International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 10 October 2026
Page No: 5616-5624
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0734

Intelligent Concealment of Healthcare Information: A Novel Machine Learning-Driven Multi-Layered Steganographic Approach for Enhanced Medical Data Privacy

Kantharaju[1], Srinidhi G A[2], Veena N D[3]
[1]Research Scholar, Dept. of Electronics and Communication Engineering, Sri Siddhartha Institute of Technology, Sri Siddhartha Academy of Higher Education, Tumakuru, Karnataka, India
[2]Research Supervisor, Dept. of Computer Science Engineering (Cyber Security), Sri Siddhartha Institute of Technology, Sri Siddhartha Academy of Higher Education, Tumakuru, Karnataka, India.
[3]Assistant Professor, Dept. of Computer Science Engineering, Sri Siddhartha Institute of Technology, Sri Siddhartha Academy of Higher Education, Tumakuru, Karnataka, India
Emails: *kantharajukck@gmail.com[1], srinidhiga@ssahe.edu.in[2], veenand@ssahe.edu.in[3],*
Orcid: 0009-0002-0480-4500[1], 0000-0002-5297-7249[2], 0009-0003-0020-2219[3]

Abstract
Rapidly, the adoption of cloud computing, the "Internet of Medical Things (IoMT)", telemedicine, and electronic medical records has made an increasing number of people concerned about the security of medical information being transmitted. This study suggests a novel multi-layered steganographic approach designed using an intelligent machine learning system for privacy preserving healthcare communication. The structure is based on the NIH Chest X-ray dataset of 112,120 X-rays from 30,805 patients. The basic steps of medical image preprocessing include resizing, image normalization, CLAHE enhancement, median filtering, and AES-256 encryption, ResNet-50 based deep feature extraction, adaptive region selection using XGBoost and DWT-LSB embedding. The medical images are preprocessed by resizing, image normalization, CLAHE enhancement, median filtering and AES-256 encryption followed by ResNet-50 deep feature extraction, XGBoost based adaptive region selection and DWT-LSB embedding. Experimental results give an impressive PSNR of 54.32 dB and SSIM of 0.978, embedding capacity of 0.175 bpp, and extraction accuracy of 99.21%. The proposed framework is also able to decrease the time of operation from 19.7% to 37.2% in terms of steganalysis detection ratio and 0.99 in terms of AUC, and reduce the encryption/decryption time to 1.72 s and 1.63 s, respectively. Based on these outcomes, the framework introduced in this study is proven to be efficient, robust, and highly secure for concealing healthcare data while maintaining user privacy in the present context of digital healthcare.

Keywords: *Medical Image Steganography; Healthcare Data Privacy; Machine Learning-Based Information Hiding; Deep Learning for Medical Security; Secure Healthcare Communication; Adaptive Steganographic Embedding.*

1. Introduction
The digitization of healthcare has enabled efficient storage and exchange of electronic medical records (EMRs), medical images, and clinical information through cloud computing, the Internet of Medical Things (IoMT), telemedicine, and artificial intelligence [1], [2]. However, increased connectivity exposes sensitive healthcare data to cyber threats, including unauthorized access, data breaches, and information manipulation [3]. Therefore, ensuring the confidentiality, integrity, and authenticity of medical information is essential [4]. Conventional encryption protects sensitive data by converting plaintext into ciphertext [5]. However, it does not conceal the existence of communication. Steganography complements encryption by embedding secret information within digital media, such as medical images, without perceptible changes [6], [7]. Existing methods have limitations: least significant bit (LSB) techniques offer high embedding capacity but are vulnerable to statistical attacks, while transform-domain methods may compromise image quality or embedding efficiency

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 10 October 2026
Page No: 5616-5624
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0734

[8]. Furthermore, fixed embedding strategies often fail to adapt to image characteristics, increasing distortion and detectability [9], [10]. Machine learning can address these limitations by identifying image features and selecting suitable embedding regions to minimize distortion [12]. Integrating intelligent region selection, adaptive embedding, and multilayer security mechanisms can improve concealment while preserving diagnostic image quality [13]. These capabilities are particularly important for secure healthcare data exchange, telemedicine, and cloud-based medical systems [14]. This study proposes an Intelligent Machine Learning-Driven Multi-Layered Steganographic Framework for secure healthcare information concealment within medical images. The framework combines intelligent region selection, adaptive embedding, and multiple security mechanisms to improve imperceptibility, embedding capacity, and resistance to steganalysis while preserving image quality. Its performance is evaluated using PSNR, SSIM, MSE, embedding capacity, and security robustness. The main contributions are:

- Developing a machine learning-driven multilayer steganographic framework for healthcare information.
- Designing adaptive embedding to minimize distortion and preserve diagnostic quality.
- Enhancing resistance to statistical analysis and steganalysis attacks.
- Evaluating performance against existing techniques using image-quality, capacity, and security metrics.

