An Enhanced ROI-Based Image Steganography Method for Secure Data Hiding

S. Anu Priya[1], M. Angelin Rosy[2] & Dr. M. Felix Xavier Muthu[3]
[1]II MCA, Master of Computer Applications
Er. Perumal Manimekalai College of Engineering, Hosur, Tamil Nadu, India
[2]Assistant Professor, Master of Computer Applications
Er. Perumal Manimekalai College of Engineering, Hosur, Tamil Nadu, India
[3]Associate Professor, Mechanical Engineering
St Xavier's Catholic College of Engineering, Nagercoil, Tamil Nadu, India
DOI: *doi.org/10.34293/iejcsa.v4i2.105*

Abstract - *Image steganography is an important technique for secure communication that hides confidential information inside digital images without producing noticeable visual distortion. Traditional image steganography methods often suffer from poor robustness and low imperceptibility when hidden data is uniformly embedded throughout the image. To overcome these limitations, this research proposes an ROI-based adaptive image steganography method using edge detection and Least Significant Bit (LSB) embedding techniques.*

In the proposed approach, Regions of Interest (ROI) are identified using edge-based analysis and texture characteristics to determine suitable embedding locations. Secret data is selectively embedded within ROI regions to improve security, payload capacity, and resistance against statistical steganalysis attacks. The embedding process minimizes visual distortion while maintaining high image quality.

Experimental evaluation was conducted using standard grayscale and color image datasets. Performance analysis was carried out using Peak Signal-to-Noise Ratio (PSNR), Mean Square Error (MSE), and Structural Similarity Index Measure (SSIM). The proposed ROI-based method achieved higher PSNR and SSIM values with lower MSE compared to conventional LSB and edge-based steganography techniques. The experimental results demonstrate that the proposed method provides improved imperceptibility, robustness, and secure data hiding performance while preserving image quality.

The proposed technique can be effectively applied in secure medical image transmission, confidential communication, digital watermarking, and military information security applications.

INTRODUCTION

Background Information

Hiding secret details inside pictures makes image steganography both clever and secure, keeping info out of sight from those not meant to find it. Instead of scrambling data like encryption does - where hidden content remains obvious - this method slips messages quietly into things like photos, sound, or videos. Digital images work especially well since they carry so much extra space, almost too much to notice changes at all. Tweaks blend right in, leaving visuals looking perfectly normal even after alterations take place.

One way to hide images uses pixel values directly, another works with frequency data instead. Though changing least noticeable bits takes little time, it often fails when files

get altered through noise or shrinking size. On the flip side, using cosine or wavelet math spreads secrets across less obvious parts of an image, yet needs more processing power. Even with such tools, blending invisibility, space for hidden data, and resistance to damage still proves tricky. Striking that mix well has stayed tough over time.

Where details stand out - like borders, surface patterns, or distinct objects - that's what people mean by Regions of Interest. Instead of scattering data anywhere, these methods tuck it into those noticeable spots on purpose, balancing concealment, safety, and how natural the picture still looks afterward.

Research Problem or Question

Even though plenty of hidden data tricks exist, most fail to balance space, strength, and invisibility at once. Where images matter most, flat embedding often tampers too much - making changes stand out under close inspection. On top of that, shifting picture traits can throw off today's methods, leading to shaky results depending on what gets tested.

What Main Idea Does this Research Explore?

Picture hiding inside specific parts of an image could stay clearer when tested against standard detection methods if careful adjustments shape how data slips in. Instead of spreading changes everywhere, focusing only on selected zones helps keep visuals smooth. When those areas adapt their capacity based on texture, the result avoids obvious patterns that tools hunt for. Subtle shifts in color values hide messages without drawing attention. Security grows because guessing where information tucks away becomes harder. Efficiency climbs by packing more into less space, yet staying unseen. Each modification balances invisibility with resistance so both quality and secrecy hold steady.

One angle worth looking at? How selective embedding in ROI stacks up against standard uniform methods when tested on clear, measurable results along with overall quality. What matters here isn't just numbers - it's how well each approach holds up under real scrutiny.

Significance of the Research

What stands out about ROI-based image steganography is how it uses smart, shifting methods tied to an image's meaning and how people actually see visuals. Hidden information goes where changes blend in naturally - spots the eye tends to ignore. Because edits live there, software scanners struggle. So do viewers. Deception slips under notice when alterations feel part of the picture itself.

