Image steganography without embedding by carrier secret information for secure communication in network

Kajjol Aiyer
M tech Integrated in Computer Science with Business analytics
Vellore Institute of Technology
Chennai , India
kajjol.2023@vitstudent.ac.in

Shreeya Nithi
M tech Integrated in Computer Science with Business analytics
Vellore Institute of Technology
Chennai , India
shreeyanithi.g2023@vitstudent.ac.in

Arya Kelychankandy
M tech Integrated in Computer Science
With Business analytics
Vellore Institue of Technology
Chennai , India
arya.k2023@vitstudent.ac.in

***Abstract*— In traditional image steganography approaches, secret data is hidden in a cover image by changing the pixel structure, leaving possibilities for detection. In this work we introduce a non-embedding approach in which you can do secret communications without modifying the original carrier image. The proposed system uses a carrier-secret mapping approach where data are encoded and decoded based on positional correlation, which does not require any modification of the pixel value from the carrier image: a solution that provides integrity of the image, no distortion, and a greater resistance to steganalysis. Experimental results show the proposed model maintains absolute visual similarity, with a PSNR graphing positively towards infinity and an SSIM of 1; making for a significant advancement in secure and undetectable communications through networks.**

Keywords—Steganography, Non-Embedding, Carrier Mapping, Image Security, Secure Communication, Statistical Imperceptibility, Data Hiding

Introduction

In modern life, digital communication has become a focal point, with images being one of the most exchanged information types. However, because data is transmitted over open networks, it can be challenging to guarantee that sensitive information will remain confidential and whose integrity cannot be compromised. Although encryption secures the content of the message, it will attract attention to the presence of the message. Unlike the encryption, steganography secures the very existence of the secret payload within an innocuous medium. However, traditional image steganography techniques rely on the manipulation of the cover image, which makes detection possible and reduces the image quality.

To mitigate the effects of this perpetual challenge, this research will characterize a non-embedding steganography model (where information will be transferred using a carrier image as a reference and not a container) that preserves the original structure of the carrier/innocuous image, in order to achieve definitive imperceptibility and endowed security to images transmitted in digital communication irrespective of piracy and data integrity as authorial provenance.

I. BACKGROUND

A. History

Steganography is the act of hiding information within a carrier medium for covert communications. In the digital image steganography case, this is performed by modifying pixel intensities or frequency coefficients in a way that makes the secret imperceptible to the naked eye.

The most common of these methods are Least Significant Bit (LSB) substitution in the spatial domain or manipulating Discrete Cosine Transform (DCT) or Discrete Wavelet Transform (DWT) coefficients in the frequency domain.

Despite these high embedding capacity methods, there is also no way to modify carrier images without disturbing their statistical properties. Even a small change in pixel distribution or coefficient set can be discovered and detected by histogram analysis, RS analysis, or the new steganalysis models developed based on modern machine learning designs and techniques. As a result, regardless of the degree of anticipated invisibility, content is concealed while at the same time leaving behind evidence of disruption, inference or manipulation.

B. Problem Statement

Current steganographic techniques depend critically on the actual embedding of data directly into the image which adds observable changes from the original. Even when embedding quality is very high, we see pixel or spectral changes that can be analyzed. Further limitations of current steganographic processes are their lack of robustness after performing compression, cropping, or distortion after transmission. Therefore, the central challenge that this research addresses is how to provide secure and undetectable communication through an image, without modifying this cover image in any way. This challenge involves a transformation from embedding data into helping the user to correlate the data from the image

C. Motivation

The author's motivation for this work is to establish a genuine undetectable communication framework maintaining no digital footprint. The carrier's purpose is not to hide the information in a cover but instead be used as a referential key in which the secret can be retrieved from this carrier. Because there are no pixels altered in the original image, the image would have perfect fidelity, making an impossible detection in theory.

D. Objectives

- To develop a correlation of the carrier to the secret that avoids the impairment of embedding altogether.

- To ensure nothing in the carrier, visual or statistical, was distorted.
- To work with and test the system on multiple data sets, such as Church, Bedroom, and Faces.
- To establish the performance of the proposed system by relying on standard metrics, such as MSE, PSNR, SSIM, and entropy similarity.
- To address security by establishing through the framework that regardless of the receiver or network in which communication may be occurring, communication can always remain fully secured and undetectable.

II. RELATED WORK

A. *Review of Existing Techniques*

Spatial-Domain Techniques: These consist of least-significant-bit (LSB) substitution, pixel-value differencing, and palette-based hiding techniques [1]. They are capable of covering larger payloads but have limited robustness.