2. Literature Review

There have been recent attempts to harness machine learning, blockchain, and advanced steganographic methods to achieve comprehensive intelligent protection of healthcare data.Recent research has shown great advances in intelligent protection of healthcare data using a combination of machine learning, blockchain, and advanced steganographic methods. In their research, Malik et al. (2025) [16] introduced a novel StegoSec-EHR framework that combines blockchain, lightweight signcryption, and machine learning techniques to enhance the security of EHRs. The framework used U-Net along with Enhanced Lizard Optimization (ELO) for feature extraction and Dynamic Coherent Quantum Neural Network (DCQNN) for disease classification. The experiment results with healthcare records of 1.28 million patients showed a 98 percent improvement in security, with high diagnostic accuracy. Haque et al. (2026) [17] developed a machine learning-driven graphene-based THz MIMO antenna for secure 6G healthcare communications with an antenna gain of 11.23 dB, efficiency of 86.87%, isolation of −34.17 dB, and XGB regression accuracy of 93.29%. Sanjalawe et al. (2025) [18] proposed a multi-layered steganographic model based on Huffman coding, LSB embedding, and deep learning, achieving SSIM values of more than 99% and achieving a text recovery rate of 100%. Aljughaiman et al. (2025) [19] proposed an adaptive LSB steganography framework based on Ant Colony Optimization and hybrid encryption which achieved PSNR values in the range of 59.7-64.5 dB, a high SSIM above 0.999 and a low MSE below 0.07. Malik et al. (2025) [20] proposed a hybrid DCT-GAN steganography method with a PSNR of 58.27%, SSIM of 94.20%, reconstruction accuracy of 96.2% and 95.7%, and better overall image quality than traditional methods. Fatima et al. (2025) [21] proposed a predictive voting-based data hiding technique that was able to embed up to 686,874 bits with reliable extraction. To enhance imperceptibility and robustness, Flores et al. (2025) [22] applied chaotic maps in conjunction with LSB steganography, producing an average PSNR of 56.49 dB, SSIM value greater than 0.9998 and MSE value as low as 0.10. Musa et al. (2025) [23] summarized the access control frameworks based on blockchain, and reported a throughput boost of up to 42% with transaction latency in the range of ~39ms, when compared to the traditional cloud access control mechanisms. In this regard, Ahmad et al. (2025) [24] introduced the CNN-DCT steganography model for cloud computing environment with a false-positive rate of 2.1%, bit error rate of 0.028, an execution time of 2.3 s and successful results on 500 high-resolution images. Basani et al. (2024) [25] developed the study of a secure manet communication system with EPCC, grey wolf optimization and AODV routing which achieved 93% success rate and 92.5% overall accuracy. Dyavani et al. (2024) [26] proposed a

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 10 October 2026
Page No: 5616-5624
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0734