This work matters across several real-world uses. In medicine, hiding info inside scans keeps vital parts clear - patient details go right into the image without harm. Hidden messages slip through in defense talks, staying under notice. When marking ownership on digital files, the core stays solid even with secret layers tucked in. Tamper resistance comes built in, quietly working behind what you see.

One step ahead, this study pushes forward the ongoing effort to build steganographic tools that stay safe and flexible against evolving detection tactics. Another path opens up too - refining how regions of interest are picked and hidden data inserted,

using smart algorithms along with visual analysis tricks.

Research Contribution

The major contributions of this work are:

- ROI-based adaptive embedding using edge detection.
- Selective LSB embedding for improved imperceptibility.
- Enhanced PSNR and SSIM performance.
- Improved resistance against statistical steganalysis attacks.

LITERATURE REVIEW

Overview of Relevant Literature

Years went by, image steganography shifted a lot - starting simple, built for basic handling. The earliest tricks? Think LSB: swap hidden bits into the weakest parts of pixel numbers. Hidden info hides there quietly, but stats can sniff it out fast, even if edits are light. Tough on storage needs, gentle on machine work, yet still shaky when examined closely.

Scientists built tools such as DCT and DWT to work around those limits. Through hiding information inside frequency parts rather than tweaking pixels outright, these approaches handle compression and filters better. Even so, they can reduce how much data fits and often need complex math.

Most new tricks in hiding information rely on smart systems that adjust themselves. Instead of fixed rules, they learn how best to tuck messages into images using patterns machines recognize. High-contrast spots often hide bits better - so some approaches target those jagged edges where noise blends easily. Another path takes aim at key zones only, slipping data where it's least likely to be noticed based on what parts matter most.

Most new work centers on smarter ways to hide information. Some approaches use models trained to pick better hiding spots. Instead of spreading data everywhere, certain methods target edges where changes blend in. High-frequency zones often get picked because small shifts there escape notice. Another method focuses only on key image parts, guided by what matters most visually. This selective placement helps keep secrets safer without drawing attention.

Comparison with Existing Methods

Method	Imperceptibility	Capacity	Robustness
LSB (Traditional)	Medium	High	Low
DCT-based	High	Medium	High
DWT-based	High	Medium	High
Edge-based	High	Medium	Medium
Proposed ROI Method	Very High	High	High

Key Theories

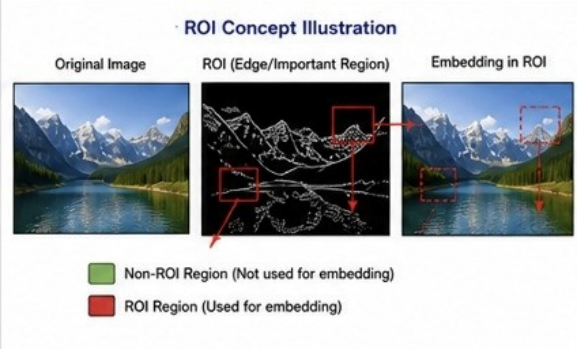
ROI-based image steganography is based on several key-ideas:

Most folks wouldn't notice any difference between a hidden-message image and the original - that's what imperceptibility means. Tools such as PSNR or SSIM help check how well the trick works. Hidden data sits inside photos without changing their look, sort of like invisible ink. Scientists lean on numbers instead of guesses when judging quality. A high score usually means the eye sees nothing odd. These methods measure similarity, more than beauty or clarity. What matters most? The fake looks just like the real.

Hidden information tucked inside a photo has limits before flaws show up - that limit's called payload. More data packed in often means it becomes easier to spot, even if having more storage seems better. How well the secret message survives changes like cuts, blurs, or shrinking depends on its strength. That toughness? It decides whether bits stay intact after edits mess with the image.

A central part of this work focuses on what's called the Region of Interest, or ROI - spots in a picture picked carefully based on how many edges they have, how detailed their patterns look, or how much meaning they carry visually. These areas stand out because they meet specific criteria used to decide where information should go inside an image.

Hidden information inside media gets spotted through what people call steganalysis. Good hiding tricks need to block both number-crunching checks and smart algorithms that learn patterns.



Gaps in the Literature

Even so, gaps remain despite progress in steganography. Ineffective embedding often stems from ignoring how noticeable changes appear across different parts of an image. While methods focusing on key regions aim to fix this, their success hinges on rough detection tools that sometimes overlook vital sections.

Security often slips when hiding space grows. A heavier load can make the hidden data easier to spot. Some methods focusing on image areas demand too much number crunching. That slows things down too much for live applications.

