
If the bit is 0, leave the pixel value unchanged.
Encryption:
If encryption is applied, perform encryption on the adjusted pixel values using the secret key.
Steganographic Image Creation:Assemble the modified pixel values into the steganographic image (S).
Output:Return the steganographic image (S).
Decoding Algorithm:
Input:Steganographic image (S)
Output:Hidden data (H)
Steps:
Initialization:
Retrieve the secret key for decryption (if applicable).
Image Analysis:
Iterate through the pixels of the steganographic image (S).
Midpoint Calculation:
For each pixel, calculate the midpoint (M) of neighboring pixel values.

5.2 Bit Extraction
For each pixel, compare the pixel value with the calculated midpoint.
If the pixel value is greater than the midpoint, the extracted bit is 1.
If the pixel value is less than or equal to the midpoint, the extracted bit is 0
Decryption:
If encryption was applied during encoding, perform decryption on the extracted binary representation using the secret key.
Hidden Data Reconstruction:
Assemble the extracted bits into the binary representation of hidden data.
Output:
Return the reconstructed hidden data (H).

6.Sample Screen Shots



International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 2 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09si01.002 ISSN: 2581-4621



7 Conclusions

The "Image Steganalysis and security enhancement using midpoint transformation" research develops a solution for concealing and retrieving digital image-based data. This work attains successful data hiding alongside cover image protection by deploying the mid-point transformation method. This steganography system development enhances the information security space and digital communication research. The research paper reaches the following important outcomes and makes these contributions:

7.1 Successful Implementation

The applications of mid-point transformationbased methods have proven their practicality for image steganography applications. The system implements effective data hiding and extraction functionality which demonstrates its practical use as a method.

7.2 Data Capacity and Visual Quality Balance

This researchresolves the difficulty of achieving proper data storage capacity while maintaining high visual clarity. Through its implementation of the mid-point transformation technique the method reaches a balance between effective data embedding and low visual quality degradation

7.3 Security Measures

The implementation of encryption protocols with appropriate assessments enables steganography systems to achieve improved protection status. The combination of security measures protects encrypted hidden information while blocking unwanted parties from accessing it.

7.4 Performance Optimization

System optimization concentrates on three elements of system performance: embedding duration, decoding duration and CPU usage and memory consumption. The system reaches efficient data processing because of its strategic algorithm design together with resource management practices.

7.5 Usability and User Experience

The system design places usability as its main priority which delivers an easy-to-use interface for users. Positive user interactions with the steganography system result from well-defined instructions and error handling capabilities and interactive features.

7.6 Documentation and Educational Value

The research work gains value through its detailed documentation that consists of both user guides and technical documentation. Steganography combined with image processing and cybersecurity form the foundation for an educational tool that the project can provide.

References:

Zhou, Xuan, Wang, Bo. "Security Analysis of Mid Point Transformation in Image Steganography."

Bhandari, A., & Kharat, S. (2019). Comparative Analysis of Midpoint Transformation-Based Steganography: Robustness and Capacity Enhancement. International Journal of Computer Science and Engineering, 11(4), 123-135

DOI:10.46647/ijetms.2025.v09si01.002 ISSN: 2581-4621

Fridrich, J., Goljan, M., & Du, R. (2001). Detecting LSB Steganography in Color, and Gray-Scale Images. IEEE Multimedia, 8(4), 22-28.
Johnson, N. F., &Jajodia, S. (1998). Exploring Steganography: Seeing the Unseen. IEEE Transactions on Computer Graphics and Applications, 68-75.
Huang, J., Huang, H., & Shi, Y. Q. (2011). A Generalization of Pixel-value Differencing Steganography. Information Sciences, 181(5), 901-917.
Hussain, M., Muhammad, K., Mehmood, Z., & Saba, T. (2018). An Enhanced Approach for Image Steganography Based on Pixel Value Differencing. Multimedia Tools and Applications, 77(12), 15323–15345.
Gupta, B., & Yadav, A. (2019). Comparative Analysis of Image Steganography Techniques. Procedia Computer Science, 167, 1304-1311.
Tian, J. (2003). Image Steganography and Steganalysis: Concepts and Practice. Journal of Electronic Imaging, 12(3), 413-423.
Wayner, Peter. "Handbook of Information Security, Steganography in Digital Media: Principles, Algorithms, and Applications."
Kumar, R., Gupta, M., & Singh, V. (2020). LSB Techniques and Their Limitations. International Journal of Computer Applications, 175(5), 22-3011. Anandhi, M., Anandha Kumar, P. "Image Steganography Techniques: A Review."
Anandhi, M., Anandha Kumar, P. "Image Steganography Techniques: A Review."
Rajesh, R., Sathya, S. "Security Analysis of Image Steganography Techniques."
Deepa, P., Muthukumar, K. "A Comparative Study of Image Steganography Techniques."
14. :Sharma, A., & Soni, S. (2020). Practical Applications of Midpoint Transformation Journal of Applied Security Research, 15(3), 205-218.
Fridrich, Jessica. "Steganography in Digital Media: Principles, Algorithms, and Applications."
Katzenbeisser, Stefan, Petitcolas, Fabien A. P. "Information Hiding Techniques for Steganography and Digital Watermarking."
Zhang, Xiaoyu, Wang, Xiaoming. "A Novel Image Steganography Method Based on Mid-Point Transformation."
Alzahrani, A., Alshamrani, O., &Alqaralleh, B. (2018). Enhanced Steganography Using Midpoint Transformation for Improved Data Embedding Capacity and Image Quality. Journal of Information Security, 9(2), 67-77.
Kaur, Manpreet, Kaur, Mandeep. "A Study of Spatial Domain Techniques in Image Steganography."
Patel, Dhaval, Patel, Bhavesh. "Image Steganography: A Survey of Techniques and Applications."
Singh, Gurjot, Kaur, Harpreet. "Advances in Discrete Cosine Transform Techniques for Image Steganography."