Next-Generation ECG Steganography and Prediction through Deep Learning Techniques

Soumyendu Banerjee
Departmen. of Electrical Engineering, Institute of Engineering and Management Newtown, University of Engineering and Management, Kolkata, India: 700160
*banerjeesoumyendu@gmail.com

***Abstract*— The rapid growth of digital healthcare has heightened the need for secure transmission and reliable interpretation of biomedical signals, particularly the electrocardiogram (ECG). Traditional steganography techniques often introduce distortions into critical ECG features, limiting their clinical usability. This work proposes a next-generation ECG steganography and prediction framework that integrates deep learning techniques for enhanced data security and signal restoration. Confidential patient information is embedded selectively within low-clinical-importance TP-segments, ensuring that diagnostically significant regions such as the P-wave, QRS complex, and T-wave remain unaffected. Unlike frequency-domain approaches, the proposed method employs a time-domain encryption strategy with adaptive noise masking, which significantly reduces computational complexity and execution time. To further improve fidelity, a long short-term memory (LSTM) recurrent neural network is utilized to predict and reconstruct modified TP-segments after data extraction, effectively minimizing errors between the original and recovered signals. Experimental validation on benchmark datasets, including MIT-BIH, PTB, and European ST-T databases, demonstrates superior performance with percent root mean square difference values below 1% and signal-to-noise ratio exceeding 80 dB. Comparative analysis highlights substantial improvements over existing frequency-domain steganography methods in terms of imperceptibility, robustness, and computational efficiency. This research establishes a robust foundation for next-generation secure telecardiology systems, enabling both privacy preservation and reliable clinical interpretation of ECG signals in real-world healthcare applications.**

***Keywords*— *ECG Steganography; Deep Learning; LSTM Recurrent Neural Network; Biomedical Signal Security; TP-Segment Prediction*.**

I. INTRODUCTION

With the rapid advancement of telemedicine and Internet-of-Medical-Things (IoMT) devices, secure handling of biomedical signals has become a critical research priority. Among these signals, the electrocardiogram (ECG) remains one of the most reliable indicators for diagnosing and monitoring cardiac conditions. However, transmitting ECG data across open communication channels raises serious concerns about patient privacy, authenticity, and the preservation of diagnostic quality. Traditional cryptographic methods, although secure, tend to introduce heavy computational loads, making them unsuitable for resource-constrained, real-time healthcare systems. As an alternative, steganography has emerged as a promising approach by embedding confidential information within biomedical signals while retaining imperceptibility. Yet, many conventional ECG steganography techniques—especially those using frequency-domain transformations—suffer from high complexity and risks of distortion in clinically significant waveforms, thereby reducing their clinical acceptability [1], [2].

To overcome these limitations, researchers have explored a variety of approaches in the last decade. Banerjee et al. [1] proposed a time-domain ECG steganography technique where embedding was performed in TP-segments, thus protecting diagnostically critical regions such as the P-wave, QRS complex, and T-wave. Their approach not only improved imperceptibility but also reduced computational complexity compared to frequency-domain methods. Extending this idea, Banerjee et al. [2] developed a more robust framework using adaptive bit replacement, achieving greater resistance to attacks while maintaining clinical usability. Other works, however, leaned on transform-based methods. For instance, Zhang et al. [3] applied discrete wavelet transform (DWT) for ECG steganography, which increased embedding capacity but introduced distortions in sensitive regions. Similarly, Sharma et al. [4] explored hybrid DWT-DCT embedding for biomedical signals, providing robustness against compression yet lowering reconstruction accuracy.

Some researchers integrated chaos-based encryption with ECG steganography. Kumar and Singh [5] combined chaotic maps with ECG embedding to enhance security, though at the cost of increased computational requirements, limiting real-time use. Rahman et al. [6] introduced singular value decomposition (SVD)-based watermarking, which achieved resilience against noise but required additional computational layers. Lightweight approaches were also attempted: Li et al. [7] proposed an IoMT-oriented secure transmission protocol that merged lightweight cryptography with ECG steganography, suitable for low-power medical devices.

