Research Article

Secure Health Data Transmission by Bayesian Fusion of Hybrid Domain and Deep Learning Steganography

Sangeetha N[1], Harshith K Raj[2], K B Raja[3] and Mamatha B[4]

[1]Dept. of ECE, Dr. Ambedkar Institute of Technology, Bengaluru, India, sangeethapramod.ec@drait.edu.in.
[2]Dept. CSE, Tandon School of Engineering, New York University, New York City. harshith.02.14@gmail.com.
[3]University Visvesvaraya College of Engineering, Bangalore University, Bengaluru, India, rajakb429@gmail.com
[4]Rajarajeswari College of Engineering, VTU, Bengaluru, India, mamatha.789@gmail.com

Abstract

Securing medical pictures during transmission is a major difficulty in telemedicine, necessitating approaches that preserve both security and diagnostic fidelity. This research provides a Bayesian fusion-based steganographic framework that combines two complimentary approaches to produce higher imperceptibility, resilience, and reconstruction quality. The first approach employs a Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD), Least Significant Bit (LSB), hybrid (DWT–SVD–LSB) technique, where the cover and secret medical images are transformed into frequency sub-bands by DWT and the low-frequency coefficients (LL bands) are embedded using SVD for high stability and noise resistance. The second technique uses a deep learning-based Convolutional Neural Networks and DWT (CNN-DWT) model, where both images go through convolutional feature extraction, multi-level wavelet decomposition, and attention-based enhancement for creating a perceptually accurate stegoimage. The two models are fused by using the results level Bayesian precision fusion, which combines their hybrid PSNR of 56.73 dB and the deep learning PSNR of 57.73 dB. The fused PSNR is 60.27 dB, which is an improvement of 2.54 dB above the best performing individual approach.

Keywords: Bayesian Fusion, CNN, DWT, Steganography, SVD.

1. Introduction

In modern telemedicine and healthcare systems, secure medical picture transmission is increasingly a fundamental requirement. Patient data, which is frequently included in diagnostic imaging tests like MRIs, CT scans, and ultrasounds, must be protected from unwanted access, alteration, and interception in digital communication. Traditional encryption techniques can reveal confidential information even when they provide protection. Steganography guarantees anonymity and imperceptibility by concealing the existence of the data by embedding it into a cover image. However, finding a balance between security, robustness, and perceptual quality is still challenging.

Recent advances in image processing have led to the emergence of steganographic techniques based on transform-domain and deep learning. Transform-based methods like the DWT and SVD have demonstrated exceptional resistance to noise and compression while offering great imperceptibility since they integrate data in low-frequency sub-bands. Deep learning-based models, particularly those that employ CNNs, have demonstrated an unexpected capacity to learn complex feature representations for dependable picture embedding and extraction. Deep networks may generate minor distortions or decreased imperceptibility because of learnt feature fusion, while transform-domain techniques are statistically stable but might not adapt to different information. This study suggests a Bayesian fusion-based steganographic framework that combines the advantages of both paradigms in order to get beyond these restrictions. To improve semantic fidelity, the first approach employs a CNN–DWT architecture that combines deep spatial features and attention processes. The second approach is a hybrid DWT–SVD–LSB model that uses robust frequency-domain embedding to obtain greater imperceptibility. The Bayesian fusion technique, which ideally integrates quality metrics to minimize mean square error (MSE) while maximizing perceptual similarity, is utilized to fuse these two complementing systems [1, 2].

Contribution: The fusion technique effectively leverages the benefits of both domains, preserving the transform-domain reliability of DWT–SVD and the feature adaptiveness of CNN–DWT, to produce a stegoimage with high-fidelity recovery of the secret medical image and superior imperceptibility. The fused technique yields a perceptually superior and statistically optimal solution for the reduction of distortion and the enhancement of image quality. Under all circumstances, the proposed Bayesian fusion framework establishes a strong foundation for the secure, highly capacious, and diagnostically accurate steganography of medical images, thereby facilitating the advancement of intelligent healthcare data security systems.