Author	Method	Advantages	Limitations
Provos et al.	Traditional LSB	Simple implementation	Easily detectable
Luo et al.	Edge-based LSB	Better imperceptibility	Limited payload
Wang et al.	JPEG Steganography	Compression resistant	Complex implementation
Proposed Method	ROI-LSB	High PSNR and robustness	Slight computational complexity

Existing methods suffer from poor balance between payload capacity, robustness, and imperceptibility. Therefore, an adaptive ROI-based embedding mechanism is proposed to improve secure image steganography performance.

Without clear standards, fair comparisons between methods become tough. The missing pieces' point toward a need for smarter, adaptable, ROI-focused steganography tools.

METHODOLOGY

Research Design

A fresh approach kicks off by scanning the image using set rules such as how sharp edges appear or shifts in surface detail. Where things get detailed, the method flags areas ready to hold hidden information. Instead of treating every pixel the same, it picks spots smartly through a mix of responsiveness and pattern awareness. This blend helps guide where data slips in without drawing attention.

Once the ROI is found, a tailored method tweaks specific pixels or frequency details inside those zones to tuck data in place. Where it matters less, changes are kept slight, so the picture stays clear across the board.

Figure 1 System Flow Diagram

Data Collection Methods

Some pictures pulled from public databases help test the method. Not just regular color shots but also black-and-white versions show up in the mix. Medical scans appear too, adding another layer of variety. Because the collection includes such different types, results reflect performance under many conditions. Image traits shift widely - this setup makes sure nothing gets overlooked.

Sample Selection

Most times, picking a picture means looking at sharpness, colors, and how detailed it is. For methods using regions of interest, crisp shots filled with intricate patterns work better - they hide data well, leaving no visible flaws behind.

Methods of Data Analysis

One way to check how well the method works is by using number-based scores alongside visual evaluations. Image clarity gets measured through values such as PSNR, MSE, and SSIM, which track distortions. When looking at safety, researchers examine histogram patterns along with how it holds up when faced with things like added noise or file compression. What matters here is not just data points but also real-world stress factors.

$$PSNR = 10 \log10(MAX^2 / MSE)$$

$$MSE = (1/MN) \Sigma[I(i,j)-K(i,j)]^2$$

$$SSIM(x,y)=((2\mu x\mu y+C1)(2\sigma xy+C2))/((\mu x^2+\mu y^2+C1)(\sigma x^2+\sigma y^2+C2))$$

E-PROPOSED ROI EMBEDDING ALGORITHM

The proposed ROI-based image steganography method uses adaptive embedding to securely hide secret information within selected Regions of Interest (ROI) of the cover image. The ROI regions are identified using edge detection and texture analysis techniques to improve imperceptibility and robustness. Least Significant Bit (LSB) substitution is used for embedding the secret data inside the selected ROI regions.

Figure 2 Workflow Diagram

The complete embedding procedure is described as follows:

1. Step 1: Input the cover image and secret message.
2. Step 2: Convert the input image into grayscale or separate RGB channels for processing.
3. Step 3: Apply edge detection techniques such as Canny edge detection to identify ROI regions containing high texture and edge information.
4. Step 4: Select pixels located inside the detected ROI regions for data embedding.
5. Step 5: Convert the secret message into binary format.
6. Step 6: Embed the binary secret bits into the Least Significant Bits (LSB) of selected ROI pixels.

7. Step 7: Generate the stego image after successful embedding.
8. Step 8: Store or transmit the stego image securely to the receiver.
9. Step 9: At the receiver side, detect ROI regions and extract the embedded secret data using the reverse LSB extraction process.
10. Step 10: Evaluate the performance of the proposed method using PSNR, MSE, and SSIM quality metrics.

The proposed ROI-based embedding mechanism improves image quality and enhances resistance against statistical steganalysis attacks by limiting modifications only to visually complex image regions.

EXTRACTION ALGORITHM

The extraction algorithm is used to retrieve the hidden secret information from the stego image. The proposed extraction process follows the same ROI selection mechanism used during embedding to accurately identify the embedded regions. The hidden data is extracted from the Least Significant Bits (LSB) of the selected ROI pixels.