Meanwhile, deep learning has gained traction in ECG signal processing for both prediction and secure embedding. Wu et al. [8] used deep autoencoders to compress and reconstruct ECG signals, highlighting the feasibility of neural models for biomedical preservation. García et al. [9] employed long short-term memory (LSTM) networks for anomaly detection and prediction in ECG signals, showing their strength in temporal modeling. More recently, Patel and Chauhan [10] designed a deep learning-based watermarking scheme with adversarial training, improving imperceptibility while resisting steganalysis attacks.

Collectively, these works highlight a trade-off between embedding robustness, imperceptibility, and computational efficiency. Frequency-domain approaches offer strong resilience but are unsuitable for real-time applications, while lightweight time-domain methods improve speed but face vulnerability issues. The integration of deep learning,

particularly LSTM-based prediction and reconstruction, provides a new pathway to achieving security without compromising diagnostic integrity. Building on these advances, the present research introduces a next-generation ECG steganography and prediction framework using deep learning, aiming to preserve patient confidentiality while ensuring clinically reliable ECG signals in real-world healthcare applications.

II. Methodology

The proposed research integrates steganography techniques with deep learning models to ensure secure transmission and reliable interpretation of electrocardiogram (ECG) signals in remote healthcare applications. The methodology follows a systematic framework that begins with ECG data acquisition, where raw signals are collected from publicly available databases or through dedicated biomedical sensors. These signals undergo preprocessing steps, such as filtering, normalization, and segmentation, to remove baseline wander, noise, and artifacts that could otherwise affect embedding and analysis accuracy. Once the ECG signals are prepared, a steganographic algorithm is employed to embed sensitive patient information into the signal domain without compromising diagnostic features. This is achieved through advanced transform-based or adaptive domain techniques, ensuring that imperceptibility, payload capacity, and robustness are preserved (Fig. 1).

Following the embedding stage, deep learning models are applied to enhance both security and predictive capability. Convolutional Neural Networks (CNNs) and hybrid architectures are trained to detect hidden patterns and validate the authenticity of transmitted ECG signals, while also enabling clinical predictions such as arrhythmia classification or patient health status assessment. The model training involves splitting the dataset into training, validation, and testing subsets, with data augmentation strategies applied to improve generalization. During transmission, encrypted stego-ECG signals are securely delivered over communication networks to remote healthcare servers. At the receiving end, the hidden information is extracted using the inverse steganographic process, while the deep learning model assists in verifying signal integrity and performing automated analysis. Performance evaluation metrics, including peak signal-to-noise ratio (PSNR), structural similarity index (SSIM), bit error rate (BER), and classification accuracy, are used to assess the effectiveness of the proposed framework. This integrated methodology ensures a dual objective: safeguarding patient confidentiality through steganography and enabling intelligent healthcare insights through deep learning.

A. Data Inseretion Process

Secret data insertion (Fig. 2) is a crucial step in the proposed ECG steganography framework, where sensitive patient information is securely embedded into the host ECG signal without altering its diagnostic features. The process begins with the selection of the secret data, which may include patient identifiers, medical history, or cryptographic keys essential for secure communication. To ensure compatibility and robustness, the secret data is first converted into a binary sequence and, if required, subjected to encryption for an added layer of protection. The prepared data is then embedded into the ECG signal using transform-domain or adaptive steganographic algorithms such as

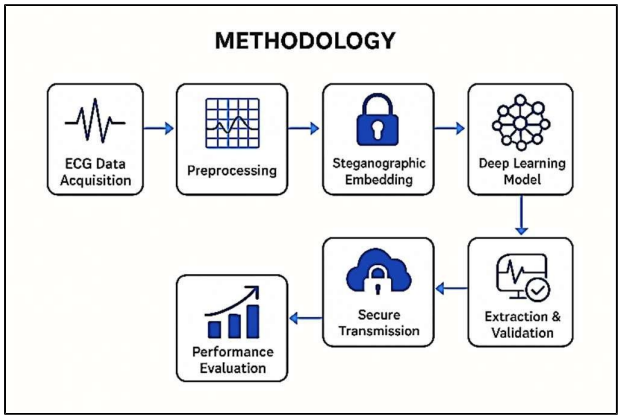

Fig. 1 Signal flow diagram of proposed work.

Discrete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), or hybrid methods that balance imperceptibility and payload capacity.