2. Literature Survey

This review examines the primary contributions, strengths, and constraints of current steganographic techniques, thereby establishing the groundwork for the proposed fusion-based approach that enhances the current state of the art in the secure transmission and concealment of medical images.

Kamalakanta Sethi et al., [3] introduced a lightweight stego-crypto framework that integrates ChaCha20 encryption with Elliptic Curve Cryptography (ECC) for efficient key management, utilizing a 2D Discrete Wavelet Transform (DWT)-based steganographic approach. The recommended procedure encrypts diagnostic text within medical images, ensuring the secure and inconspicuous transfer of critical information. Jingxue Chen et al., [4] advised a digital medical image confidentiality protection architecture using information steganography and fuzzy deep learning. The framework changes patient confidentiality information into imperceptible noise and conceals it within the profound concealed space of the image. This approachwas essential for protecting patient privacy and data security. This skill can attain high accuracy in image segmentation, enabling the advancement of individualized medical services. The experimental results indicate that the system integrates patient information into medical images without compromising segmentation performance, while also effectively preserving privacy. Partha Chowdhuri et al., [5] introduced a practical authentication approach for digital picture steganography in medical imaging, leveraging the integration of Support Vector Machine (SVM) and Integer Wavelet Transform (IWT). The SVM initially distinguishes the Region of Interest (ROI) from the Non-Region of Interest (NROI) inside the medical image. Subsequently, IWT is utilized to incorporate confidential information within the NROI segment of the medical image (Cover Image). The circular array and a shared secret key are employed to augment the resilience of the proposed solution. Subhedar [6] posited that transform-domain picture steganography is enhanced by the ridgelet transform and singular value decomposition (SVD). The primary component derived from the singular value decomposition of the ridgelet coefficient functions is an embedding location. A stegoimage is created by embedding a secret image into it. Standard picture-quality metrics confirm experimental findings on imperceptibility and robustness. Suresh Babu et al., [7] introduced a technique, Robust and High-Capacity Image Steganography using SVD (RHISSVD), founded on the SVD transformation of digital images. This technique employs two fundamental features of SVD. The singular values (SVs) denote the brightness or energy of the digital image layer. The corresponding pair of singular vectors denotes the image geometry. A minor alteration to the SV cannot affect the image's visual impression. The cover image is dissected using Singular Value Decomposition (SVD), and the confidential message is encoded within its singular values.

Ye Yao et al. [8] introduced an end-to-end deep neural network for image steganography that leverages a generative adversarial network (GAN) and the discrete wavelet transform (DWT), thereby markedly enhancing the method's invisibility. Originally, the cover image is transformed from the RGB domain to the DWT domain to facilitate information embedding in the frequency domain. Additionally, a multi-scale attention convolution is used to integrate feature information across several scales, assisting the model in identifying a more optimal site for information embedding. The fusion module is employed to incorporate the information into the cover image at varying levels of alteration intensity. A discriminator has been introduced to assess cover and stegoimages patch-by-patch, thereby enhancing its efficacy. Amal Khalifa and Yashi Yadav [9] presented a Deep Wavelet Fusion Tool, categorized by a lightweight architecture that uses a bespoke DWT image dataset and incorporates the Mean Squared Error (MSE) loss function during training, thereby markedly dropping model complication and processing costs. Ambika et al. [10] ventured a coverless image steganography method for generating images imbued with inherent color and texture attributes that conceal private information. Recently, deep learning transformers using Generative Adversarial Networks (GANs) have been working to create concealed images. This approach, while resistant to steganalysis, modifies vital information in photos, rendering themunsuitable for tasks such as detecting illness in medical images shared in the cloud. The alterations in color and texture produced by GANs influence the feature vector derived from certain image regions utilized for disease detection. This study proposes an attention-guided GAN that modifies images only in specific areas while preserving their authenticity. Consequently, there is insignificantfalsification in feature extraction and a negligible effect on illness classification accuracy.

