I. J. Mathematical Sciences and Computing, 2026, 3, 65-80
Published Online on August 8, 2026 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijmsc.2026.03.04

From Pixels to Processes: A Process Mining-Inspired Approach to Image Steganalysis

Shikha Badhani*
Department of Computer Science, Maitreyi College, University of Delhi, India
E-mail: sbadhani@maitreyi.du.ac.in
ORCID iD: https://orcid.org/0000-0002-8535-1808
*Corresponding author

Vinita Verma
Department of Computer Science, Rajdhani College, University of Delhi, Delhi, India
E-mail: vinitaa@rajdhani.du.ac.in
ORCID iD: https://orcid.org/0000-0003-1318-8041

Manju Bhardwaj
Department of Computer Science, Maitreyi College, University of Delhi, India
E-mail: mbhardwaj@maitreyi.du.ac.in
ORCID iD: https://orcid.org/0000-0002-8696-3953

Sakeena Shahid
Department of Computer Science, Sri Guru Tegh Bahadur Khalsa College, University of Delhi, Delhi, India
E-mail: sakeena@sgtbkhalsa.du.ac.in
ORCID iD: https://orcid.org/0009-0003-1596-4742

Geetan Manchanda
Department of Mathematics, Maitreyi College, University of Delhi, India
E-mail: gmanchanda@maitreyi.du.ac.in
ORCID iD: https://orcid.org/0000-0003-0785-4909

Received: February 25, 2026; Revised: April 8, 2026; Accepted: July 12, 2026; Published: August 8, 2026

Abstract: Steganography attempts to conceal messages in plain sight while steganalysis seeks to identify them or, more importantly, to extract the embedded data. Low-payload and spatially localized steganographic embedding is increasingly used to evade detection by classical steganalysis methods. While such strategies preserve global image statistics and remain visually imperceptible, they can disrupt natural pixel-level behavior. This work proposes a behavioral steganalysis framework inspired by process mining that detects image steganography by analyzing localized behavioral deviation using regional behavioral contrast and behavioral amplification. Experiments on lossless grayscale PNG images from the USC SIPI database and 10,000 images from the BOWS2 dataset using 1-bit LSB embedding show that the proposed framework reliably identifies steganographic embedding. On the USC SIPI dataset, conventional statistical detectors, including chi-square analysis and the StegExpose tool, showed limited detection capability under the evaluated localized embedding settings. Despite high perceptual quality of stego images (PSNR > 55 dB), significant behavioral deviation is consistently observed within embedded regions. These results demonstrate that the proposed process mining-inspired framework provides an interpretable and complementary direction for image steganalysis, particularly under low-payload and localized embedding scenarios.

Index Terms: Steganalysis, Process Mining, Behavioral Modeling, LSB Embedding, Digital Image Forensics, Localized Steganography.

1. Introduction

Digital images have become a dominant medium for communication in modern information systems. At the same time, images have increasingly been exploited as covert carriers for hidden communication through steganography [1].

Cryptographic techniques focus on making the content of a hidden message unreadable while steganography seeks to conceal the very existence of hidden message, thereby posing a significant challenge for digital forensics and multimedia security [2,3]. As steganographic techniques continue to evolve toward utilizing lower payloads in carrier images and localized embedding strategies for hiding messages, the development of interpretable steganalysis methods remains an open research problem [4,5].

The early methods of steganalysis were based on visual analysis and global statistical analysis. Histogram comparison, Chi-square analysis, Regular-Singular (RS) analysis, and sample pair analysis were developed to detect the statistical anomalies caused by embedding procedures, especially in LSB-based steganography [6]. Although useful under certain conditions, these methods tend to be inefficient in low payload cases and in their reliance on global statistics of the image [7].

The current state of steganalysis has been pushed forward by machine learning and deep learning methods, which identify characteristic features in labeled samples to provide high detection rates [3,8]. Although effective, these methods also introduce new issues in the forensic analysis process. These methods are highly sensitive to the availability of representative training samples, embedding models, and payload assumptions. Additionally, the decision-making process of these models is not transparent, providing little information on why an image is identified as steganographic.

Concurrently, a useful paradigm for analyzing behavioral phenomena in event-driven systems is process mining. Process mining is a data-driven technique that analyzes event logs to reconstruct and visualize the actual behavior of processes [9]. It has been successfully applied in areas such as business process analysis, healthcare, and security monitoring, including anomaly detection using behavioral deviation [10,11]. However, process mining has not been investigated in the context of image steganalysis.

The motivation of this research lies in visualizing the pixel-level activity in digital images, particularly at the LSB level, as a behavioral process. Steganographic embedding introduces transition pattern changes and artificial regularity, which disrupts the natural behavior of pixel groups. Based on this observation, this research work proposes a framework for steganalysis that models, compares, and measures pixel-level behavior in clean and stego images based on process mining principles.

The main contributions of this work are summarized as follows:

- A new approach to image steganalysis is proposed in this research, where the LSB activity at the pixel level is modeled as a behavioral process. A systematic approach is developed to transform images into event logs. The approach uses behavioral analysis to detect the anomalies caused by steganographic embedding.
- The approach clearly identifies the differences in behavioral patterns between the embedded area and the non-embedded background of the same image. Unlike supervised learning approaches, the proposed framework does not require labeled training data or pretrained models. Clean images are used solely for experimental validation.
- The idea of behavioral amplification is developed to quantify the impact of embedding relative to the natural variability in images. This approach eliminates the need for fixed thresholds or general statistical models.
- Experiments were carried out on lossless grayscale PNG images from the USC SIPI Image Database and an additional set of 10,000 images from the BOWS2 dataset with localized 1-bit LSB embedding.

2. Background

In this section, we review existing literature on image steganalysis and place the proposed framework within the broader research landscape.

2.1. Image Steganalysis

Early research in image steganalysis was based on visual inspection, histogram analysis, and statistical tests in order to detect the anomalies introduced due to embedding. A seminal contribution by Westfeld and Pfitzmann [12] introduced the chi-square attack, which detects irregularities in the distribution of LSBs. Shortly thereafter, Fridrich et al. [13] proposed RS analysis, which evaluates changes in pixel smoothness under controlled LSB flipping to estimate both the presence and approximate payload of hidden data. Related techniques, including sample pair analysis and optimization-based strategies, further exploited inter-pixel dependencies to enhance detection reliability [14]. These statistical methods established the foundation of image steganalysis by exploiting changes in global image statistics. However, their effectiveness decreases for low-payload, localized, or adaptive embedding schemes, where embedding introduces only subtle changes to the overall statistical characteristics of the image [3,7].

To better capture dependencies between neighboring pixels, researchers explored Markov-based steganalysis, where transitions between neighboring pixel values or image residuals are modeled using Markov chains. Sullivan et al. [15] demonstrated that Markov transition statistics provide a richer representation of image structure than global statistical measures, while later studies further extended these ideas for image steganalysis [16]. Although these methods improved detection performance, they primarily rely on transition probabilities as statistical features and do not explicitly model or interpret pixel behavior at the regional level.

