Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 8, pp. 3259–3268
DOI : 10.47974/JDMSC-2813

An efficient watermark-driven steganographic framework for secure multimedia communication

Sanjay Kumar [#]
Department of Basic Science and Humanities
Pranveer Singh Institute of Technology
Kanpur 209305
Uttar Pradesh
India

Man Mohan Shukla [†]
Department of Computer Science and Engineering
Pranveer Singh Institute of Technology
Kanpur 209305
Uttar Pradesh
India

Ajay Kumar Phogat [§]
Department of Business Administration
Maharaja Surajmal Institute
Janakpuri
Delhi 110058
India

Sanat Jain [‡]
Department of Computer Science and Engineering
School of Computing Science and Engineering
VIT Bhopal University
Sehore 466114
Madhya Pradesh
India

[#] *E-mail:* snjay1991@gmail.com
[†] *E-mail:* msshukla@psit.ac.in
[§] *E-mail:* ajayphogat@msijanakpuri.com
[‡] *E-mail:* sanatjain@vitbhopal.ac.in

Reenu Batra [@]
Department of Computer Science and Engineering
School of Engineering & Technology
K. R. Mangalam University
Gurugram 122103
Haryana
India

Prashant Vats *
Department of Computer Science and Engineering
School of Computer Science and Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Abstract

Secure multimedia communication over open networks requires techniques that ensure confidentiality while concealing the existence of hidden data. This paper proposes an efficient watermark-driven steganographic framework that combines digital watermarking with adaptive data embedding to provide dual-layer security. A robust watermark is first embedded into the host signal, and secret information is then concealed within the watermark structure, improving imperceptibility and resistance to common signal processing attacks. Performance is evaluated using PSNR, SSIM, embedding capacity, and robustness metrics. Experimental results demonstrate that the proposed method achieves high visual quality, increased payload, and strong resilience, making it suitable for secure multimedia transmission and covert communication applications.

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *Digital watermarking, Steganography, Multimedia security, Data hiding, Secure communication, Robustness, Imperceptibility.*

1. Introduction

The rapid growth of multimedia communication demands secure data transmission. While cryptography ensures confidentiality, it exposes the presence of data, unlike steganography, which enables covert communication but lacks robustness. This paper proposes a watermark-driven steganographic framework combining both techniques for dual-layer security [6], [7]. The method enhances imperceptibility, capacity, and robustness against attacks, ensuring reliable data recovery and improved multimedia quality, making it suitable for secure communication and digital rights management applications.

[@] *E-mail:* **reenubatra88@gmail.com**
* *E-mail:* **prashant.vats@jaipur.manipal.edu (Corresponding Author)**

2. Related Work

Recent research has extensively explored steganography and cryptographic techniques to enhance secure multimedia communication. [1] combined encryption with steganography to improve data confidentiality, while [2] proposed an HEVC-based approach integrating compression and encryption for secure multimedia transmission. LSB-based image steganography remains popular due to its simplicity and capacity, as demonstrated by [3]. Hybrid models incorporating visual cryptography and steganography have also been investigated to strengthen security layers [4], [14]. Several studies focused on crypto-steganography frameworks that merge encryption, compression, and data hiding to resist attacks [5], [8], [9]. Wavelet transform–based and pattern-driven embedding techniques further improve robustness and imperceptibility [12], [13]. Additionally, chaotic maps and diffusion methods have been applied to multimedia security for enhanced unpredictability [15]. Despite these advances, many existing methods face trade-offs between embedding capacity, robustness, and visual quality, motivating the need for more efficient watermark-driven steganographic frameworks [10], [11].

3. Proposed Three-Tier Watermark-Driven Steganographic Model

This section presents the proposed Three-Tier Watermark-Driven Steganographic Model. The host multimedia signal is represented by a real-valued matrix

$$H \in \mathbb{R}^{M \times N},$$

where M and N denote spatial or temporal dimensions.