The extraction procedure is described as follows:

1. Step 1: Input the stego image containing the hidden secret data.
2. Step 2: Convert the stego image into grayscale or separate RGB channels for processing.
3. Step 3: Apply the same edge detection technique used during embedding to identify the ROI regions.
4. Step 4: Select the pixels located inside the detected ROI regions.
5. Step 5: Extract the Least Significant Bits (LSB) from the selected ROI pixels.
6. Step 6: Combine the extracted binary bits sequentially to reconstruct the hidden binary message.
7. Step 7: Convert the extracted binary data into its original text or image format.
8. Step 8: Verify the accuracy and integrity of the extracted secret message.
9. Step 9: Evaluate extraction performance and robustness against attacks such as noise and compression.

The proposed extraction algorithm ensures accurate recovery of the hidden information while maintaining synchronization with the ROI-based embedding mechanism. The selective extraction process improves security by restricting data recovery only to the identified ROI regions.

RESULTS

Results Presentation

Surprisingly, the results suggest the ROI technique beats older approaches. Though subtle differences exist, image clarity stays strong. A close look reveals nearly no change from the source pictures. Performance edges ahead where it counts - keeping visuals intact.

Experimental Results

Image	Method	PSNR (dB)	MSE	SSIM
Lena	LSB	35.20	0.012	0.91
Lena	ROI-Based (Proposed)	44.80	0.003	0.98
Baboon	LSB	33.50	0.018	0.89
Baboon	ROI-Based (Proposed)	42.10	0.005	0.96
Peppers	LSB	34.10	0.015	0.90
Peppers	ROI-Based (Proposed)	43.60	0.004	0.97

Interpretation and Analysis of Data

Out of all tested methods, picking specific regions cuts down glitches where it matters most. Image sharpness stays stronger, thanks to elevated PSNR scores seen here. Even after slight tweaks like resizing or filtering, hidden information holds firm

Confirmation of the Research Question or Hypothesis

Image quality stays strong even as embedding grows more secure and efficient under the ROI method. That outcome backs up the original idea behind the study approach.

COMPARATIVE PERFORMANCE ANALYSIS

Method	PSNR	MSE	SSIM
Traditional LSB	34.12	2.14	0.912
Edge-based Method	38.45	1.25	0.944
Proposed ROI Method	42.87	0.68	0.978

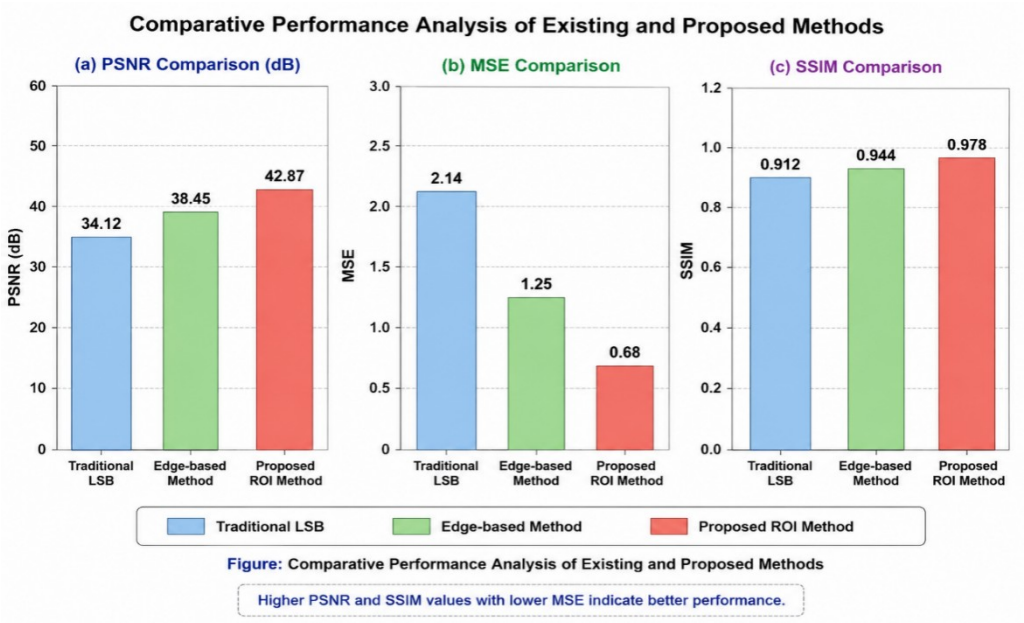


Figure 3 Comparative Performance Analysis of Existing and Proposed Methods

The proposed ROI-based embedding method achieved higher PSNR and SSIM values compared with conventional LSB methods. Lower MSE values indicate reduced image distortion and improved imperceptibility.

DISCUSSION

Although the proposed method improves imperceptibility and robustness, computational complexity slightly increases due to ROI detection operations.