To address these limitations, machine learning-based steganalysis emerged. Rather than relying on single statistical tests, these methods extract high-dimensional representations that capture subtle spatial dependencies within images. The Subtractive Pixel Adjacency Matrix (SPAM) and the Spatial Rich Model (SRM) represent notable milestones in this direction, which are often combined with SVMs or ensemble classifiers [17,18]. By modeling richer spatial relationships, these approaches significantly improved detection performance, particularly for moderate embedding payloads. However, their effectiveness depends on the extracted features, whose discriminative capability may vary across embedding algorithms and payload settings.

The success of machine learning-based methods subsequently motivated the adoption of deep learning techniques, which automatically learn discriminative representations directly from image data. Convolutional neural networks (CNNs), introduced to this domain by Qian et al. [19], demonstrated the feasibility of learning discriminative representations directly from image data without handcrafted features. Subsequent architectures, including SRNet and residual-based CNN variants, have achieved state-of-the-art performance across diverse embedding algorithms and payload settings [20,21]. More recently, deep learning-based steganalysis has continued to evolve through entropy-guided feature learning, multi-scale residual networks, and dual-path feature enhancement, enabling improved feature extraction and robustness against increasingly sophisticated embedding schemes [22]. These methods have further advanced detection accuracy, particularly for adaptive steganographic techniques.

Recent studies explore hybrid models that incorporate attention mechanisms and graph-based representations to understand complex pixel relationships [25,26]. Although these approaches continue to improve detection accuracy, they generally rely on large labeled datasets and considerable computational resources, while offering limited interpretability of the learned decision process.

2.2. Behavioral Perspectives and Process Mining

Natural images are characterized by strong spatial dependencies due to spatial correlation, texture, and image acquisition methods. However, embedding information through steganography disrupts these dependencies. Consequently, this disruption leads to steganalysis techniques that examine relationships between pixels rather than focusing on isolated statistics [13,14]. However, most of the steganalysis methods still consider images as fixed objects defined by global distributions or feature vectors. They primarily summarize statistical properties without explicitly modeling how pixel-level behavior evolves across spatial positions. At the same time, process mining has become an effective approach for discovering, analyzing, and monitoring behavioral patterns in event-driven systems. By modeling systems as sequences of events organized as cases and activities, process mining helps to identify structural patterns, deviations, and anomalies [9]. It has been successfully applied in business process analysis, healthcare workflows, and security monitoring, including identifying anomalies based on behavioral changes [10,11]. These use cases demonstrate how process mining can reveal subtle behavioral shifts that static statistical summaries might overlook.

2.3. Positioning of the Present Work

The present study introduces a behavioral steganalysis framework based on process mining principles. Unlike classical statistical methods that rely on global distributional assumptions, and unlike learning-based approaches that depend on training data and black-box decision models, the proposed method models pixel-level LSB activity as an event-driven process. It quantifies the behavioral changes caused by steganographic embedding through a comparative regional analysis. This leads to the idea of behavioral amplification compared to natural image variability. By offering an understandable, region-aware, and training-free perspective, the proposed method enhances existing steganalysis techniques and addresses key limitations of prior work. Although the proposed framework is based on LSB transition information, it is fundamentally different from conventional Markov-based steganalysis. Markov-based methods directly model transition probabilities as statistical features for detection, whereas the proposed framework uses transition information only as an intermediate representation for behavioral modeling. By organizing pixel transitions into event traces and deriving interpretable behavioral measures, the proposed approach provides a process mining-inspired perspective for analyzing localized steganographic embedding.

3. Methodology

This section presents the proposed process mining-inspired steganalysis framework for detecting steganographic embedding through the analysis of behavioral deviations in image regions.

3.1. Overview of the Proposed Framework

The core idea behind the present study is to compare regional behavioral patterns between clean and stego images and quantify how embedding amplifies behavioral deviation beyond what naturally occurs in an image. The architecture of the proposed steganalysis framework is illustrated in Fig. 1.

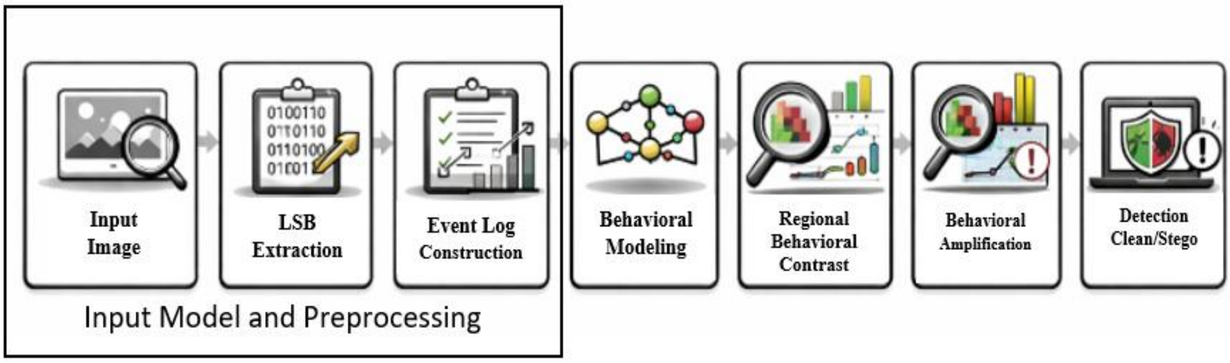


Fig. 1. Proposed Steganalysis Framework.

3.2. Image Model and Preprocessing

Let an input grayscale image I of size $M \times N$ be denoted using (1) as follows:

$$I \in \{0,1,\dots,255\}^{M\times N} \tag{1}$$

Each pixel intensity $I(x,y)$ is represented using 8-bit binary encoding. The LSB plane is extracted using (2). The binary plane obtained forms the basis for behavioral analysis.

$$LSB(x,y) = I(x,y) mod 2 \tag{2}$$

For controlled evaluation, steganographic embedding is performed by replacing the LSBs within a localized region of interest (ROI) with the most significant bits of a secret image. Outside the ROI, in the region referred as background, the pixel values remain unmodified.

Event Log Construction

In order to map process mining to steganalysis, the input image is transformed into an event log by interpreting pixel-level behavior as event-driven activity as discussed below:

CaseID

In process mining, a case corresponds to an individual process instance. In the proposed framework, pixels are grouped into cases based on their intensity proximity in order to capture consistent behavioral patterns. Thus, the case identifier c for a pixel at position (x,y) is defined using (3) as provided.

$$c = \lfloor\frac{I(x,y)}{2}\rfloor \tag{3}$$

This equation groups together the pixels that differ only in their least significant bit, thereby ensuring that each case represents a stable pixel intensity baseline while allowing LSB variations to be observed as behavioral changes. Thus, the pixels that differ only in LSB get the same case ID. Therefore, the case definition isolates the bit-level behavior from visual content behavior.