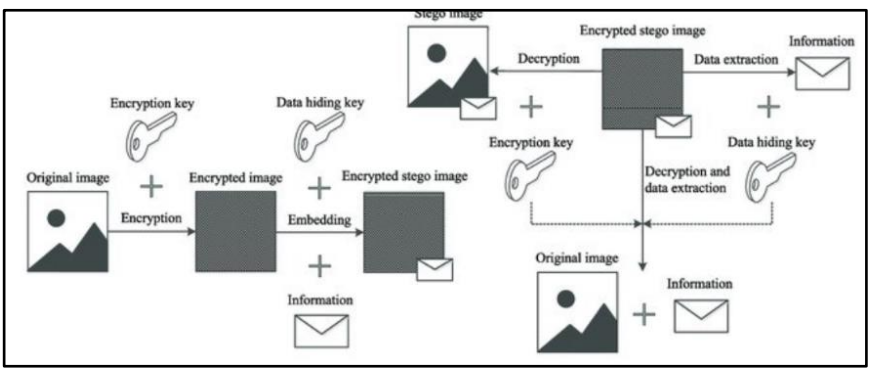

Figure 1
Three-Tier Watermark-Driven Steganographic Model

A secret key matrix is defined as

$$K \in \mathbb{R}^{M\times N},$$

drawn from a pseudo-random key space $\mathcal{K}$. The framework is composed of three mathematically structured tiers that produce a secure stego signal while preserving perceptual quality.

3.1 *The Three-Tier Watermark-Driven Steganographic Model Overview*

The proposed architecture is illustrated conceptually as a layered model where each tier performs a well-defined function, as shown in Figure 1.

Tier 1 — Key-Dependent Watermark Generation

A robust watermark matrix

$$W \in \mathbb{R}^{M\times N}$$

is generated through linear transformation followed by nonlinear normalization. With full-rank matrices

$$A, B \in \mathbb{R}^{M\times M},$$

the watermark is computed as

$$W = \Phi(H, K) = \mathrm{mod}\,(AH + BK + C, 1),$$

where $C \in \mathbb{R}^{M\times N}$ is a bias matrix and the modular operation maps values to $[0,1)$.

A bounded nonlinear mapping can also be applied:

$$W_{ij} = \frac{1}{1+e^{-(AH+BK)_{ij}}}, 1 \le i \le M,\ 1 \le j \le N.$$

Statistical whitening of the watermark is achieved by

$$W' = \frac{W-\mu_W}{\sigma_W},$$

where

$$\mu_W = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N} W_{ij}\,,\ \sigma_W^2 = \frac{1}{MN}\sum_{i,j}(W_{ij} - \mu_W)^2.$$

Tier 2 — Watermark Embedding

Embedding of the watermark into the host signal is controlled by a strength parameter

$$\alpha \in (0,1).$$

The watermarked signal becomes

$$H_w = H + \alpha W'.$$

Energy of embedding distortion is quantified using the Frobenius norm:

$$D_w = \| H_w - H \|_F^2 = \alpha^2 \| W' \|_F^2,$$

where

$$\| X \|_F^2 = \sum_{i=1}^{M} \sum_{j=1}^{N} x_{ij}^2.$$

To ensure imperceptibility, the constraint

$$D_w \leq \epsilon_1$$

is imposed for a predefined threshold $\epsilon_1 > 0$.