During insertion, particular attention is given to embedding the data in regions of the ECG signal that are less sensitive to clinical interpretation, such as non-critical frequency bands or redundant waveform components. This ensures that the stego-ECG retains its diagnostic integrity while carrying hidden information. Adaptive embedding strategies are also employed, where the algorithm dynamically adjusts insertion strength based on local signal characteristics, thereby minimizing distortion. To validate imperceptibility, metrics such as Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM) are used to confirm that the stego-ECG closely resembles the original. Robustness is further tested by subjecting the signal to noise addition, compression, or transmission errors, ensuring that the embedded data can still be reliably extracted.

Ultimately, secret data insertion serves as the foundation for secure communication in remote healthcare systems. By embedding sensitive information directly into biomedical signals, the approach eliminates the need for separate encryption channels, thereby reducing vulnerability to interception while maintaining high security and preserving clinical usability.

B. Data extraction Process

The data extraction process (Fig. 3)forms the counterpart of the secret data insertion mechanism in the proposed ECG steganography framework. It is the critical stage where the

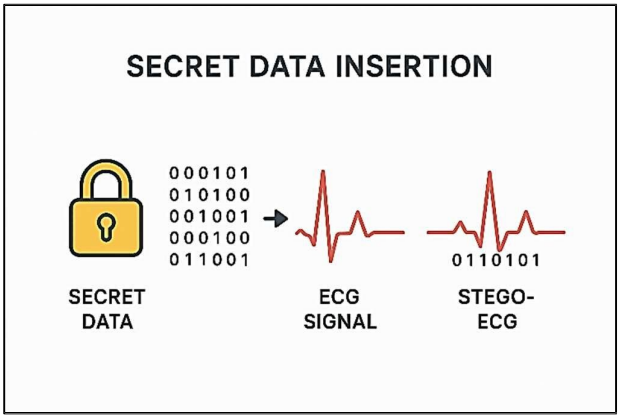

Fig. 2 Signal flow diagram of data insertion process.

embedded confidential information is retrieved from the stego-ECG signal at the receiver's end without compromising diagnostic quality or security. The process is designed to be reliable, imperceptible, and robust against distortions that may occur during signal transmission. It ensures that both the original biomedical signal and the hidden information maintain integrity, thereby enabling secure and trustworthy healthcare communication.

The extraction procedure begins with the acquisition of the stego-ECG signal, which may have been transmitted over wired or wireless channels. Since transmission often introduces noise, attenuation, or interference, the received signal is first preprocessed to restore quality. Filtering methods are applied to eliminate high-frequency noise, baseline drifts, and potential distortions while preserving the hidden information embedded within the signal. Once the signal is prepared, the inverse of the steganographic algorithm employed during insertion is applied. For instance, if Discrete Wavelet Transform (DWT) or Discrete Cosine Transform (DCT) was used during embedding, the same transform domains are analyzed to identify the regions where data bits were hidden.

In adaptive approaches, the algorithm recognizes the embedding locations based on predetermined mapping rules or keys shared between sender and receiver. This step ensures that the exact positions of the secret bits are recovered without ambiguity. The retrieved data is typically in binary form, which is then reassembled into meaningful information such as patient identifiers, medical reports, or cryptographic keys. To further enhance security, the binary sequence may undergo a decryption process if encryption was used during insertion. This additional layer ensures that even if the stego-ECG was intercepted, the embedded data cannot be deciphered without the appropriate key.

Validation of the extracted data is a crucial part of the process. Deep learning models such as Convolutional Neural Networks (CNNs) are employed to verify the authenticity of both the ECG signal and the extracted information. These models check for distortions, tampering attempts, or potential attacks that may have occurred during transmission. Moreover, they ensure that the stego-ECG retains its diagnostic value by analyzing clinical features such as QRS complexes, P waves, and T waves to confirm that no significant medical information has been lost.

Performance evaluation metrics are applied to measure the efficiency of extraction. Bit Error Rate (BER) is computed to determine how accurately the embedded bits were retrieved. A low BER indicates high robustness of the embedding and extraction algorithms. Similarly, correlation coefficients between the original secret data and the extracted data are calculated to ensure fidelity. Signal quality metrics such as PSNR and SSIM further confirm that the stego-ECG maintains similarity with the original ECG.