Activity

Every pixel generates an activity defined by its LSB. The activity space consists of two activities, LSB0 and LSB1, corresponding to LSB values of 0 and 1, respectively, as defined in (4). This binary activity encoding captures the fundamental unit of behavior induced by LSB-based steganographic embedding. Different pixel values can produce the same activity.

$$a \in \{LSB_0, LSB_1\} \tag{4}$$

Trace Construction

A trace in process mining shows a sequence of activities linked to one case. In the proposed model, traces are formed by arranging pixel activities based on a set path through the image, such as scanning row by row or column by column. Unless otherwise specified, traces are constructed using a row-wise raster scan (left-to-right and top-to-bottom), ensuring a consistent traversal order for all images throughout the experiments. For a given case c, the trace is defined by (5), where each $a_i \in \{LSB_0, LSB_1\}$ corresponds to the LSB activity of a pixel assigned to case c encountered during traversal.

$$T_c = \langle a_1, a_2, \dots, a_k \rangle \tag{5}$$

Each pixel thus contributes an event $e = (c, a)$, and the complete image is represented as a collection of traces $\{T_c\}$ forming a structured event log. This representation allows the use of process mining techniques to analyze LSB behavior in terms of persistence, alternation, and transition dynamics, as described in subsequent sections. This enables the detection of deviations introduced by steganographic embedding.

Fig. 2 illustrates the construction of event traces from a 2×2 grayscale image, showing the mapping from pixel intensities to cases, activities, and traces.

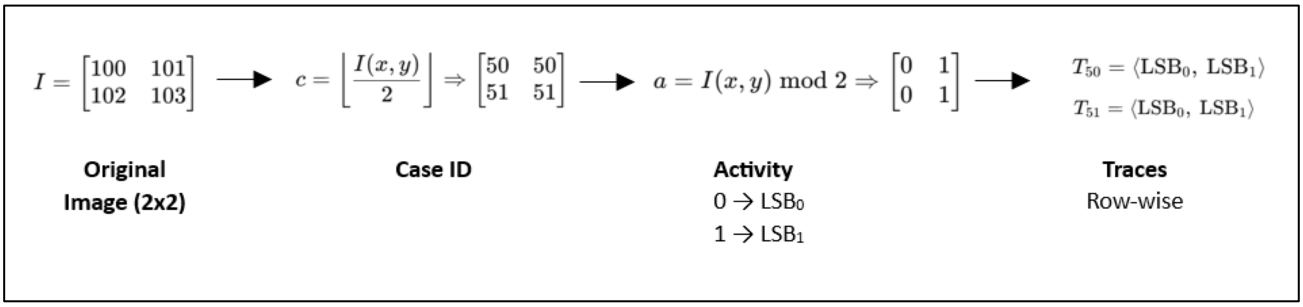


Fig. 2. Illustration of an Event-Log Construction from a 2×2 Grayscale Image.

3.3. Behavioral Modeling

Following the construction of event log, the next step is to model the behavioral structure of LSB activities across traces. In process mining, behavioral modeling focuses on the order and frequency of activities within traces. It captures how execution behavior changes rather than relying on static summaries [9].

Every trace T_c as defined in (5) represents the ordered sequence of LSB activities observed for pixels grouped under the same intensity-based case c. Since the activity space is binary consisting of $\{LSB_0, LSB_1\}$, only four possible relations can occur between consecutive activities as shown in (6).

$$LSB_0 \rightarrow LSB_0, LSB_0 \rightarrow LSB_1, LSB_1 \rightarrow LSB_0, LSB_1 \rightarrow LSB_1 \tag{6}$$

These relations correspond to two basic behavioral patterns: persistence, which reflects the stability in LSB values, and alternation which reflects the switching behavior between LSB values. These relations form the basis of behavioral modeling in process mining and help characterize regularity and deviation in execution behavior [27].

To obtain a global behavioral representation of the image, transition frequencies are aggregated across all traces, resulting in the transition matrix as given by (7), where f_{ij} denotes the number of occurrences of the transition $LSB_i \rightarrow LSB_j$. This matrix is similar to the graph representation often used in process mining [9].

$$M = \begin{bmatrix} f_{00} & f_{01} \\ f_{10} & f_{11} \end{bmatrix} \tag{7}$$

While the matrix captures complete behavioral information, raw frequencies depend on image size and pixel distribution. For meaningful comparison across images, normalized behavioral metrics are derived from this matrix. These metrics are calculated to quantify LSB dynamics in a clear and interpretable manner. Similar normalization strategies are commonly used in process mining–based anomaly detection to compare behavioral patterns across logs of different sizes [10].

The **persistence ratio**, which measures the tendency of LSB values to remain unchanged, is defined using (8) given below.:

$$P = \frac{f_{00} + f_{11}}{\sum_{i,j} f_{ij}} \tag{8}$$

The **alternation ratio**, which measures the degree of switching between LSB values, is computed using (9) given below.

$$A = \frac{f_{01} + f_{10}}{\sum_{i,j} f_{ij}} \tag{9}$$

These metrics summarize the behavioral characteristics of LSB evolution without relying on absolute pixel counts. Natural images exhibit strong local dependencies, which leads to higher persistence and lower alternation. In contrast, LSB-based steganographic embedding disrupts these dependencies and exhibits increasing alternation while preserving a statistically balanced global LSB distribution.

3.4. Regional Behavioral Contrast

While the behavioral metrics defined in Section 3.3 summarize global LSB dynamics, natural images are complex. They are inherently heterogeneous and exhibit local variations due to texture, edges, and illumination. Such variability can hide effects introduced due to embedding if only global measures are considered. To address this, we use a regional behavioral comparison strategy. This approach is consistent with localized steganalysis approaches reported in the literature [13].

The image is partitioned into two disjoint regions:

- **Region of Interest (ROI):** the embedded or suspected region,
- **Background (BG):** the remaining non-embedded region.

Behavioral metrics are computed independently for each region. Regional behavioral contrast is defined as the absolute difference between corresponding metrics as given in (10), where P denotes the persistence ratio and A denotes the alternation ratio.

$$\Delta B = \mid BROI - BBG \mid, B \in \{P, A\} \tag{10}$$

This contrast indicates the deviation in behavior within an image, capturing how LSB dynamics in the ROI differ from the natural baseline as seen in the background. In clean images, these contrasts are expected to be small because both regions tend to have similar pixel dependency structures. However, localized LSB steganographic embedding disrupts these dependencies, causing an increase in the behavioral contrast between ROI and BG. Previous studies have shown that similar region-based comparative methods can enhance sensitivity in steganalysis, especially for localized or low-payload embedding [28].

3.5. Behavioral Amplification

Although regional behavioral contrast highlights localized deviations, its absolute magnitude may still depend on image content and texture complexity. To separate embedding effects from inherent natural variability, a behavioral amplification measure is introduced.