3. Proposed Fused algorithm

Problem Definition:

The suggested research identifies the issue as a statistical fusion challenge, seeking to integrate the advantages of both traditional and deep learning methodologies. A Bayesian fusion-based hybrid steganographic framework is established, integrating two complementary techniques: the Hybrid DWT-SVD-LSB method, which guarantees frequency-domain stability and minimal embedding distortion, and the CNN-DWT method, which captures multi-scale spatial-frequency features for enhanced flexibility. Bayesian precision fusion at the results level yields an elevated PSNR, signifying enhanced image quality.

Objectives:

- Create and verify a fused steganographic technique.
- By using Bayesian precision fusion, it achieves a better PSNR than the best individual technique.
- Maintains stegoimage quality appropriate for telemedicine in real time.

3.1 Embedding Algorithm

Inputs

Cover image C**,** Secret image S.

Outputs

Stegoimage, Extracted secret image

3.1.1 Effective Steganography-Based Health Data Transmission System Using Hybrid Domain [11].

Step 1: Input Cover image, Secret Image, and Preprocessing

- Read the cover image C and secret image G
- Convert color images to greyscale images and resize them to appropriate values.
- Convert both images to float 32 types and normalize to [0, 1] range

Step 2: Attention_Weight [attention_map] = Attention Module (C)

- An attention map uses variations in brightness to represent the intensity of attention the model gives to different parts of the image.

•Process cover image in 64×64 chunks

•Apply self-attention mechanism

•Normalize the attention map to the range [0.25, 0.75] to obtain the attention weight.

•Brighter regions closer to white indicate areas the model is more attentive to. Darker regions, closer to black, indicate areas the model is paying less attention to.

Step 3: Discrete Wavelet Transform

DWT (C_block, 'haar') = [LL_c, (LH_c, HL_c, HH_c)] % Cover image

DWT (G_block, 'haar') = [LL_s, (LH_s, HL_s, HH_s)] % Secret image

Step 4: SVD Decomposition

- SVD (LL_s) = [U_s, S_s, V_s] % Secret image
- SVD (LL_c) = [U_c, S_c, V_c] % Cover image

Step 5: Generate Singular Values of Stegoimage

- Singular Values for stegoimage is S_stego = S_c + α * attention_weight * S_s

Where,

α: A scaling factor of 0.100 is considered in our proposed model for better results.

Attention_weight, depending on the image, is normalized to 0.25-0.75.

Step 6: Stego Image Block Construction

- LL_stego = U_c * S_stego * VT _c %Multiplication
- Key = S_c, α, and attention_weight; embed in HL_c band using LSB Technique.
- The cover image HL_c band will be new band HL_new
- Stegoimage C'_block = IDWT (LL_stego, (LH_c, HL_new, HH_c), 'haar') %Spatial domain Stegoimage.

3.1.2 Deep Convolutional Networks and Multi-Level Wavelet Decomposition for Secure Medical Image Hiding [12]

Step 1: Resize and Normalize:

• The cover and secret images of different sizes are converted into a uniform size of 256 x 256.

• Normalize both cover and secret images to [0, 1] to prepare for CNN processing.

Step 2: Feature Extraction:

The features are extracted using a CNN and a DWT. The cover and secret-image features are concatenated to obtain the stego-image features.

Step 3: The Inverse DWT (IDWT) is applied to generate a stegoimage in the spatial domain.

3.1.3 Proposed Secure Health Data Transmission by Bayesian Fusion of Hybrid Domain and Deep Learning Steganography.

Combine Effective Steganography-Based Health Data Transmission System Using Hybrid Domain Method and Deep Convolutional Networks and Multi-Level Wavelet Decomposition for Secure Medical Image Hiding at the results level in terms of PSNR between cover image and stegoimage using Bayesian precision fusion [13] given in Equation 1.