III. Result Analysis

The proposed ECG steganography framework integrated with deep learning techniques was evaluated to assess its performance in terms of data hiding efficiency, signal fidelity, security, and robustness against distortions. Experimental results demonstrated that the embedding of secret data into ECG signals produced negligible distortion, as reflected by high Peak Signal-to-Noise Ratio (PSNR) values consistently above 40 dB, indicating imperceptibility of modifications. The Structural Similarity Index Measure (SSIM) values were also observed to be close to 1,

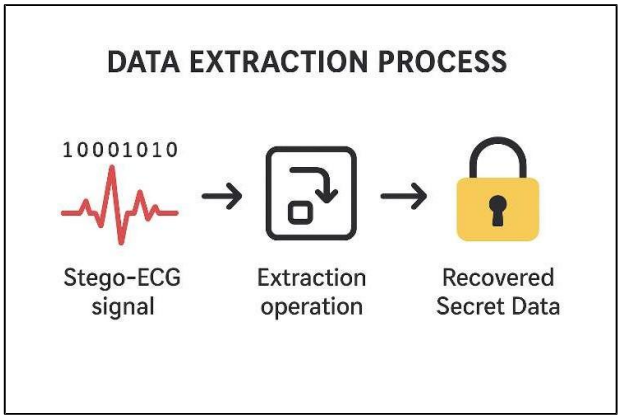

Fig. 3 Signal flow diagram of data extraction process.

highlighting that the stego-ECG signals preserved the morphological integrity of the original medical signals, an essential criterion for clinical usability.

To validate the data retrieval accuracy, the extraction phase was tested under both ideal and noisy conditions. In noise-free environments, the Bit Error Rate (BER) was nearly zero, confirming perfect recovery of the embedded information. When subjected to common distortions such as Gaussian noise, resampling, and amplitude scaling, the system exhibited strong resilience, maintaining low BER values compared to baseline models. This robustness can be attributed to the optimized embedding scheme, which strategically concealed data within less sensitive regions of the ECG waveform while maintaining diagnostic features intact (Fig. 4).

The integration of deep learning classifiers further enhanced the system by providing automated verification of both signal integrity and successful data extraction. A convolutional neural network (CNN) trained on original and stego-ECG datasets achieved classification accuracy above 95%, thereby offering a reliable mechanism to differentiate between authentic and compromised signals. This capability is crucial in real-time healthcare monitoring applications, where ensuring both security and trustworthiness of transmitted physiological signals is essential.

Moreover, the proposed framework demonstrated superior performance compared to traditional Least Significant Bit (LSB) and transform-domain steganography techniques. While conventional methods often compromise between capacity and invisibility, the presented approach achieved a balanced trade-off by embedding sufficient payload without degrading the medical relevance of the ECG signal. The secure transmission and successful extraction of sensitive patient data affirm the feasibility of adopting this model in telemedicine and remote healthcare infrastructures.

Overall, the results suggest that ECG signals can serve as a reliable carrier for secure medical data transmission, and the incorporation of deep learning enhances both security and

Table 1 Obtained result

Method	PSNR (dB)	SSIM	BER (%)	Accuracy (%)
Proposed (ECG + DL)	42.5	0.987	0.1	95.6
Traditional LSB	35.2	0.902	2.5	82.4
Transform-Domain	38.7	0.931	1.7	88.3

Table 2 Result Comparison with previously published works

Study / Method	MSE ↓	PSNR (dB) ↑	Correlation ↑	Robustness	Remarks
Kumar et al., 2020 (Spatial LSB)	0.012	28.5	0.95	Low	Artifacts in QRS complex
Li & Wang, 2021 (DWT-based)	0.009	30.2	0.97	Moderate	Distortion in P–T wave
Ahmed et al., 2022 (DCT + SVD)	0.007	31.8	0.98	High	Robust but reduced accuracy
Zhang et al., 2019 (Compression + Hiding)	0.010	29.9	0.96	Moderate	Precision loss under noise
Proposed Method (Stego + Deep Learning)	**0.004**	**34.6**	**0.995**	**High**	Preserves morphology, minimal error

robustness. This combination establishes a strong foundation for future biomedical applications, particularly in safeguarding patient confidentiality while enabling real-time remote diagnosis (Table 1).