Let ΔB_{stego} and ΔB_{clean} represent the regional behavioral contrasts calculated for stego and clean images, respectively. Behavioral amplification Γ_B is calculated using (11), where ε is a small constant added to for numerical stability. In the present study, ε was empirically set to 10^{-9}, which is sufficiently small to avoid division-by-zero and numerical instability.

$$\Gamma_B = \frac{\Delta B_{stego} + \varepsilon}{\Delta B_{clean} + \varepsilon}, B \in \{P, A\} \tag{11}$$

In this study, the clean image is used solely to establish a controlled baseline for quantifying embedding-induced behavioral deviation and validating the proposed framework.

The behavioral amplification Γ_B measures the relative rise in behavioral deviation caused by embedding, adjusted for natural variability within images. Similar normalization methods are often used in process mining-based anomaly detection to separate abnormal behavior from background noise [9,10].

3.6. Detection Rule

Presence of steganography in an image is detected by evaluating absolute regional contrast and relative behavioral amplification together. An image is identified as stego when it meets these conditions:

1. The stego contrast is much higher than the clean contrast. This shows that embedding has changed the LSB transition behavior more than natural variation does.
2. The behavioral amplification must be greater than what is normally expected from the image's inherent variability.

4. Implementation Details

All experiments have been implemented in Python 3.x using the following Python libraries: NumPy and Pillow for image processing, SciPy for statistical analysis, and Matplotlib for visualization. All images are processed in 8-bit grayscale format.

4.1. Dataset and Preprocessing

Experiments were conducted on two publicly available benchmark datasets: the USC SIPI Image Database (http://sipi.usc.edu/database/) and the BOWS2 dataset [29,30]. The USC SIPI dataset consists of grayscale PNG images of size 512 × 512 and includes widely used standard test images such as *Aerial, Airplane, Boat.512, Car and APCs, Couple, Gray21.512, Stream and Bridge, Tank, Truck, and Truck and APCs,* which exhibit varied texture, structural complexity, and intensity distributions and are commonly employed in image processing research. To further evaluate the generalizability of the proposed framework, additional experiments were conducted on the BOWS2 dataset, comprising 10,000 grayscale images resized to 512 × 512 pixels. The secret image, used for embedding, is also obtained from the same SIPI database, a grayscale PNG image (the *Moon* image) of size 256×256 pixels. Prior to processing, all images are converted to unsigned 8-bit integer format.

4.2. Steganographic Embedding and Payload Control

Steganographic embedding has been performed using 1-bit LSB replacement within a square region of interest (ROI) located at the top-left corner of the image. Only pixels inside the ROI are modified, while pixels outside in the background region remained unchanged. The payload size is controlled by varying the ROI dimensions. Specifically, three ROI sizes are used:

- (64 x 64) pixels (4096 embedded pixels),
- (128 x128) pixels (16384 embedded pixels),
- (256 x 256) pixels (65536 embedded pixels).

For a given ROI size (h, w), embedding is performed as given in (12):

$$I_{stego}(x,y) = (I_{cover}(x,y) \wedge 254) \vee MSB_{secret}(x,y), 0 \le x < h, 0 \le y < w \tag{12}$$

where the most significant bit (MSB) of the secret image has been embedded into the least significant bit (LSB) of the cover image. This approach simulates low-payload, localized embedding, which is known to be difficult to detect.

5. Results and Discussion

This section presents the experimental evaluation of the proposed framework. The USC SIPI image database is first used for detailed qualitative and quantitative analysis of the proposed behavioral measures. Subsequently, large-scale validation is performed on the BOWS2 dataset comprising 10,000 grayscale images to evaluate the robustness and generalizability of the framework. For each cover image, localized steganographic embedding is performed using 1-bit LSB replacement within a square region of interest (ROI), while pixels outside the ROI remained unmodified. All experiments have been conducted under identical conditions across the dataset to ensure fair and consistent evaluation. The results obtained are discussed next.

5.1. Visual Analysis and Embedding Verification

Visual analysis of images verifies the perceptually indistinguishable behavior obtained between the stego images and their corresponding cover images. No visible artifacts or structural distortions have been observed in any of the stego images, even under close examination. The cover and stego images are shown in Table 1.

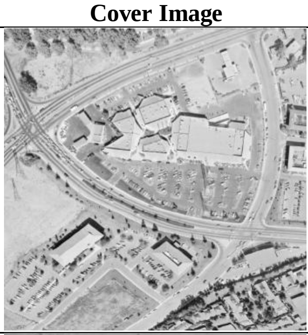
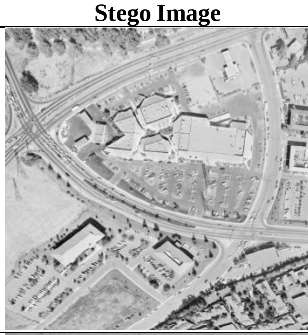
This qualitative observation is supported by Peak Signal-to-Noise Ratio (PSNR) which measures the quality of stego image S compared to its original or cover image C. It is calculated using (14), where MSE, the mean squared error between images has been computed using (13), and MAX refers to the highest possible pixel value in Image I, such as 255 for 8-bit images.

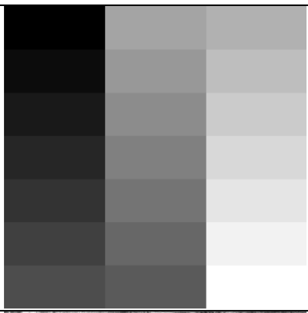
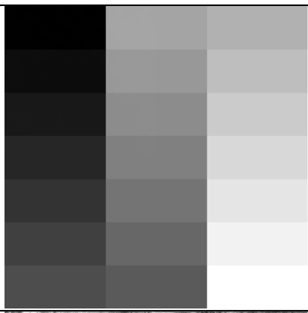
$$MSE = \frac{1}{MxN} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (C(i,j) - S(i,j))^2 \tag{13}$$

$$PSNR = 20. log_{10} \frac{MAX_I}{MSE} \tag{14}$$

Our analysis showed high PSNR values that consistently exceeded 55 dB across the dataset. This finding indicates that the embedding process caused very little visual distortion. Table 1 shows the results. The results confirm that the proposed embedding strategy keeps perceptual quality intact, and any detected anomalies are not due to visible image degradation.

Table 1. Cover and Stego Images and the Corresponding PSNR Values.

Image	Cover Image	Stego Image	PSNR (dB)
Aerial			57.16
Airplane			57.30
Boat.512			57.20
Car and APCs			57.15
Couple			57.18

Gray21.512			56.10
Stream and Bridge			57.00
Tank			57.28
Truck			57.09
Truck and APCs			57.15

To further check the location of embedding, the LSB maps and LSB difference maps were examined. While the stego images looked visually the same as the cover images, the LSB maps showed slight changes at the bit level. The LSB difference maps clearly pinpointed these changes to the predefined ROI. This confirms that pixel changes were limited to the intended embedding area and that no unintended changes happened elsewhere in the image.