Markov Models Topological Data Analysis based adaptive access control system for cloud healthcare with a 97.63% anomaly detection rate, 93.78% access control accuracy and 2.45% false-positive rate. Guan et al. presented a blockchain-IoT system for secure information management which provides high-level security against tampering with a real-time communication system (Guan et al., 2023) [27]. In their study, Ahmad et al. (2025) [28] tested seven deep learning based steganography architectures, with a PSNR of 43.5 dB and a SSIM of 0.995 produced by Wavelet Hybrid Network and a detection rate of close to the random probability (0.501–0.502) produced by Mutual Attention Transformer and Efficient Attention Pyramid Transformer. Kanimozai et al. (2025) [29] proposed a deep reinforcement learning-based intrusion detection system model that achieved 99.85% detection accuracy, 98.67% detection sensitivity, 97.42% detection specificity with a response time of 1423 ms. Moghadasi et al. (2025) [30] discussed the new framework of intelligent control of wastewater treatment plants based on artificial intelligence and showed that artificial intelligence is being increasingly used to improve the prediction accuracy, process optimization, and operational efficiency of wastewater treatment plants. Tiwari et al. (2025) [31] explored the role of artificial intelligence in the intelligent control of wastewater treatment plants, which includes different types of artificial intelligence, such as deep learning, fuzzy logic, and artificial neural networks. In all, the studies confirm that the combination of machine learning, deep learning, blockchain, adaptive optimization and intelligent steganography significantly enhances the security, imperceptibility, robustness and computational efficiency of contemporary healthcare information protection systems. Though modern studies have enhanced the security of healthcare data with blockchain, cryptography, deep learning, and traditional steganography, there are still some drawbacks. Most approaches in the literature focus on either encryption or data hiding and do not provide a smart multi-layered approach to simultaneously optimize security, embedding capacity, imperceptibility and robustness. Moreover, the use of adaptive machine learning-based embedding region selection for medical images is still under-explored. Hence, it is necessary to develop a unified multi-layered steganographic framework based on machine learning for the secure, efficient and privacy-preserving transmission of healthcare information.

3. Research Methodology

The proposed methodology proposes a multi-layered stealthy concealment system to transmit confidential information in the medical image space through machine learning based approach. The framework employs four techniques: medical image preprocessing, AES-256 encryption for safeguarding medical image data, ResNet-50 deep feature extraction for generating deep feature maps, and intelligent embedding region selection using XGBoost model, and adaptive DWT-LSB steganographic embedding. Lastly, the framework is tested with image quality and security metrics such as PSNR, MSE, BER, embedding capacity and extraction accuracy to show its efficacy in the context of privacy-preserving medical data transmission. As shown in Figure 1 framework of methodology.

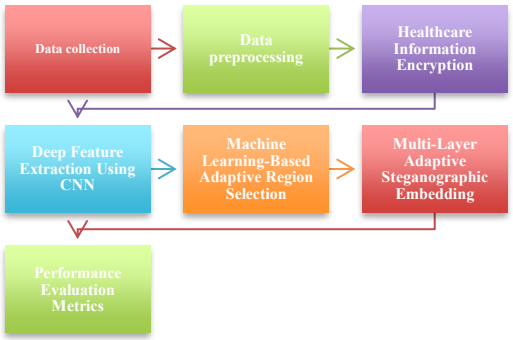


Figure 1 framework of methodology

3.1.Data collection

The NIH Chest X-ray Dataset [32] is a widely used and accessible medical imaging dataset that is among the largest available for the use of artificial intelligence and medical research. It was developed at the National Institutes of Health (NIH) and has 112,120 images of the front of the chest taken from 30,805 different patients. This is a dataset of 14 thoracic disease types, including Atelectasis, Cardiomegaly, Effusion, Infiltration, Mass, Nodule, Pneumonia, Pneumothorax, and No Finding. The images are annotated by utilizing natural language

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 10 October 2026
Page No: 5616-5624
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0734

processing of radiology reports. The dataset is used in a variety of applications such as medical image classification, deep learning and steganography, preservation of privacy, and secure healthcare information hiding studies, due to its large size, high-quality annotations, and classes of diseases.

3.2.Data preprocessing

3.2.1. Image Resizing

The resolution of medical images is resized to a uniform size of 512 × 512 pixels to have uniform input dimension for deep learning and Steganographic processing. The uniformity of image size reduces computational complexity, and provides a uniform feature representation throughout the data set. The latter, resizing, also enables efficient convolution operations during the extraction of the features, thereby retaining important anatomical structures needed for an effective embedding operation. The resizing operation is represented by:

$$I_r=Resize(I,512\times512) \qquad (1)$$

Where I is the original image, Ir is the resized image.

3.2.2. Intensity Normalization

Images of the chest X-ray are resized and then normalized for intensity to minimise the effects of different imaging devices and acquisition conditions. Normalization: This helps to reduce the difference between pixel intensities, which facilitates convergence in deep learning, and stable feature extraction. It also helps to make the embedding process more consistent as it minimizes the variations of intensity of the medical images. The normalization equation is:

$$I_n = \frac{I-I_{min}}{I_{max}-I_{mi}} \qquad (2)$$

Where I denotes the resized image, In denotes the normalized image.