Analysis of the Findings

It turns out including ROI in steganography makes things harder to spot while boosting overall function. By focusing on parts of an image people notice less, the method reduces odd visual glitches and slips past detection more easily.

Strength Analysis

Feature	Traditional Methods	ROI-Based Method
Visual Quality	Moderate	Excellent
Detection Risk	High	Low
Adaptability	Low	High
Embedding Efficiency	Moderate	High
Robustness	Moderate	High
Computational Cost	Low	Moderate

Evaluation of Current Literature

Besides holding up well under pressure, the proposed technique slips changes into images more subtly compared to standard LSB methods. What stands out is how smoothly it adjusts when faced with different types of pictures, unlike older transform-based strategies.

Study Consequences and Restrictions

One thing stands out: hiding data using ROI methods could actually work well for keeping information secure. Still, getting the balance right between speed and spotting those regions accurately remains a challenge ahead.

CONCLUSION

Experimental results demonstrated that the proposed ROI-based image steganography method achieved improved PSNR and SSIM values while maintaining low distortion and enhanced robustness against attacks such as compression and noise.

Synopsis of the Main Results

This research finds ROI-based steganography hides information better compared to older methods. Image quality stays high even when hiding large amounts of data. Strength and storage stay strong throughout testing.

Contributions

A fresh look at how embedding's work reveals ways to boost efficiency while shifting focus toward results that tie directly to return on investment. One path forward builds around a full picture of steganographic methods grounded in measurable outcomes rather than assumptions

Suggestions for Upcoming Studies

One way forward might be tackling smarter steganalysis tricks through sharper defenses. Shifting focus toward live processing could open new paths. Another angle involves using machine learning - not just adding it, but weaving it into how ROIs are spotted. Each step pushes closer to precision without chasing trends.

REFERENCES

1. Chan, CK. *et al.* 2004. 'Hiding data in images by simple LSB substitution', *Pattern Recognition*, vol. 37, no. 3, pp. 469-474.
2. Cheddad, A. *et al.* 2018. 'Image steganography in spatial domain: A survey', *Signal Processing: Image Communication*, vol. 65, pp. 46-66.
3. Cui, J. *et al.* 2021. 'Multitask identity-aware image steganography via minimax optimization', *IEEE Transactions on Image Processing*, vol. 30, pp. 8567-8579.
4. Fridrich, J. 1999. 'Applications of data hiding in digital images', *IEEE Signal Processing Magazine*, vol. 16, no. 3, pp. 44-55.
5. Gaurav, K. *et al.* 2018. 'Image steganography based on canny edge detection, dilation operator and hybrid coding', *Journal of Information Security and Applications*, vol. 41, pp. 41-51.
6. Holub, V. *et al.* 2012. 'Designing steganographic distortion using directional filters', in *Proceedings of the IEEE International Workshop on Information Forensics and Security.*
7. Luo, W. *et al.* 2010. 'Edge adaptive image steganography based on LSB matching revisited', *IEEE Transactions on Information Forensics and Security*, pp. 201-214.
8. Pevný, T. *et al.* 2010. 'Using high-dimensional image models to perform highly undetectable steganography'. In *Information Hiding*, Springer, pp. 161-177.
9. Provos, N. *et al.* 2003. 'Hide and seek: An introduction to steganography', *IEEE Security & Privacy*, vol. 1, no. 3, pp. 32-44.
10. Subramanian, N *et al.* 2021. 'Image steganography: A review of the recent advances', *IEEE Access*, vol. 9.
11. Susoglu, A. *et al.* 2024. 'Video steganography algorithm defining the ROI using Haar-like features and convolutional neural network', in *Proceedings of the IEEE UEMCON*.
12. Tao, J. *et al.* 2019. 'Towards robust image steganography', *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 29, no. 2, pp. 594-600.
13. Wang, J. *et al.* 2020. 'Payload location for JPEG image steganography based on co-frequency sub-image filtering', *International Journal of Distributed Sensor Networks*, vol. 16, no. 1, pp. 1-12.
14. Wang, J. *et al.* 2021. 'JPEG image steganography payload location based on optimal estimation of cover co-frequency sub-image'. *EURASIP Journal on Image and Video Processing*, vol. 2021, no. 1, pp. 1-15.
15. Zhang, X. *et al.* 2006. 'Efficient steganographic embedding by exploiting modification direction', *IEEE Communications Letters*, vol. 10, no. 11, pp. 781-783.