$PSNR_{fused=} 10\log_{10}(10^{0.1P1}+10^{0.1P2})$ --------------------------(1)

Where, P1 = PSNR in dB between the cover image and the stegoimage of Efficient Health Data Transmission System Based on Steganography Using Hybrid Domain Technique.

P2 = PSNR in dB between the cover image and the stegoimage of Secure Medical Images Hiding Using Deep Convolutional Networks and Multi-Level Wavelet Decomposition.

3.2 Fused Extraction Algorithm

Input

- Stegoimage
- Pre-trained CNN–DWT decoder model

Outputs

- Extracted secret image
- Fused PSNR values

3.2.1 Effective Steganography-Based Health Data Transmission System Using Hybrid Domain.

Step 1: DWT Decomposition of Stego Image

Perform one-level DWT on the received stegoimage

(LL’,LH’,HL’,HH’)=DWT(Stegoimage)

Step 2: Extraction via Hybrid DWT–SVD–LSB Branch

- Retrieve the stego key from the LSB bits of HL’’.
- Apply SVD on the low-frequency band LL’.
- Recover the secret singular values:
- Reconstruct the LL band of the secret image:
- Perform Inverse DWT using the reconstructed LL band and corresponding high-frequency bands of the secret image.

3.2.2 Deep Convolutional Networks and Multi-Level Wavelet Decomposition for Secure Medical Image Hiding

Step 1: Extraction via CNN–DWT Decoder Branch

- Feed the samestego image into the pre-trained CNN–DWT decoder network.
- The decoder performs multi-level wavelet decomposition, followed by convolutional feature reconstruction.
- The network outputs the extracted secret image

Step 2: Compute the Individual PSNRs between the secret and the extracted secret image

Step 3: Bayesian Precision Fusion

PSNR between the secret image and the extracted secret image using Bayesian precision fusion is given in Equation 2.

$PSNR_{fused=}10\log_{10}(10^{0.1P3}+10^{0.1P4})$ -----------------------(2)

Where,

P3 = PSNR in dB between thesecret image and the extracted secret imageof the Efficient Health Data Transmission System Based on Steganography Using Hybrid Domain Technique.

P4 = PSNR in dB between the secret image and the extracted secret image of Secure Medical Images Hiding Using Deep Convolutional Networks and Multi-Level Wavelet Decomposition.

4. Performance Analysis

Two steganographic methods are compared in Table 1. One uses a hybrid DWT-SVD-LSB approach with a PSNR of 1, and the other uses deep convolutional networks with multi-level wavelet decomposition to achieve a PSNR of 2, along with their Bayesian-fused results for medical images. Optimal and statistically superior results were obtained by combining the PSNR data from the two approaches using the Bayesian fusion algorithm. All test situations show an improvement of about +2.5 dB when the data are added together. Take MRI cover-stego pairs as an example; the PSNR increases from 56.73 dB and 57.73 dB to 60.27 dB. On the other hand, it rises from 52.86 dB and 53.86 dB to 56.40 dB for X-ray images, suggesting less distortion and better imperceptibility. For the secret-extracted picture pairs, the PSNR goes up from 34–35 dB to 37 dB, which means the secret-image reconstruction is better. Based on the findings, it appears that Bayesian fusion is a great way to combine the PSNR of the hybrid model with the adaptive learning capabilities of the deep model. This results in a fused steganographic system that is perfect for secure medical data transfer because it increases imperceptibility.