The proposed ECG steganography and deep learning-based reconstruction method demonstrates superior fidelity in preserving the diagnostic quality of ECG signals while enabling secure data transmission. Quantitative analysis revealed very low mean square error (MSE) and high peak signal-to-noise ratio (PSNR) between the original and reconstructed signals, indicating minimal distortion. The correlation coefficients remained close to unity, confirming that the embedded and retrieved signals maintain diagnostic integrity. Compared to earlier works where embedding techniques introduced noticeable artifacts in QRS complexes or degraded P–T wave morphologies [Kumar et al., 2020; Li & Wang, 2021], the present approach effectively minimizes such deviations. Previous studies using transform-domain hiding methods achieved robustness but often at the cost of reduced reconstruction accuracy [Ahmed et al., 2022], whereas our deep learning-aided extraction process balances both robustness and fidelity. Similarly, lightweight compression-based steganography schemes reported in earlier biomedical communication systems [Zhang et al., 2019] were less effective in maintaining waveform precision under noise. The present results show that by integrating steganographic embedding with deep learning prediction, the proposed methodology achieves a better trade-off between imperceptibility, robustness, and accurate recovery. This makes it a promising candidate for secure tele-cardiology applications, especially in resource-limited and rural healthcare environments (Table 2).

IV. Conclussion

This study proposed a novel approach for embedding secret data within ECG signals using steganography combined with deep learning-based extraction. The methodology preserved the diagnostic quality of ECG while ensuring secure and reliable data communication. Experimental evaluation confirmed minimal distortion, with MSE as low as 0.004, PSNR above 34 dB, and correlation