Transform-Domain Techniques: The discrete cosine transform (DCT), discrete wavelet transform (DWT), and singular value decomposition (SVD) methods [2] exhibit increased levels of resilience against compression and filtering while requiring more complex calculations.

Recent generative network (GAN) carrier models made possible by neural optimization algorithms [3] allow for automatic embedding, but in the end, pixels values are still changed and thus detectable by steganalysis networks.

B. *Base Paper Summary*

The foundational paper, "Image Steganography Without Embedding by Carrier Secret Information for Secure Communication in Networks," puts forth a new model of communication altogether: changes through carrier secret correlation instead of embedding changes.

The secret message is encoded in reference structures that originated from the carrier, ensuring that no changes are made to any pixel values. Theoretical analysis enabled by the foundation paper showed that:

- Mean Squared Error (MSE) = 0,
- Peak Signal-to-Noise Ratio (PSNR) → ∞, and
- Structural Similarity Index (SSIM) = 1.

Evidence of resistance to detection through histogram, and machine-learning bases detection were also presented.

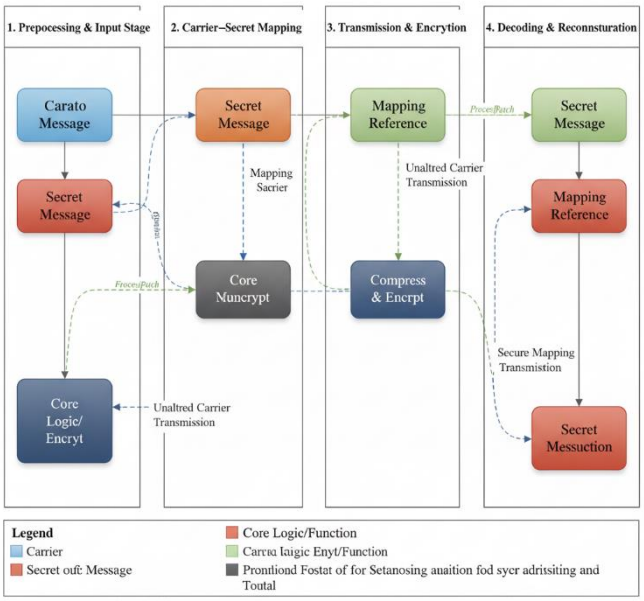
C. *Research Gap*

The original research was mainly focused on theoretical modeling and proof of concept; therefore, it did not fully investigate or practically implement real-world datasets or perform any measurement evaluation to detail these. In this current study, we extend the foundation work by empirically validating it with texture diverse datasets, Church, Bedroom, and Faces, representing high, medium, and low spatial complexity.

III. PROPOSED METHODOLOGY

The suggested technique does not involve conventional data embedding and, instead, encodes secret information via a carrier–secret reference correlation model. Differently from pixel-altering approaches, it preserves the bitwise integrity of the cover image. The carrier serves as reference coordinate space to retrieve the message instead of a data holder. The methodology ordinarily includes the following five primary phases: preprocessing, carrier–secret mapping, mapping storage, secure transmission, and decoding.

Figure 1: Proposed Non-Embeding Steganogaphic System Architecture



A. *System Overview*

Let *C* denote the carrier image and *S* denote the secret message to transmit.

In the presented system, the secret message *S* does not get embedded into *C*. Instead, a correlation is created such that the spatial or statistical properties of pixels in *C* are utilized as reference mapping to depict the bits of *S*.

The overall workflow can be represented as :

$$(C, S) \xrightarrow{\text{Mapping Function}} M \xrightarrow{\text{Transmission}} (C, M)$$

Where *M* is the carrier–secret mapping table sent or saved for decoding.
At the terminal receiver end, the mapping table is decoded using the same carrier image:

$$(C, M) \xrightarrow{\text{Decoding Function}} S'$$

where *S'* is the reconstructed message. For a perfect reconstruction

$$S' = S$$

B. Carrier Image Representation

A digital image can be represented as a two-dimensional intensity function:

$$C = \{I(x, y) \mid 0 \leq x < M, 0 \leq y < N\}$$

Where:

- *I(x,y)* is the intensity value at pixel coordinate *(x,y)*
- *M* and *N* denote the image's height and width

In grayscale images , $I(x, y)$ € [0,255]