3.2.3. Contrast Enhancement Using CLAHE

Contrast Limited Adaptive Histogram Equalization (CLAHE) is used after normalization to enhance the local contrast without too much noise amplification. CLAHE splits the image into small contextual regions and does histogram equalization in each region separately and then reconstructs the image using bilinear interpolation. It improves the similarity of fine anatomical structures, e.g. lung boundaries, vascular patterns, which further improves the feature extraction and better embedding region selection for intelligent operations. To achieve the enhanced image, the equation is shown as:

$$I_c = \text{CLAHE}(I_n) \qquad (3)$$

Where In is the normalized image, Ic is the contrast-enhanced image.

3.2.4. Noise Reduction

The acquisition noise on medical images can impact the feature extraction and embedding quality. A 3 × 3 median filter is used to reduce impulsive noise, while retaining significant structural information and edges. To alleviate embedding distortion and enhance the overall imperceptibility of the steganographic framework, the noise is effectively removed while deep features are extracted afterward.Removing noise can make the deep features extracted after better and improve the robustness of the subsequent deep features extraction, which can minimize embedding distortion and enhance the overall imperceptibility of the steganographic framework. The filtering operation is described by the equation:

$$I_f = \text{MedianFilter}(I_c) \qquad (4)$$

Where Ic is the enhanced image, If is the denoised image.

3.3.Healthcare Information Encryption

Sensitive healthcare information such as patient identity information, diagnostic reports, lab test results, prescriptions, and clinical notes are encrypted using the Advanced Encryption Standard (AES-256) with a 256-bit key before being embedded. AES-256 is chosen due to its high computational security, speed of encryption and resistance to brute force and cryptographic attacks. The data is encrypted prior to the steganographic embedding into the medical image, thus the hidden data is kept confidential even if the attacker able to recover the hidden data from the medical image. Finally, using the proposed multi-

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 10 October 2026
Page No: 5616-5624
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0734

layer steganographic framework, the encrypted ciphertext is embedded inside the selected regions of the cover image. The encryption operation is shown as: Figure 2 AES-256 encryption process.

$$C = E_k P \qquad (5)$$

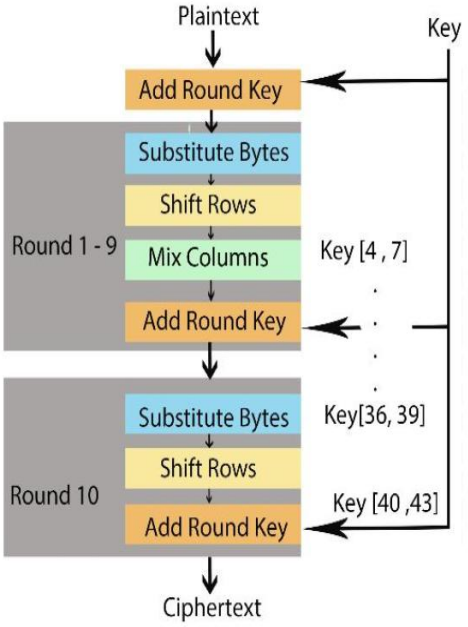


Figure 2 AES-256 encryption process [33]

3.4.Deep Feature Extraction Using CNN

A pre-trained ResNet-50 Convolutional Neural Network (CNN) is used to extract spatial and texture features that are discriminative for intelligent steganographic embedding from this preprocessed chest X-ray image. The convolutional layers learn hierarchical representations on their own, such as edges, anatomical structures and texture variations and the ReLU activation function adds non-linearity and reduces negative responses. The extracted feature maps contain detailed information about the image features which can be used to correctly identify the embedding region without influencing the diagnosticity of the image and without causing visual distortion. The convolution operation is written as:

$$F = f(W * X + b) \qquad (6)$$

Where (X) is the input medical image, (W) is the convolution kernel,(b) is the bias, (f(.)) denotes the ReLU activation function, (F) is the extracted feature map.