Representative examples of the clean and stego LSB maps, and the LSB difference map are illustrated in Fig. 3. These visualizations demonstrate that, although embedding remains imperceptible at the image level, it introduces structured changes at the LSB level that are later captured by the proposed behavioral analysis.

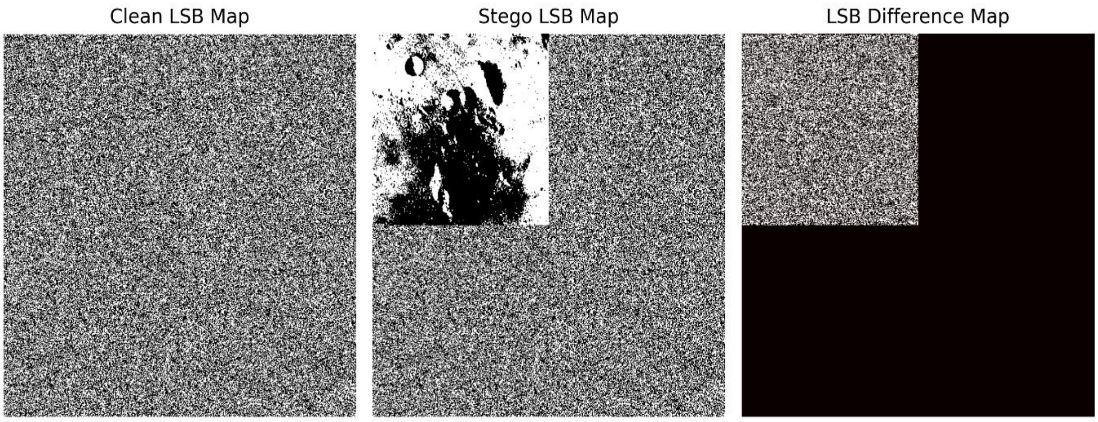


Fig. 3. LSB Difference Map for the Aerial Image.

5.2. Regional Behavioral Contrast

Table 2 reports the regional behavioral contrast for clean and stego images in terms of persistence P and alternation A metrics. These metrics are calculated using (8) and (9) respectively.

Table 2. Regional Behavioral Contrast on SIPI PNG Images.

Image	Clean Contrast (P/A)	Stego Contrast (P/A)
Aerial	0.0011	0.1822
Airplane	0.0007	0.1721
Boat.512	0.0007	0.2222
Car and APCs	0.1376	0.1668
Couple	0.0011	0.2187
Gray21.512	0.0000	0.1334
Stream and Bridge	0.0000	0.2678
Tank	0.0513	0.1267
Truck	0.1682	0.0967
Truck and APCs	0.0545	0.0458

Across the dataset, images such as *Couple*, *Aerial*, *Airplane*, and *Boat.512* exhibit very low clean contrast (≈ 0.0007–0.0011), indicating stable baseline LSB transition behavior. After embedding, contrast increases substantially (≈ 0.17–0.22), reflecting measurable deviation in transition structure. This suggests that embedding introduces systematic changes in local LSB dynamics in images with stable natural behavior. *Tank* also shows higher stego contrast as compared to clean contrast.

Similarly, *Gray21.512* and *Stream and Bridge* show nearly zero clean contrast and non-zero stego contrast (0.133-0.268). This further confirms that embedding disrupts consistent LSB transition patterns. In contrast, *Truck*, *Truck and APCs,* and *Car and APCs* have relatively higher clean contrast (approximately 0.05 to 0.16). This suggests greater intrinsic LSB variability, likely due to texture complexity. In these cases, the absolute difference between clean and stego contrast is smaller. This indicates that the changes caused by embedding compete with natural random variation. These results show that behavioral contrast effectively captures the changes caused by embedding, especially in images with stable baseline LSB dynamics.

5.3. Behavioral Amplification

To normalize the differences caused by embeddings compared to natural image variability, we calculated behavioral amplification using (11). The results are shown in Table 3.

Table 3. Behavioral Amplification on SIPI Images.

Image	Behavioral Amplification (Γ_B)
Aerial	163.26
Airplane	238.85
Boat.512	322.13
Car and APCs	1.21
Couple	205.96
Gray21.512	1.33×10^{8}
Stream and Bridge	2.68×10^{8}
Tank	2.47
Truck	0.6
Truck and APCs	0.84

As shown in Table 3, structurally stable images show strong behavioral amplification. Images like *Couple*, *Aerial*, *Airplane*, and *Boat.512* demonstrate behavioral amplification ranging from 163× to 322×. This indicates that embedding substantially increases behavioral deviation compared to the baseline.

Extremely large behavioral amplification values are observed for *Gray21.512* and *Stream and Bridge* (10^8 order of magnitude). These high values result from near-zero clean contrast combined with measurable stego deviation. This reflects high sensitivity of the proposed framework under stable baseline conditions.

Moderate behavioral amplification is observed for *Tank* and *Cars and APCs* which suggests that deviation is detectable but less pronounced.

Conversely, *Truck* and *Truck and APCs* yield behavioral amplification values below unity. In these images, natural LSB variability is already substantial, and embedding does not produce proportionally larger behavioral deviation. This indicates that texture-driven intrinsic variability can reduce relative behavioral amplification, though not necessarily eliminate embedding-induced effects.

5.4. Detection

The detection criteria in the framework were applied to all test images by evaluating regional contrast and behavioral amplification together. Structurally stable images, which have low baseline contrast, consistently met both detection conditions. In these cases, stego contrast was much higher than clean contrast, and behavioral amplification values were large, often exceeding 150×. The deviation caused by embedding was clearly dominant over the natural LSB behavior, allowing for confident identification of stego images.

For structurally unstable images, intrinsic LSB variability was much higher. In these images, natural fluctuations reduced the impact of the deviation caused by embedding. As a result, the behavioral amplification values were smaller and sometimes close to one, indicating that the deviation did not significantly exceed the baseline variability.

To address this behavior, the detection rule is adjusted by including structural stability into the decision-making process. In images with higher baseline contrast, a larger behavioral amplification is needed before classifying the image as stego. If the embedding deviation does not clearly exceed intrinsic variability, the image is seen as behaviorally inconclusive rather than stego.

This refinement, which considers stability, keeps detection reliable in stable images while preventing overconfident classifications in unstable ones. By grounding detection confidence in measurable baseline behavior, the framework naturally fits the specific characteristics of each image instead of depending on a single global threshold.

5.5. Payload Sensitivity

To evaluate the robustness of the proposed behavioral framework under varying embedding strengths, behavioral amplification was measured at three payload levels: 4096, 16384, and 65,536 pixels and the results are presented in Table 4.

Table 4. Payload Sensitivity Analysis.