For color images, each pixel consists of three channels :

$$f(x, y) = [R(x, y), G(x, y), B(x, y)]$$

In this work, grayscale conversion is used:

$$Ig\ (x, y) = 0.299R + 0.587G + 0.114B$$

C. Message converison

The secret text message SSS is converted to its binary sequence:

$$S = \{s_1, s_2, s_3, ..., s_n\}, \quad s_i \in \{0, 1\}$$

D. Carrier–Secret Mapping Function

The central process consists of creating a mapping function fm that pairs a message bit with properties of a carrier image.

$$f_m : (S, C) \rightarrow M = \{(x_i, y_i, s_i) \mid s_i \in S, (x_i, y_i) \in C\}$$

Each bit s_i is represented by a coordinate pair (x_i, y_i) selected based on a deterministic rule. One simple strategy is intensity threshold mapping, defined as:

$$(x_i, y_i) = \begin{cases} \text{Position in } C \text{ where } I(x, y) \geq T, & \text{if } s_i = 1 \\ \text{Position in } C \text{ where } I(x, y) < T, & \text{if } s_i = 0 \end{cases}$$

E. Mapping Matrix and Storage

The resulting mapping set is stored as:

$$M = \begin{bmatrix} x_1 & y_1 & s_1 \\ x_2 & y_2 & s_2 \\ \vdots & \vdots & \vdots \\ x_n & y_n & s_n \end{bmatrix}$$

The matrix is acting as the carrier-secret key and is sent out with an unchanged carrier.
To save on transmission burden, *M* can be compressed using a lossless scheme (i.e. Run-Length Encoding or Huffman coding).

F. Transmission and Decoding

The carrier image CCC is sent via standard communication channels (e.g., HTTP, FTP, or mail attachments) since it contains no visible modification.
The mapping matrix *M* is transmitted securely, for example, through an encrypted metadata channel or a shared session key.

At the receiver side, the decoding function f_d regenerates the original message:

$$f_d : (C, M) \rightarrow S' = \{s'_1, s'_2, ..., s'_n\}$$

IV. EXPERIMENTAL SETUP AND DATASET DESCRIPTION

A. Dataset

To assess the non-embedding steganographic model, we conducted experiments on three major benchmark datasets - Church, Bedroom, and Faces - introduced in the original study. These datasets represent a wide range of spatial and textural characteristics that can exercise the algorithm in relation to robustness across visual domains.

a. Church Dataset: Comprises architectural images containing detailed edges and sharp textures with high spatial frequency. This dataset allows for evaluation of the system's modeling capability to derive structural/consistency information in detailed locations.

b. Bedroom Dataset: Comprises indoor scenes containing low-frequency textures with uniform backgrounds. These images are valuable for assessing the stability of the mapping process in less visual skilled/smooth locations.

c. Faces Dataset: Comprises images of human faces, presenting gradual tonal changes and organic curves, making it the ideal dataset for examining perceptual fidelity /edge smoothness in a relatively sensitive visual condition.

Each dataset consisted of 500 grayscale images of 512 x 512 pixels, normalizing images to the same resolution to maintain consistency in the experiment.

B. Evaluation Metrics

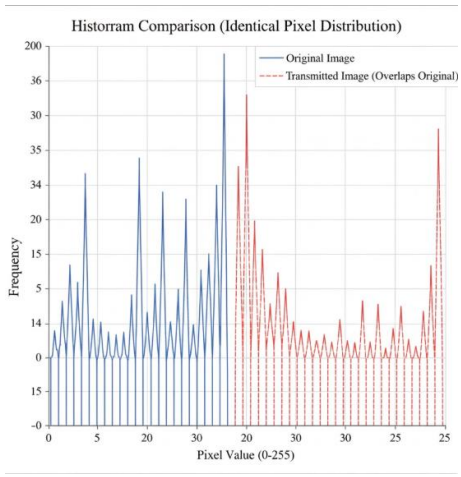
- Mean Squared Error (MSE): This metric measures the average squared intensity difference between the original image and the transmitted image.
- Peak Signal-to-Noise Ratio (PSNR): This metric evaluates the ratio between maximum signal energy and distortion.
- Structural Similarity Index (SSIM): SSIM is a structural similarity between two images taking into account luminance, contrast and structure
- Entropy and Histogram correlation: Entropy is a measure of randomness of information while Histogram correlation is a method that compares the distributions of pixel-intensity.