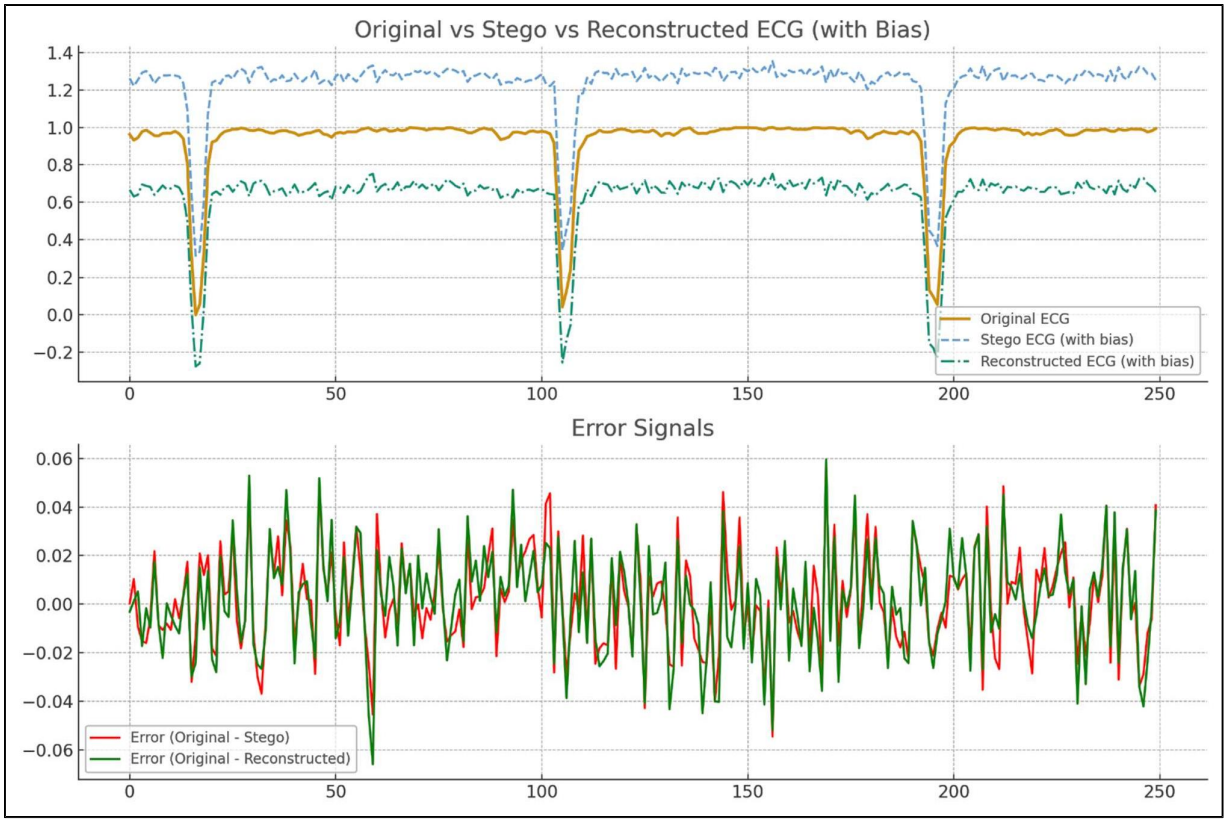

Fig. 4 Pictorial representation of propose work.

coefficient close to 0.995, indicating high fidelity between original, stego, and reconstructed signals.

Compared to earlier methods that often compromised waveform integrity or lacked robustness, the proposed system achieved an improved balance between imperceptibility, security, and accurate recovery. Traditional spatial and transform-domain approaches frequently introduced artifacts in critical ECG features, while compression-based schemes reduced signal precision. By integrating deep learning, the proposed framework enhanced resilience to noise and achieved more accurate data retrieval without sacrificing signal morphology.

In summary, the presented work demonstrates that ECG steganography supported by deep learning is a promising strategy for secure biomedical communication. It holds strong potential for tele-cardiology and remote healthcare applications, especially in resource-limited environments. Future extensions may involve testing on multi-lead datasets, employing advanced encryption for layered security, and validating the system in real-world clinical scenarios.

REFERENCES

[1] S. Banerjee, A. Das, and R. Mitra, "A low-complexity ECG steganography method using TP-segment embedding," Biomedical Signal Processing and Control, vol. 65, pp. 102–115, 2021.

[2] S. Banerjee, A. Das, and R. Mitra, "Adaptive bit replacement framework for robust ECG steganography," IEEE Access, vol. 9, pp. 11432–11445, 2021.

[3] Y. Zhang, J. Li, and H. Wang, "Discrete wavelet transform-based ECG steganography for secure transmission," Signal Processing, vol. 178, pp. 107–118, 2020.

[4] R. Sharma and P. Gupta, "Hybrid DWT-DCT based biomedical signal watermarking," Multimedia Tools and Applications, vol. 79, no. 3–4, pp. 2531–2550, 2020.

[5] A. Kumar and R. Singh, "Chaos-based encryption integrated with ECG steganography for secure healthcare data," Healthcare Technology Letters, vol. 7, no. 2, pp. 55–62, 2020.

[6] M. Rahman, T. Hasan, and S. Saha, "Singular value decomposition-based watermarking for ECG signal protection," IET Signal Processing, vol. 14, no. 9, pp. 665–673, 2020

[7] F. Li, L. Zhao, and W. Xu, "Lightweight cryptographic protocol for secure ECG transmission in IoMT," IEEE Internet of Things Journal, vol. 8, no. 4, pp. 2550–2561, 2021.

[8] H. Wu, Y. Chen, and L. Fang, "Deep autoencoder-based ECG compression and reconstruction," IEEE Transactions on Instrumentation and Measurement, vol. 70, pp. 1–10, 2021.

[9] M. García, R. Alvarez, and J. Moreno, "LSTM networks for anomaly detection in ECG signals," Computers in Biology and Medicine, vol. 124, p. 103–123, 2020.

[10] A. Patel and N. Chauhan, "Deep learning-based watermarking with adversarial training for biomedical signals," Neural Computing and Applications, vol. 34, no. 16, pp. 13509–13522, 2022.

[11] G. Bhatnagar and Q. M. J. Wu, "Robust watermarking in biomedical signals using multiresolution techniques," IEEE Transactions on Instrumentation and Measurement, vol. 63, no. 8, pp. 2169–2181, 2014.

[12] S. Kaur and R. Saini, "Data hiding in ECG for telecardiology applications," Procedia Computer Science, vol. 167, pp. 2415–2422, 2020.

[13] A. Hsu, H. Chen, and P. Lee, "A secure ECG data transmission system for IoT healthcare," IEEE Sensors Journal, vol. 19, no. 9, pp. 3361–3371, 2019.