3.5.Machine Learning-Based Adaptive Region Selection

These deep feature vectors obtained from ResNet-50 are fed into a medical image-based optimal embedding region identification classifier called Extreme Gradient Boosting (XGBoost). Conventional fixed embedding methods do not take into account the texture complexity and local image characteristics to produce an adaptive embedding priority map as does the XGBoost. High texture complexity areas are chosen for being able to embed encrypted information with minimal perceptual distortion while hiding healthcare information in the image and also being resistant to steganalysis attacks. The prediction function is given by:

$$\hat{y} = \sum_{k=1}^{K} f_k(x) \qquad (7)$$

3.6.Multi-Layer Adaptive Steganographic Embedding

The proposed approach proposes two-layer adaptive steganographic embedding algorithm to effectively embed the encrypted healthcare data into medical images in a secure manner without compromising diagnostic accuracy of medical images. The cover image is firstly converted into 4 sub-bands in the frequency domain by Discrete Wavelet Transform (DWT). The encrypted healthcare data are then inserted to the high frequency coefficients by applying an adaptive Least Significant Bit (LSB) technique. Locations for embedding are selected by the XGBoost region selection model to minimize visual distortion and greatly improve resistance to both statistical and steganalysis attacks and enhance embedding capacity and imperceptibility. The DWT decomposition is represented as:

$$I \rightarrow \{LL, LH, HL, HH\} \qquad (8)$$

Where (LL) denotes the approximation coefficients, (LH) represents the horizontal detail coefficients, (HL) represents the vertical detail coefficients, (HH)

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 10 October 2026
Page No: 5616-5624
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0734

represents the diagonal detail coefficients. The adaptive LSB embedding is represented as

$$S = (P \,\&\, 254) \mid B \qquad (9)$$

Where (P) denotes the original cover pixel, (B) is the encrypted secret bit, (S) represents the generated stego pixel.

3.7.Performance Evaluation Metrics

Mean Squared Error (MSE)

$$\boldsymbol{MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(I_{ij} - S_{ij})^2} \qquad (10)$$

Peak Signal-to-Noise Ratio (PSNR)

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{255^2}{MSE}\right) \qquad (11)$$

Bit Error Rate (BER)

$$\boldsymbol{BER = \frac{N_e}{N_b}} \qquad (12)$$

Embedding Capacity (EC)

$$\mathrm{EC} = \frac{N_b}{M \times N} \qquad (13)$$

Extraction Accuracy

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \qquad (14)$$

4. Result And Discussion

The proposed multi-layered machine learning-based steganographic framework was evaluated using the NIH Chest X-Ray dataset to assess image quality, embedding capacity, computational efficiency, extraction accuracy, and security.The proposed framework achieved a PSNR of 54.32 dB and an SSIM of 0.978, demonstrating high image quality and effective preservation of medical image structures. The framework achieved an embedding capacity of 0.175 bpp, outperforming traditional LSB, DCT-based, and previous LSB-DCT methods in embedding healthcare information.The overall steganalysis detection rate was reduced to 31.5%, compared with 45.8% for LSB-DCT, 58.7% for DCT-based methods, and 73.2% for traditional LSB. Across medical imaging modalities, the framework achieved PSNR values of 56.8 dB for X-ray, 55.2 dB for ultrasound, 53.4 dB for MRI, and 53.1 dB for CT scans. The highest embedding capacity was obtained for MRI at 0.182 bpp, followed by CT at 0.178 bpp, ultrasound at 0.171 bpp, and X-ray at 0.168 bpp. Under different steganalysis attacks, the proposed method achieved detection rates of 28.4% for RS analysis, 24.1% for Chi-Square, 19.7% for SPA, 33.8% for machine learning, and 37.2% for deep learning. The proposed framework completed encryption in 1.72 seconds, outperforming CNN-DWT at 2.11 seconds and conventional AES at 2.54 seconds.The decryption time of the proposed method was 1.63 seconds, compared with 2.04 seconds for CNN-DWT and 2.36 seconds for AES, demonstrating improved computational efficiency under the reported conditions.The proposed framework achieved an extraction accuracy of 99.21%, outperforming LSB-DWT (96.13%), DCT (93.67%), and traditional LSB (91.24%). The integration of ResNet-50 feature extraction, XGBoost-based adaptive region selection, and DWT-LSB embedding improved the reported recovery accuracy and supported reliable concealment of confidential healthcare information.The ROC analysis reported an AUC of approximately 0.99, a TPR of 0.99, and an FPR below 0.10, indicating strong discrimination performance; further validation is needed to confirm the framework's robustness and security against steganalysis attacks.