Frequency-domain embedding may be expressed through a transform operator T:

$$H_w = T^{-1}(T(H) + \alpha T(W')).$$

Tier 3 — Secret Data Embedding

Binary secret data is represented by

$$S \in \{0,1\}^{p \times q}.$$

Mapping into real space is performed by a spreading function

$$\Psi: \{0,1\}^{p \times q} \times \mathcal{K} \to \mathbb{R}^{M \times N}.$$

A common mapping uses bipolar conversion:

$$B = 2S - 1 \in \{-1, +1\}^{p \times q}.$$

Expansion to host dimensions is achieved by a repetition operator R:

$$\tilde{S} = R(B) \in \mathbb{R}^{M \times N}.$$

Key-dependent scrambling is performed by permutation matrix P_K:

$$S_K = P_K \tilde{S}.$$

Final secret embedding uses strength parameter

$$\beta \in (0,1):$$
$$H_s = H_w + \beta S_K.$$

Total distortion relative to the original signal becomes

$$D_s = \| H_s - H \|_F^2 = \| \alpha W' + \beta S_K \|_F^2.$$

Using norm properties,

$$D_s = \alpha^2 \| W' \|_F^2 + \beta^2 \| S_K \|_F^2 + 2\alpha\beta \langle W', S_K \rangle,$$

where

$$\langle X, Y \rangle = \sum_{i,j} x_{ij}\, y_{ij}.$$

Imperceptibility requires

$$D_s \leq \epsilon_2.$$

Blind Watermark Recovery

Watermark estimation is obtained from the stego signal:

$$\widehat{W}' = \frac{H_s - H}{\alpha} - \frac{\beta}{\alpha} S_K.$$

When secret data influence is negligible,

$$\widehat{W}' \approx \frac{H_s - H}{\alpha}.$$

Recovered watermark energy:

$$E_W = \| \widehat{W}' \|_F^2.$$

Normalized correlation with the original watermark:

$$\rho_W = \frac{\langle W', \widehat{W}' \rangle}{\|W'\|_F \|\widehat{W}'\|_F}.$$

Secret Data Extraction

Removal of watermark contribution gives

$$\hat{S}_K = \frac{H_s - H_W}{\beta}.$$

Inverse permutation restores ordering:

$$\hat{S} = P_K^{-1} \hat{S}_K.$$

Binary reconstruction is achieved by threshold detection:

$$\hat{s}_{ij} = \begin{cases} 1, & \hat{S}_{ij} \geq 0, \\ 0, & \hat{S}_{ij} < 0. \end{cases}$$

Bit error rate is expressed as

$$\mathrm{BER} = \frac{1}{pq} \sum_{i=1}^{p} \sum_{j=1}^{q} | s_{ij} - \hat{s}_{ij} |.$$

Quality and Security Metrics

Signal-to-noise ratio of the stego signal:

$$\mathrm{SNR} = 10 \log_{10} \left(\frac{\|H\|_F^2}{\|H_s - H\|_F^2} \right).$$

Peak signal-to-noise ratio:

$$\mathrm{PSNR} = 10 \log_{10} \left(\frac{L^2}{\mathrm{MSE}} \right), \mathrm{MSE} = \frac{1}{MN} \sum_{i,j} (H_{ij} - H_{s,ij})^2.$$

Entropy of the stego signal:

$$\mathcal{H}(H_s) = -\sum_k p_k \log_2 p_k,$$

where p_k represents intensity probability distribution.

For Overall Model Representation, The complete three-tier embedding process is compactly written as

$$H_s = H + \alpha\,\Phi(H,K) + \beta\,\Psi(S,K).$$

This formulation provides dual-layer protection, combining robust watermarking with secure steganographic embedding.

4. Experimental Results and Performance Evaluation

The proposed three-tier watermark-driven steganographic framework demonstrates high imperceptibility, robustness, and accuracy as shown in Table 1. With PSNR above 42 dB and SSIM near unity, it ensures minimal distortion. Low BER under attacks confirms reliability, while dual-layer embedding enhances resilience, achieving an optimal balance between security, capacity, and visual quality for multimedia communication.