Image	Embedded Pixels		
	4,096 pixels	**16,384 pixels**	**65,536 pixels**
Aerial	251.55	157.86	163.26
Airplane	198.15	303.91	238.85
Boat.512	454.79	309.25	322.13
Car and APCs	0.26	1.13	1.21
Couple	315.54	207.78	205.96
Gray21.512	8.84×10^7	1.74×10^8	1.33×10^8
Stream and Bridge	1.76×10^8	3.06×10^8	2.68×10^8
Tank	1.48	2.80	2.47
Truck	0.08	0.61	0.60
Truck and APCs	1.37	0.41	0.84

Structurally stable images such as *Couple*, *Aerial*, *Airplane*, and *Boat.512* show high behavioral amplification across all payload levels. There is a noticeable strong deviation even with the smallest payload. *Tank* shows low behavioral amplification across all payload levels. Images with near-zero baseline contrast like *Gray21.512*, *Stream*, and *Bridge* show extremely large behavioral amplification, indicating high sensitivity under stable LSB dynamics. On the other hand, texture-dominated images like *Car and APCs*, *Truck*, and *Truck and APCs* show weak and inconsistent behavioral amplification, which indicates that the intrinsic LSB variability affects detection strength. Overall, behavioral amplification is influenced more by baseline stability than by payload size alone.

5.6. Comparison with Classical Steganalysis Tools

5.6.1. Chi-Square Analysis

The chi-square attack, introduced by Westfeld and Pfitzmann [12], detects LSB steganography by measuring deviations in pair-of-values distributions. In our experiments, the global chi-square steganalysis has produced extremely small or numerically zero p-values for both clean and stego images across the USC SIPI dataset. This behavior indicates sensitivity to global LSB imbalance rather than localized embedding and confirms the known limitations of chi-square analysis under spatially confined payloads.

5.6.2. StegExpose

For comparative evaluation, StegExpose [31], an open-source steganalysis tool that integrates chi-square testing, RS analysis, sample pair analysis, and related statistical detectors, was applied to all images in the dataset. Across the full set of experiments, StegExpose did not flag any stego image as suspicious. The internal decision indicator ("*Above stego threshold?*") remained false in every instance, despite the presence of embedded payloads ranging from 6 bytes to 3870 bytes. Chi-square p-values were frequently reported zero or extremely small for stego images, offering no meaningful discrimination under localized embedding. Similarly, RS analysis and sample pair statistics produced low to moderate values that did not exceed StegExpose's predefined detection thresholds. As a result, the final fusion scores remained consistently low—typically below 0.08—leading to negative detection decisions across all stego samples.
These findings indicate that the classical statistical detectors implemented within StegExpose are primarily sensitive to global LSB distribution distortions. When embedding is spatially confined and payload is limited, global statistics may remain largely unchanged, thereby reducing the effectiveness of such methods. In contrast, the proposed behavioral framework evaluates intra-image deviation by explicitly comparing regional LSB dynamics within the same image. This localized comparison allows embedding-induced disturbances to be interpreted as behavioral anomalies relative to the image's own baseline structure.

An additional advantage of the framework lies in its interpretability. Detection strength can be directly associated with measurable behavioral stability in the cover image, making it possible to understand why certain images yield stronger separability than others. This advantage over black-box learning-based methods highlights the suitability of the proposed approach for forensic and investigative settings.

5.7. Validation on the BOWS2 Dataset

To further evaluate the generalizability of the proposed framework, additional experiments were conducted on the BOWS2 dataset [29,30], which comprises 10,000 grayscale images. The same preprocessing, localized 1-bit LSB embedding strategy, and behavioral analysis procedure used for the USC SIPI dataset were applied. Owing to the large size of the dataset, presenting image-wise results is impractical. Therefore, the results are summarized using representative statistics.

The perceptual quality of the stego images was first evaluated using the Peak Signal-to-Noise Ratio (PSNR). Similar to the observations on the USC SIPI dataset, the embedding process introduced negligible visual distortion. All 10,000 stego images exhibited PSNR values greater than 55 dB, with values ranging from 56.23 dB to 58.65 dB. These results confirm that the localized 1-bit LSB embedding remained visually imperceptible across the entire dataset, ensuring that the behavioral analysis is not influenced by visible image degradation.

The regional behavioral contrast was then compared between the clean and stego images. For 88.77% (8,877 out of 10,000) of the images, the stego images exhibited a higher regional behavioral contrast than its corresponding clean image, indicating that localized LSB embedding generally increased behavioral deviation. In the remaining 11.23% (1,123 images), the clean image showed equal or higher regional behavioral contrast, suggesting that the natural variability of the image was comparable to or greater than the changes introduced by embedding. These observations are consistent with the results obtained on the USC SIPI dataset and demonstrate that regional behavioral contrast effectively captures embedding-induced behavioral changes across a large and diverse image collection.

Table 5 summarizes the distribution of behavioral amplification across the BOWS2 dataset. A total of 1,123 images (11.23%) exhibited behavioral amplification values below 1, indicating that the behavioral deviation introduced by embedding did not exceed the natural variability of these images. The majority of the images (6,359 images; 63.59%) showed amplification values between 1 and 5, suggesting that embedding produced noticeable behavioral changes while remaining influenced by the underlying image characteristics. In contrast, 2,518 images (25.18%) exhibited behavioral amplification values of 5 or greater, demonstrating substantially stronger embedding-induced behavioral deviation relative to the natural baseline. Among these, 284 images (2.84%) produced amplification values exceeding 100. These exceptionally high values occurred in images with very low clean regional behavioral contrast, where even modest embedding-induced changes resulted in a large relative increase in behavioral deviation. Overall, these findings are consistent with the observations on the USC SIPI dataset and further demonstrate that the proposed behavioral framework effectively distinguishes embedding-induced changes across a large and diverse collection of images.

Table 5. Distribution of Behavioral Amplification on the BOWS2 Dataset.

Behavioral Amplification (Γ_B)	Number of Images	Percentage
$\Gamma_B < 1$	1,123	11.23%
$1 \leq \Gamma_B < 5$	6,359	63.59%
$\Gamma_B \geq 5$	2,518*	25.18%

*Among the 2,518 images with $\Gamma_B \geq 5$, 284 images (2.84%) exhibited amplification greater than 100.

To evaluate the influence of embedding payload on the proposed behavioral framework, experiments were conducted using three region-of-interest (ROI) sizes corresponding to payloads of 4,096, 16,384, and 65,536 embedded pixels. The summary results are presented in Table 6. As expected, increasing the embedding payload resulted in a gradual reduction in PSNR, reflecting the larger number of modified pixels. Nevertheless, all stego images maintained PSNR values above 55 dB, confirming that the embedding remained visually imperceptible across all payload levels. Behavioral amplification was observed at all payload levels, indicating that the proposed framework consistently captured embedding-induced behavioral changes. While the average amplification varied across payloads, the differences were relatively small compared to the influence of the intrinsic characteristics of individual images. These findings suggest that baseline LSB behavior has a greater impact on behavioral amplification than payload size alone, consistent with the observations reported for the USC SIPI dataset.

Table 6. Summary of Results for Different Embedding Payloads on the BOWS2 Dataset.