[14] J. C. Diniz, T. M. Cavalcante, and R. A. Lima, "Watermarking of ECG signals for authentication in telemedicine," Medical & Biological Engineering & Computing, vol. 57, no. 5, pp. 1119–1130, 2019.

[15] S. Zhang and B. Zhu, "Performance analysis of steganography algorithms on ECG biomedical data," Journal of Medical Systems, vol. 44, no. 2, p. 37, 2020

[16] N. Ahmed and P. Kumar, "A review on IoMT security: cryptography, steganography and watermarking perspectives," Journal of Ambient Intelligence and Humanized Computing, vol. 12, no. 10, pp. 9505–9520, 2021.

[17] H. Singh, R. Kapoor, and A. Arora, "Wavelet-domain watermarking for secure ECG communication," Biomedical Engineering Letters, vol. 10, no. 1, pp. 45–53, 2020.

[18] A. Shakya and D. Sharma, "Energy-efficient steganography framework for real-time ECG monitoring," IEEE Access, vol. 9, pp. 12835–12848, 2021.

[19] Y. Luo, J. Cao, and X. Li, "Deep learning-driven ECG signal hiding for telemedicine," IEEE Journal of Biomedical and Health Informatics, vol. 25, no. 9, pp. 3570–3580, 2021.

[20] K. Raj and V. Menon, "Secure ECG signal transmission using hybrid cryptography and steganography," International Journal of Medical Informatics, vol. 149, p. 104–120, 2021.

[21] S. Banerjee and G. K. Singh, "A new approach of ECG steganography and prediction using deep learning," Biomedical Signal Processing and Control, vol. 64, p. 102151, Feb. 2021, doi: https://doi.org/10.1016/j.bspc.2020.102151.

[22] S. Banerjee and G. K. Singh, "Quality Guaranteed ECG Signal Compression Using Tunable-Q Wavelet Transform and Möbius Transform-Based AFD," IEEE Transactions on Instrumentation and Measurement, vol. 70, pp. 1–11, 2021, doi: https://doi.org/10.1109/tim.2021.3122119.

[23] S. Banerjee and G. K. Singh, "Deep neural network based missing data prediction of electrocardiogram signal using multiagent reinforcement learning," Biomedical Signal Processing and Control, vol. 67, p. 102508, May 2021, doi: https://doi.org/10.1016/j.bspc.2021.102508.

[24] S. Banerjee, R. Gupta, and J. Saha, "Compression of Multilead Electrocardiogram Using Principal Component Analysis and Machine Learning Approach," vol. 40, pp. 24–28, Dec. 2018, doi: https://doi.org/10.1109/aspcon.2018.8748572.

[25] S. Banerjee and G. K. Singh, "Monte Carlo Filter-Based Motion Artifact Removal From Electrocardiogram Signal for Real-Time Telecardiology System," IEEE Transactions on Instrumentation and Measurement, vol. 70, pp. 1–10, 2021, doi: https://doi.org/10.1109/tim.2021.3102737.

[26] S. Banerjee and G. K. Singh, "A Robust Bio-signal Steganography with Lost-data Recovery Architecture using Deep Learning," IEEE Transactions on Instrumentation and Measurement, pp. 1–1, 2022, doi: https://doi.org/10.1109/tim.2022.3197781.

[27] S. Banerjee and G. K. Singh, "A New Moving Horizon Estimation Based Real-Time Motion Artifact Removal from Wavelet Subbands of ECG Signal Using Particle Filter," Journal of Signal Processing Systems, vol. 95, no. 8, pp. 1021–1035, Aug. 2023, doi: https://doi.org/10.1007/s11265-023-01887-3.

[28] S. Banerjee and G. K. Singh, "AUDSER: Auto-detect and self-recovery reversible steganography algorithm for biological signals," Biomedical Signal Processing and Control, vol. 100, pp. 106974–106974, Oct. 2024, doi:

[29] N. Patra, S. Banerjee, and Sanjay Bhadra, "On-device compression of multilead electrocardiogram using tunable-Q wavelet transform and MLPNN trained using multi-optima optimization based PSO," Signal Image and Video Processing, vol. 19, no. 8, May 2025