The results in Table 2 clearly indicate the superiority of the proposed Bayesian Fusion based steganographic method over the existing methods. The model of Wenjie Lin et al. [14] used the encoder-decoder architecture based on CNN, and only obtained PSNRs of 31.70 dB between the cover and stegoimage and 11.48 dB between the secret and extracted image, which means much distortion and weak recovery.
Bini M. Issac et al. [15] proposed a method combining CNN and DWT to extract better features, achieving a PSNR of 39 dB, which demonstrates higher imperceptibility but limited augmentation. However, the suggested Bayesian Fusion model, which combines the advantages of CNN–DWT and DWT–SVD–LSB approaches, attains a significant PSNR of 60.27 dB between the cover and stegoimages and 37.66 dB between the secret and extracted secret pictures.

Table 1. The improvement in PSNR is achieved through Bayesian fusion.

This significant improvement demonstrates the usefulness of the Bayesian precision fusion technique in balancing spatial adaptivity and frequency-domain stability. The results validate that the fused technique results in improved picture quality and efficient extraction of secret image from stegimage and is an effective option for secure and invisible medical image communication

Table 2: Result comparison of the proposed method and the existing methods

Sl. No.	**Authors**	**Techniques**	**PSNR (dB)**	
			Cover and Stegoimage	**Secret and Extracted secret image**
1	Wenjie Lin et al., [14], 2022	CNN-based encoder and decoder	31.7026	11.4829
2	Bini M. Issac et al., [15], 2025	CNN–DWT architecture	39	--------
3	Proposed Fusion Method	Bayesian Fusion	60.2690	37.6590

Sl No.	**Types of Cover and Secrete Images**	**Existing Techniques presented by Sangeetha et al., [11] and [12]**		**Proposed Technique**
		PSNR-1	PSNR-2	PSNR
1	Cover Image (MRI Image) and Stegoimage	56.73	57.73	60.2690
	Secret Image (Boy) and Extracted Secret Image	34.12	35.12	37.6590
2	Cover Image (X-Ray Image) and Stegoimage	52.86	53.86	56.40
	Secret Image (Girl) and Extracted Secret Image	33.45	34.45	37.00

5. Conclusion

This research presented a Bayesian fusion-based steganographic framework for secure medical image transmission. It successfully combines two complementary methodologies, a hybrid DWT-SVD-LSB technique and a CNN-DWT model based on deep learning. The goal is to achieve an optimal balance among imperceptibility, robustness, and reconstruction fidelity. By using singular value embedding, the hybrid approach provides robustness in the frequency domain and good statistical stability, while the deep learning model improves learning of spatial-frequency features and adaptive attention-driven refinement.. The best-performing individual approach was about 2.54 dB lower than the fused PSNR of 60.27 dB, which was achieved by applying Bayesian precision fusion at the results level and combining the separate outputs based on their PSNR values. The suggested

Bayesian fusion framework has the potential to become an AI-driven healthcare system cornerstone in the future due to its increased adaptability, intelligence, security, and scalability.

References

[1]. D. L. Hall and J. Llinas, "An Introduction to Multisensor Data Fusion," IEEE Journal, vol. 85, no. 1, pp. 6-23, January 1997, doi: 10.1109/5.554205.

[2]. Shutao Li, Xudong Kang, Leyuan Fang, Jianwen Hu, and Haitao Yin, “Pixel-Level Image Fusion: A Survey of the State of the Art,” Elsevier Information Fusion, vol. 33, pp. 100–112, 2017, doi.org/10.1016/j.inffus.2016.05.004.

[3]. Kamalakanta Sethi, Bishwajeet Sahoo, Shrishti, B. N. Pavan Kumar, Kasturi Dhal, Woong Cho and Gyanendra Prasad Joshi, "Lightweight DWT Steganography With ECC-ChaCha20 for Secure Medical IoT Systems," IEEE Access, vol. 13, pp. 142948-142960, 2025, doi: 10.1109/ACCESS.2025.3598099.