Embedded Pixels	Mean PSNR (dB)	Images with PSNR > 55 dB	Mean Behavioral Amplification	Median Behavioral Amplification
4,096	69.30	100%	48.70	2.64
16,384	63.23	100%	31.34	1.79
65,536	57.18	100%	32.65	1.90

Overall, the results obtained on the BOWS2 dataset are consistent with those observed on the USC SIPI dataset. These findings further support the use of behavioral modeling as a practical and interpretable approach for localized image steganalysis.

6. Conclusion

This study presents a behavioral framework for image steganalysis inspired by process mining. It models pixel-level LSB activity as structured behavior instead of depending on global statistical tests or learned features. By modeling intra-image deviations through regional contrast and behavioral amplification, the approach offers a mechanism for detecting localized and low-payload embedding. The experimental evaluation was conducted on grayscale PNG images from the USC SIPI image database and the BOWS2 dataset. The results show that localized LSB embedding creates measurable behavioral disruption while remaining visually imperceptible (PSNR > 55 dB). The proposed method shows strong separability in structurally stable images, but detection strength decreases in images with high intrinsic LSB variability. The additional evaluation on the BOWS2 dataset, comprising 10,000 images demonstrated similar behavioral trends, indicating that the proposed framework generalizes well across different image collections. The findings suggest that behavioral amplification is closely linked to baseline structural stability. Images with stable LSB dynamics display noticeable embedding-induced deviation, while texture-dominated images show reduced relative improvement. These observations clarify the operational range of the framework and highlight the role of baseline structural stability in behavioral separability. For the experimental settings used in this study, conventional detectors such as chi-square analysis and StegExpose showed limited detection capability for the evaluated localized LSB embeddings on the USC SIPI dataset. Future work will extend the proposed framework to color and JPEG images, evaluate adaptive steganographic techniques, and explore reference-free behavioral analysis for practical applications. In summary, these results position behavioral modeling as a practical and useful direction for steganalysis in localized embedding scenarios. It offers clarity while identifying important boundary conditions.

All the Declarations and Statements

Author Contributions Statement

Shikha Badhani – Conceptualization, Methodology, Data curation, Software, Writing – original draft.
Vinita Verma – Methodology, Data curation, Software, Validation, Writing – original draft.
Manju Bhardwaj – Methodology, Investigation, Formal analysis, Visualization, Writing – review & editing.
Sakeena Shahid – Conceptualization, Data curation, Investigation, Visualization, Writing – original draft.
Geetan Manchanda – Methodology, Validation, Formal analysis, Writing – review & editing

All authors have read and agreed to the published version of the manuscript.

Conflict of Interest Statement

The authors declare no conflicts of interest.

Funding Declaration

None.

Data Availability Statement

This study analyzed publicly available datasets.
The datasets can be found here:
http://sipi.usc.edu/database/
https://data.mendeley.com/datasets/kb3ngxfmjw/1

Ethical Declarations

Not applicable. This study does not involve human subjects or animal experiments.

Acknowledgments

We sincerely thank the experts for their professional evaluation and valuable recommendations, which have contributed to improving the quality of the experiment and the reliability of its results.

Declaration of Generative AI in Scholarly Writing

None.

Abbreviations

The following abbreviations are used in this manuscript:

AI **-** Artificial Intelligence
BG **-** Background
CNN **-** Convolutional Neural Network
dB **-** Decibel
LSB **-** Least Significant Bit
MSB **-** Most Significant Bit
MSE **-** Mean Squared Error
PNG **-** Portable Network Graphics
PSNR **-** Peak Signal-to-Noise Ratio
ROI **-** Region of Interest
SVM **-** Support Vector Machine

APPENDIX

None.

References

[1] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, “Information hiding—A survey,” *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1062–1078, 1999, doi: 10.1109/5.771065.
[2] C. E. Shannon, “Communication theory of secrecy systems,” *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949, doi: 10.1002/j.1538-7305.1949.tb00928.x.
[3] K. Karampidis, E. Kavallieratou, and G. Papadourakis, “A review of image steganalysis techniques for digital forensics,” *Journal of Information Security and Applications*, vol. 40, pp. 217–235, 2018, doi: 10.1016/j.jisa.2018.04.005.
[4] D. R. I. M. Etiadi, S. Rustad, P. N. Andono, *et al.*, “Maximizing complex features to minimize the detectability of content-adaptive steganography,” *Multimedia Tools and Applications*, vol. 84, pp. 23813–23831, 2025, doi: 10.1007/s11042-024-20056-7.
[5] S. A. Naji, H. N. Mohaisen, Q. S. Alsaffar, and H. A. Jalab, “Automatic region selection method to enhance image-based steganography,” *Periodicals of Engineering and Natural Sciences*, vol. 8, no. 1, pp. 67–78, 2020.
[6] B. R. Ghosh, S. Banerjee, and J. K. Mandal, “A survey on LSB replacement-based statistical image steganalysis techniques,” in *Advances in Data Science and Computing Technologies*, Springer Nature Singapore, 2022, pp. 313–320.
[7] C. Ye and N. S. M., “Uncovering hidden data: A comparative study of statistical detection models for grayscale image steganography,” *European Journal of AI, Computing & Informatics*, vol. 1, no. 2, pp. 14–22, 2025.
[8] A. Amsaveni and P. T. Vanathi, “A comprehensive study on image steganography and steganalysis techniques,” *International Journal of Information and Communication Technology*, vol. 7, no. 4–5, pp. 406–424, 2015, doi: 10.1504/IJICT.2015.070300.
[9] W. M. P. van der Aalst, *Process Mining: Data Science in Action*, 2nd ed. Springer, 2016, doi: 10.1007/978-3-662-49851-4.
[10] F. Bezerra, J. Wainer, and W. M. P. van der Aalst, “Anomaly detection using process mining,” in *Enterprise, Business-Process and Information Systems Modeling*, T. Halpin *et al*., Eds., Springer, 2009, pp. 149–161, doi: 10.1007/978-3-642-01862-6_13.
[11] R. S. Mans, M. H. Schonenberg, M. Song, W. M. P. van der Aalst, and P. J. M. Bakker, “Process mining in health care,” in *Proc. Int. Conf. on Health Informatics (HEALTHINF’08)*, Jan. 2008, pp. 118–125.

[12] A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems," in *Proc. 3rd Int. Workshop on Information Hiding*, LNCS vol. 1768, I. S. Moskowitz, Ed., Springer, 2000, pp. 61–76, doi: 10.1007/10719724_5.

[13] J. Fridrich, M. Goljan, and R. Du, "Reliable detection of LSB steganography in color and grayscale images," in *Proc. ACM Workshop on Multimedia and Security*, 2001, pp. 27–30, doi: 10.1145/1232454.1232466.

[14] X. Yu, T. Tan, and Y. Wang, "Extended optimization method of LSB steganalysis," in *Proc. IEEE Int. Conf. on Image Processing*, vol. 2, 2005, pp. II-1102–II-1105, doi: 10.1109/ICIP.2005.1530252.