Conclusion

The present study proposed an intelligent machine learning based multi-layered steganographic system for secure transmission of medical information through steganography approach. The proposed framework used AES-256 for encryption, ResNet-50-based deep feature extraction, XGBoost for adaptively selecting the regions and DWT-LSB

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 10 October 2026
Page No: 5616-5624
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0734

embedding for achieving a trade-off between security and image quality, which greatly enhanced the security and image quality. The experimental results showed PSNR value of 54.32 dB, SSIM value of 0.978, and the embedding capacity of 0.175 bpp, which indicates that the image was highly imperceptible while maintaining the diagnostic quality of the image. The framework also provides high extraction accuracy of 99.21%, which guarantees the embedded healthcare information extracted without significant bit loss. The proposed approach also achieved lower percentages for steganalysis detection of 28.4%, 24.1%, 19.7%, 33.8% and 37.2% for RS Analysis, Chi-Square, SPA, Machine Learning, and Deep Learning attacks, respectively, better than the existing methods. Furthermore, its encryption and decryption time were decreased to 1.72 s and 1.63 s, respectively, showing its high computational efficiency. The AUC of the ROC analysis was around 0.99, which indicates that the system has a high level of security and excellent discrimination capabilities. In conclusion, the proposed framework offers an effective, reliable, and patient-privacy oriented approach to secure healthcare information sharing in today's digital healthcare landscape.

References

[1]. Hu, Jianuo, Menglu Tang, Haoyang Qu, Dawei Zhao, Fenghua Tong, Wei Wu, and Haipeng Peng. "A Survey of Deep Learning-Based Compressed Sensing Information Hiding Techniques: Methodological Evolution and Cross-Modal Extensions." Available at SSRN 5954637.

[2]. Coman, Ecaterina, Claudiu Coman, Mihai Bogdan Alexandrescu, and Raluca-Simina Bilți. "Mapping the Frontiers of Cybersecurity and Data Protection: Insights from a Bibliometric Study." Electronics 14, no. 19 (2025): 3769.

[3]. Ghosal, Sudipta Kr, and Aditya Kumar Sahu. "AI-powered steganography: Advances in image, linguistic, and 3D mesh data hiding–a survey." Journal of Future Artificial Intelligence and Technologies 2, no. 1 (2025): 1-23.

[4]. Kanimozhi, R., and P. S. Ramesh. "Deep reinforcement learning-based intrusion detection scheme for software-defined networking." Scientific Reports 15, no. 1 (2025): 38827.

[5]. Awadallah, Abeer, Khouloud Eledlebi, Mohamed Jamal Zemerly, Deepak Puthal, Ernesto Damiani, Kamal Taha, Tae-Yeon Kim et al. "Artificial intelligence-based cybersecurity for the metaverse: Research challenges and opportunities." IEEE Communications Surveys & Tutorials 27, no. 2 (2024): 1008-1052.

[6]. Chung, Keywhan. "Machine learning in the hands of a malicious adversary: A study on ML-driven malware." PhD diss., University of Illinois at Urbana-Champaign, 2022.

[7]. Nelsonmandela, Dr Murugan R., Solomon Jebaraj, Manju Bargavi SK, and R. Raghavendra, eds. "Conference Proceedings 21 & 22 March, 2025 International Conference On TechWork." In Proceedings of the 38th International Conference on Machine Learning, pp. 10430-10441. by:- Book Rivers HN 22 Kanchan Nagar Kalyanpur Lucknow UP, 2021.

[8]. Krishna, D. Shivarama, and M. Nagaratna. "A COMPARATIVE ANALYSIS OF A HYBRID CRYPTOGRAPHIC FRAMEWORK FOR SECURE IMAGE TRANSMISSION IN CLOUD ENVIRONMENTS." Advanced Engineering Sciences 58, no. 1 (2026): 2343-2359.

[9]. Shetty, Swapnil, and R. P. Puneeth. "Secure Image Steganography with GAN

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 10 October 2026
Page No: 5616-5624
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0734

Architecture: A High-Fidelity and Robust Data Hiding Approach." In 2025 9th International Conference on Electronics, Communication and Aerospace Technology (ICECA), pp. 1999-2005. IEEE, 2025.