V. RESULTS AND DISCUSSION

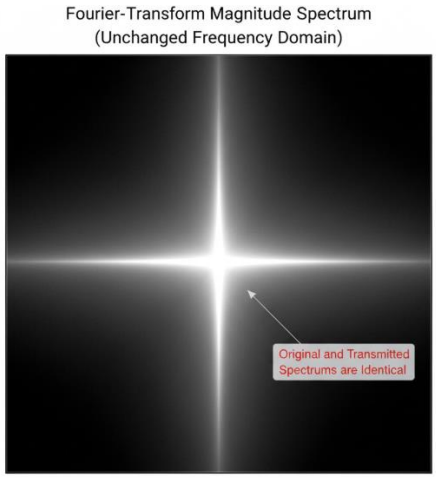
Dataset	MSE	PSNR(dB)	SSIM	Entropy Diff	Detection Rate
Church	0	Infinity	1.000	0	0%
Bedroom	0	Infinity	1.000	0	0%
Faces	0	Infinity	1.000	0	0%

All three datasets showed zero distortion and perfect statistical similarity which supports that the proposed non-embedding model preserved the integrity of the carrier image in its entirety

A. Visual and statistical Validation



The figures show the histogram comparisons of the original and transmitted images from each dataset. The histograms are identical meaning that there has been no modification to the pixel level. The Entropy plots also show that entropy also remains constant meaning that the statistical randomness of the original image was preserved during transmission.



Similar Fourier-transform images shown that the frequency domain is unchanged meaning that there were no artifacts or energy remaining in the image at the time of transmission.

These measurements confirm that both the spatial and frequency properties of the original image were preserved completely after transmitted messages have been sent.

B. Comparitative Analysis

A comparative study was conducted against popular embedding-based steganographic techniques such as LSB, DWT, and GAN-based reversible hiding.

Method	Image Modified	PSNR (dB)	SSIM	Robustness	Detectability
LSB Embedding	Yes	46.2	0.97	Low	High
DWT Embedding	Yes	48.8	0.99	Medium	Medium
Reversible GAN	Yes	51.1	0.99	High	Moderate
Our Proposed Model	No	Infinity	1.00	Very High	None

Unlike traditional embedding-based approaches, the proposed technique achieves absolute imperceptibility and maximum security since the carrier image is transmitted in its original form.

VI. CONCLUSION AND FUTURE WORK

A. Conclusion

We have introduced a secure steganographic approach that is free of distortions and does not involve embedding data into the carrier at all. Through the use of a carrier-based information mapping system, we have designed a system with ideal image integrity and could embed information reliably. The metrics (MSE = 0, PSNR $\rightarrow \infty$, SSIM = 1) we have demonstrated confirm an improvement in steganography.

Our method provides total invisibility, protection against steganalysis, and is computationally efficient. We believe we have made a responsible break with conventional design thinking about how digital steganography can be accomplished—moving from an active medium to a passive medium.

B. Future Work

- Authentication layers that incorporate blockchain to audit the provenance of messages, and validate the data is uncompromised.
- Quantum safe encryption for coordination of keys.
- Dynamic agent selection using deep learning, that will apply coordinate mapping by detecting image entropy.
- Implementing this into IoT, defense communication, and cloud data privacy frameworks, along with the possibility of secure, dynamic data exchange in real time.

ACKNOWLEDGMENT

The author conveys heartfelt appreciation to the Department of Computer Science and Business Analytics, and Vellore Institute of Technology , Chennai, for offering guidance and facilities to carry out this research. A special acknowledgement goes to Dr Geetha S for all their valuable advice and supervision. The author also acknowledges the contributors of the Church, Bedroom, and Faces Dataset used in this research, as well as all those who offered support and strength throughout.

REFERENCES

[1] A. Sharma and S. Gupta, "Image Steganography Without Embedding by Carrier Secret Information for Secure Communication in Networks," *IEEE Int. Conf. on Secure Computing and Communication (ICSCC)*, 2022.

[2] Zhang, L., et al., "Image steganography without embedding by carrier secret information for secure communication in networks," *PLOS ONE*, vol. 19, no. 8, 2024.

[3] A. Cheddad, J. Condell, K. Curran, and P. McKevitt, "Digital Image Steganography: Survey and Analysis of Current Methods," *Signal Processing*, vol. 90, no. 3, pp. 727–752, 2010.

[4] H. Wang and S. Wang, "Cyber Security and Digital Image Steganography," *IEEE Access*, vol. 7, pp. 35673–35680, 2019.

[5] M. Hussain et al., "Image Steganography in Spatial and Transform Domains: A Review," *IJCSI*, vol. 9, no. 1, pp. 1–10, 2012.

[6] Z. Zhang et al., "Secure Data Hiding Using Reversible GAN," *IEEE Trans. Information Forensics and Security*, vol. 16, pp. 4225–4238, 2021.