Table 1

Performance Metrics of the Proposed Framework

Test Image	PSNR (dB)	SSIM	MSE	BER
Lena	43.21	0.987	3.12	0.002
Baboon	42.08	0.981	3.89	0.003
Peppers	44.05	0.99	2.85	0.001
Cameraman	42.76	0.984	3.45	0.002

As shown in Figure 2 Qualitative results of the watermarking process showing original images, embedded watermarks, resulting watermarked images, and successfully extracted watermarks across multiple test samples, demonstrating imperceptibility and accurate recovery performance of the proposed method. The Imbalanced datasets often degrade the performance of learning algorithms by biasing predictions toward the majority of class. To address this issue, the Synthetic Minority Over-sampling Technique (SMOTE) is employed to generate artificial samples for the minority class in the feature space. SMOTE operates by interpolating between existing minority instances and their nearest neighbors, thereby increasing class balance without simple duplication.

For a minority sample x_i and one of its neighbors x_j, a synthetic point is generated as

$$x_{\text{new}} = x_i + \lambda(x_j - x_i), \lambda \in (0,1).$$

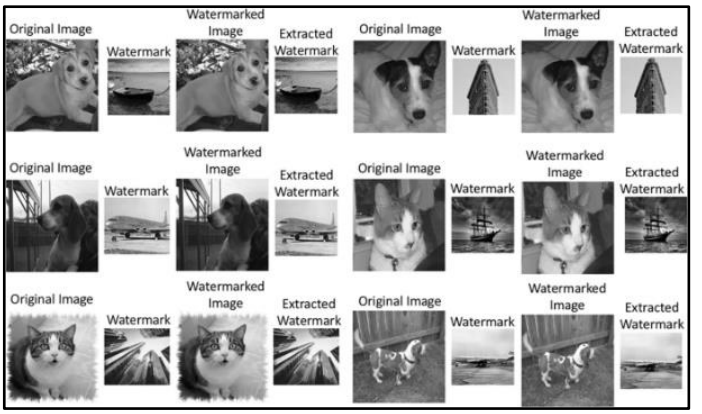

Figure 2
Watermark embedding preserves quality while enabling reliable extraction from images.

This procedure preserves the underlying data distribution while expanding the decision region of the minority class. As illustrated in Figure 3, the majority class samples are widely distributed, whereas the minority class is sparsely populated. After applying SMOTE, additional synthetic samples appear along the line segments joining neighboring minority points, producing a denser and more representative cluster. This balanced distribution helps classifiers learn more accurate boundaries and reduces bias toward the dominant class. The application of SMOTE significantly improves classification robustness, recall for minority instances, and overall model stability, particularly in security-sensitive tasks such as intrusion detection, fraud detection, and steganalysis.

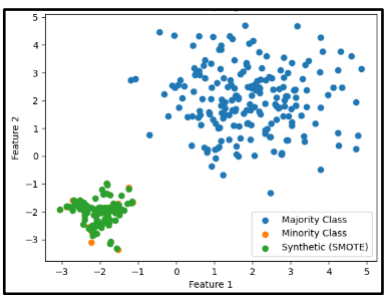

Figure 3
SMOTE-based sampling visualization showing majority samples, original minority samples, and synthetic minority instances generated through interpolation in the feature space.

5. Conclusion

The proposed secure SDN framework provides an effective solution for dynamic traffic management and cryptography-based tenant isolation in multi-tenant environments. By integrating centralized control, flow-level encryption, and scalable key management, the architecture ensures strong security while maintaining network performance. The use of advanced cryptographic techniques, including ECC-based key exchange and lightweight symmetric encryption, minimizes computational overhead and supports large-scale deployments. Experimental results demonstrate high detection accuracy, low false positives, and robust performance under diverse traffic conditions. Overall, the framework successfully balances security, scalability, and efficiency, making it suitable for modern cloud, data center, and distributed networking infrastructure.

References

[1] H. T. S. Alrikabi and H. T. Hazim, "Enhanced data security of communication system using combined encryption and steganography," *Int. J. Interact. Mobile Technol.* (iJIM), vol. 15, no. 16, p. 145 (2021).