[15] K. Sullivan, U. Madhow, S. Chandrasekaran, and B. S. Manjunath, "Steganalysis for Markov cover data with applications to images," *IEEE Transactions on Signal Processing*, vol. 54, no. 2, pp. 225–236, 2006, doi: 10.1109/TSP.2005.861882.

[16] Y. Q. Shi, C. Chen, and W. Chen, "A Markov process based approach to effective attacking JPEG steganography," in *Proc. 9th Int. Workshop on Information Hiding (IH 2007)*, Lecture Notes in Computer Science, vol. 4567, Springer, Berlin, Heidelberg, 2007, pp. 249–264, doi: 10.1007/978-3-540-74124-4_17.

[17] T. Pevný, P. Bas, and J. Fridrich, "Steganalysis by subtractive pixel adjacency matrix," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 215–224, 2010, doi: 10.1109/TIFS.2010.2045842.

[18] J. Kodovský, J. Fridrich, and T. Holotyak, "Ensemble classifiers for steganalysis of digital media," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 432–444, 2012, doi: 10.1109/TIFS.2011.2170809.

[19] Y. Qian, J. Dong, W. Wang, and T. Tan, "Deep learning for steganalysis via convolutional neural networks," in *Media Watermarking, Security, and Forensics 2015*, vol. 9409, p. 94090J, 2015, doi: 10.1117/12.2083479.

[20] J. Ye, J. Ni, and Y. Yi, "Deep learning hierarchical representations for image steganalysis," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 11, pp. 2545–2557, 2017, doi: 10.1109/TIFS.2017.2710946.

[21] M. Boroumand, M. Chen, and J. Fridrich, "Deep residual network for steganalysis of digital images," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 5, pp. 1181–1193, 2019, doi: 10.1109/TIFS.2018.2871749.

[22] S. Agarwal and K.-H. Jung, "Digital image steganalysis using entropy driven deep neural network," *Journal of Information Security and Applications*, vol. 84, Art. no. 103799, 2024, doi: 10.1016/j.jisa.2024.103799.

[23] H. Chen, Q. Han, Q. Li, *et al*., "Image steganalysis with multi-scale residual network," *Multimedia Tools and Applications*, vol. 82, no. 15, pp. 22009–22031, 2023, doi: 10.1007/s11042-021-11611-7.

[24] T. Fu, L. Chen, Y. Jiang, J. Jia, and Z. Fu, "Image steganalysis based on dual-path enhancement and fractal downsampling," *IEEE Transactions on Information Forensics and Security*, vol. 20, pp. 1–16, 2025, doi: 10.1109/TIFS.2024.3493615.

[25] R. Yang, Y. Yang, L. Zhou, and X. Meng, "A steganalysis method based on relationship mining," *Electronics*, vol. 14, no. 21, Art. no. 4347, 2025, doi: 10.3390/electronics14214347.

[26] Z. He, R. Wu, and X. Wang, "Image steganalysis based on an adaptive attention mechanism and lightweight DenseNet," *Computers, Materials & Continua*, vol. 85, no. 1, pp. 1631–1651, 2025, doi: 10.32604/cmc.2025.067252.

[27] W. M. P. van der Aalst and S. Dustdar, "Process mining put into context," *IEEE Internet Computing*, vol. 16, no. 1, pp. 82–86, 2012, doi: 10.1109/MIC.2012.12.

[28] J. Fridrich and J. Kodovský, "Rich models for steganalysis of digital images," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 3, pp. 868–882, 2012, doi: 10.1109/TIFS.2012.2190402.

[29] A. Gupta, "BOWS2," *Mendeley Data*, V1, 2023, doi: 10.17632/kb3ngxfmjw.1.

[30] P. Bas and T. Furon, "BOWS-2 Contest (Break Our Watermarking System)," 2007–2008.

[31] B. Boehm, "StegExpose: A tool for detecting LSB steganography," arXiv:1410.6656, 2014. [Online]. Available: http://arxiv.org/abs/1410.6656

Authors' Profiles

Shikha Badhani is an Associate Professor in the Department of Computer Science at Maitreyi College, University of Delhi, with over 16 years of experience in teaching, research, and academic leadership. A University Gold Medalist at both undergraduate and postgraduate levels from the University of Delhi, she specializes in Information Security, Android Malware Detection, Machine Learning, Explainable AI, and Generative AI. Her Ph.D. from the University of Delhi focused on developing novel techniques for Android malware detection, leading to publications in reputed international journals, including *Computers & Security*, and prominent international conferences. She is currently exploring the area of LLMs to further her research.

Vinita Verma is an Assistant Professor in Rajdhani College, University of Delhi. She has done Ph.D. from Department of Computer Science, University of Delhi. She received her Master of Science degree in Computer Science and Bachelor of Science Honours degree in Computer Science from the University of Delhi in 2017 and 2015 respectively. She has research interest in the field of information security and malware detection. She has two journal publications in Scopus-indexed journals with four conference publications.

Manju Bhardwaj is an Associate Professor of Computer Science at Maitreyi College, University of Delhi, with nearly three decades of teaching experience. She earned her Ph.D. in Computer Science in 2018, following an MCA and a B.Sc in Mathematics from University of Delhi. Her teaching portfolio spans undergraduate and postgraduate courses in programming, data structures, operating systems, AI, machine learning, and data mining. Her research interests focus on artificial intelligence, machine learning, natural language processing, sentiment analysis, and classification ensembles. She has published extensively, with recent works on cryptocurrency security research and sunspot prediction using machine learning, alongside earlier studies on ensemble methods, sentiment analysis of COVID-19 tweets, and biological data classification. She has presented papers at international conferences, including ICDM in the USA and ICAISA in India.

Sakeena Shahid received the B.Sc. (Hons.) and M.Sc. degrees in Computer Science from the University of Delhi, India, where she is currently pursuing the Ph.D. degree with the Department of Computer Science, in the area of assessment of depth of anesthesia using machine learning and explainable AI. She is also an Assistant Professor with the Department of Computer Science, Sri Guru Tegh Bahadur Khalsa College, University of Delhi. Her research interests include the application of machine learning and deep learning in the medical domain. She is a member of ACM.

Geetan Manchanda is a Professor in the Department of Mathematics at Maitreyi College, University of Delhi, specializing in Numerical Analysis. She holds a B.Sc. (Hons.) from Sri Venkateswara College and an M.Sc. from Hindu College, University of Delhi, and earned her Ph.D. from Jamia Millia Islamia. Over her long academic career at Maitreyi College, she has taught core subjects such as Real Analysis, Abstract Algebra, Complex Analysis and Numerical Methods. She has published several research articles in international journals of repute.

How to cite this paper:

Shikha Badhani, Vinita Verma, Manju Bhardwaj, Sakeena Shahid, Geetan Manchanda, "From Pixels to Processes: A Process Mining-Inspired Approach to Image Steganalysis", International Journal of Mathematical Sciences and Computing(IJMSC), Vol.12, No.3, pp. 65-80, 2026. DOI: 10.5815/ijmsc.2026.03.04