[4]. Jingxue Chen,Pengbiao Zhao, Erqiang Deng, Fazlullah Khan, Ryan Alturki, Bandar Alshawi, and Hu Xiong, "Fused Fuzzy Deep Learning and Information Steganography for Privacy Preservation in Medical Consumer Electronics," IEEE Transactions on Consumer Electronics, vol. 71, no. 2, pp. 7105-7116, May 2025, doi: 10.1109/TCE.2025.3525536.

[5]. Partha Chowdhuri, Pabitra Pal, and Tapas Si, “A novel steganographic technique for medical image using SVM and IWT,” Springer Nature Multimed Tools Applications, 82(13), pp 20497–20516, 2023, doi: 10.1007/s11042-022-14301-0.

[6]. SubhedarM,“Image Steganography Using Ridgelet Transform and SVD,”Springer International e-Conference on Intelligent Systems and Signal Processing. Advances in Intelligent Systems and Computing, vol 1370, pp 81-91, Singapore, 2022, https://doi.org/10.1007/978-981-16-2123-9_6.

[7]. K Suresh Babu, K. B. Raja, U. M. K. Rao, K. A. Rashmi, K. R. Venugopal, and L. M. Patnaik, "Robust and high-capacity image steganography using SVD," IEEE IET-UK International Conference on Information and Communication Technology in Electrical Sciences (ICTES 2007), Chennai, India, 2007, pp. 718-723.

[8]. Ye Yao, Junyu Wang, Junyu Wang, Qi Chang, Yizhi Ren, andWeizhi Meng, “High Invisibility Image Steganography with Wavelet Transform and Generative Adversarial Network,” Elsevier Expert Systems with Applications, vol 249, Part A, 2024, doi: 10.1016/j.eswa.2024.123540.

[9]. Amal Khalifa and Yashi Yadav, “Wavelet-Based Fusion for Image Steganography Using Deep Convolutional Neural Networks,”MDPI Electronics, vol 14, issue 14, pp 1-13, 2758; 2025, doi.org/10.3390/electronics14142758.

[10]. Ambika, Virupakshappa, and Deepak S. Uplaonkar, “Deep Learning-Based Coverless Image Steganography on Medical Images Shared via Cloud,” MDPI Engineering, vol 59, issue 1, pp 1-10, 176; 2024, doi.org/10.3390/engproc2023059176.

[11]. Sangeetha N, Harshith K Raj, and K B Raja, “Efficient Health Data Transmission System Based on Steganography Using Hybrid Domain Technique**,**” Journal of Electronics and Communication Engineering and Technology (Scopus), vol 6, issue 1, pp 1-23, 2025, doi.org/10.34218/JECET_06_01_001.

[12]. Sangeetha N, Harshith K Raj, and K. B. Raja, “Secure Medical Images Hiding Using Deep Convolutional Networks and Multi-Level Wavelet Decomposition,” STAPS Journal (Scopus, WoS), vol 11, issue 10, pp 164-194, 2025, doi: 24. 20089.STAPS. 2025.V11.10.02114.

[13]. Jürgen Beyerer, Michael Heizmann, Jennifer Sander, Ioana Gheţa,“7- Bayesian Methods for Image Fusion,”Image Fusion, Algorithms and Applications, pp 157-192, 2008, doi.org/10.1016/B978-0-12-372529-5.00003-2.

[14]. Wenjie Lin, Xueke Zhu, Wujian Ye, Chin-Chen Chang, Yijun Liu, and Chengmin Liu1, “An Improved Image Steganography Framework Based on Y Channel Information for Neural Style Transfer,” Hindawi Security and Communication Networks, vol 2022, Article ID 2641615, pp 1-12, January 2022, doi.org/10.1155/2022/2641615.

[15]. Bini M. Issac, S. N. Kumar, Sherin Zafar, Kashish Ara Shakil, and Mudasir Ahmad Wani, “Deep Learning Steganography for Big Data Security Using Squeeze and Excitation with Inception Architectures,” Scientific Reports, 15, 31193, 2025, doi.org/10.1038/s41598-025-16394-7.