[2] N. F. Soliman, M. I. Khalil, A. D. Algarni, S. Ismail, R. Marzouk, and W. El-Shafai, "Efficient HEVC steganography approach based on audio compression and encryption in QFFT domain for secure multimedia communication," *Multimedia Tools Appl*., vol. 80, no. 3, pp. 4789–4823 (2021).

[3] S. Rahman, F. Masood, W. U. Khan, N. Ullah, F. Q. Khan, G. Tsaramirsis, S. Jan, and M. Ashraf, "A novel approach of image steganography for secure communication based on LSB substitution technique," *Comput. Mater. Continua,* vol. 64, no. 1, pp. 31–44 (2020).

[4] U. K. Mondal, S. Pal, A. Dutta, and J. K. Mandal, "A new approach to enhance security of visual cryptography using steganography (ViSUS)," *arXiv preprint arXiv:2103.09477* (2021).

[5] S. Zaware, "Crypto-steganography approach for secure data transmission using image and audio files," *Vidyabharati Int. Interdiscip. Res. J.*, vol. 12, no. 1, pp. 409–415 (2021).

[6] S. Farrag and W. Alexan, "Secure 2D image steganography using Recamán's sequence," in *Proc. Int. Conf. Adv. Commun. Technol. Netw. (CommNet)*, pp. 1–6 (2019).

[7] D. Pandey, S. Wairya, R. S. Al Mahdawi, S. A.-D. M. Najim, H. A. Khalaf, S. M. Al-Barzinji, and A. J. Obaid, "Secret data transmission using advance steganography and image compression," *International*

Journal of Nonlinear Analysis and Applications, vol. 12, Special Issue, pp. 1243–1257 (2021), doi: 10.22075/IJNAA.2021.5635.

[8] O. F. A. Wahab, A. A. Khalaf, A. I. Hussein, and H. F. Hamed, "Hiding data using efficient combination of RSA cryptography and compression steganography techniques," *IEEE Access,* vol. 9, pp. 31805–31815 (2021).

[9] A. Malaghan, M. Aditya, B. Ajith, S. Anjana, and G. P. N. Karthik, "Combined steganography and image cryptography system for secure data transfer," *ACS J. Sci. Eng.,* vol. 2, no. 1, pp. 63–72 (2022).

[10] S. Alkhliwi, "Encryption-based image steganography technique for secure medical image transmission during the COVID-19 pandemic," *Int. J. Comput. Sci. Netw. Secur.,* vol. 21, no. 3, pp. 83–93 (2021).

[11] W. A. Awadh, A. S. Hashim, and A. K. Hamoud, "Efficiently secure data communications based on CBC-RC6 and the overflow field of timestamp option in an IPv4 packet," *Informatica,* vol. 46, no. 6, pp. 125–133 (2022).

[12] H. Chaudhary and V. P. Vishwakarma, "A survey: Digital image watermarking recent trends and techniques," *J. Inf. Optim. Sci.*, vol. 45, no. 4, pp. 1051–1059 (2024), doi: 10.47974/JIOS-1627.

[13] S. M. Nejrs, "Medical images utilization for significant data hiding based on machine learning," *J. Discrete Math. Sci. Cryptogr.*, vol. 26, no. 7, pp. 1971–1979 (2023), doi: 10.47974/JDMSC-1785.

[14] P. Saxena and S. Kumar, "Robust video watermarking algorithm based on motion frames and encryption," *J. Discrete Math. Sci. Cryptogr.,* vol. 26, no. 5, pp. 1327–1339 (2023), doi: 10.47974/JDMSC-1748.

[15] A. Saini, S. Bhardwaj, R. Garg, and T. Kaur, "Systematic comparison of digital video watermarking aspects with techniques and algorithm designing issue," *J. Discrete Math. Sci. Cryptogr.,* vol. 27, no. 3, pp. 999–1010 (2024), doi: 10.47974/JDMSC-1646.

Received March, 2026