[10]. Saadaoui, Naima, Boukhamla Akram Zine Eddine, Narima Zermi, Amine Khaldi, Mohamed Redouane Kafi, and Aditya Kumar Sahu. "Frequency domain watermarking of medical images based on fractional discrete Cosine, Mellin, and Schur transforms." Multimedia Tools and Applications 85, no. 3 (2026): 204.

[11]. Gupta, Reetu, Priyesh Kanungo, Nirmal Dagdee, Golla Madhu, Kshira Sagar Sahoo, N. Z. Jhanjhi, Mehedi Masud, Nabil Sharaf Almalki, and Mohammed A. AlZain. "Secured and privacy-preserving multi-authority access control system for cloud-based healthcare data sharing." Sensors 23, no. 5 (2023): 2617.

[12]. Asokan, R., V. Malathy, and Dineshkumar Thangaraju. "A Hybrid Chaotic Model with Steganography to Improve Image Security." In 2025 International Conference on NexGen Networks and Cybernetics (IC2NC), pp. 168-173. IEEE, 2025.

[13]. Norchayev, Mirjalol, Toshpulat Oqboyev, Nurali Islamov, Abbos Sattorov, Malohat Yaxshiyeva, Zahraa Eisa, and Mustafa Ali Alwash. "Privacy-Preserving COVID-19 Screening Using Homomorphic Encryption and Logistic Regression." In 2025 3rd International Conference on Cyber Resilience (ICCR), pp. 1-7. IEEE, 2025.

[14]. Nadhan, Archana S., and Jeena Jacob. "Next-Gen Image Shielding: Deep Learning's Stealthy Image Encryption for Health-Tech IoT." In 2023 International Conference on Recent Advances in Science and Engineering Technology (ICRASET), pp. 1-6. IEEE, 2023.

[15]. Cina, Elda, and Edmira Xhaferra. "A Novel Steganographic Framework Using Spiral Path Traversal and Data Compression Techniques." In 2025 5th International Conference on Electrical, Computer and Energy Technologies (ICECET), pp. 1-6. IEEE, 2025.

[16]. Malik, Varun, Mudassir Khan, Punam Bhoyar, Kimmi Gupta, Mohammed Ashfaq Hussain, Kavita Arora, and Barga Mohammed Mujahid. "StegoSec-EHR: A blockchain-enabled IoTFramework for secure HER sharing via steganography in genetic disease diagnosis." Peer-to-Peer Networking and Applications 18, no. 6 (2025): 325.

[17]. Haque, Md Ashraful, Mahafujul Haq Riad, Maruf Billah, Jun-Jiat Tiang, Narinderjit Singh Sawaran Singh, Hanaa A. Abdallah, and Abdelhamied A. Ateya. "Ultra-Wideband Multi-Resonance High-Performance Graphene-Enhanced Multi-Square Slotted 2-Port MIMO Antennas with Machine Learning-Driven Optimization for 6G Terahertz Communication." IEEE Access (2026).

[18]. Sanjalawe, Yousef, Salam Al-E'mari, Salam Fraihat, Mosleh Abualhaj, and Emran Alzubi. "A deep learning-driven multi-layered steganographic approach for enhanced data security." Scientific Reports 15, no. 1 (2025): 4761.

[19]. Aljughaiman, Ahmed, and Rana Alrawashdeh. "Content-adaptive LSB steganography with saliency fusion, ACO dispersion, and hybrid encryption with ablation study." Scientific Reports (2025).

[20]. Malik, Kaleem Razzaq, Muhammad Sajid, Ahmad Almogren, Tauqeer Safdar Malik, Ali Haider Khan, Ayman Altameem, Ateeq Ur

Rehman, and Seada Hussen. "A hybrid steganography framework using DCT and GAN for secure data communication in the big data era." Scientific Reports 15, no. 1 (2025): 19630.

[21]. Fatima, Kanza, Nan-I. Wu, Chi-Shiang Chan, and Min-Shiang Hwang. "A High-Payload Data Hiding Method Utilizing an Optimized Voting Strategy and Dynamic Mapping Table." Electronics 14, no. 17 (2025): 3498.

[22]. Flores-Quispe, Roxana, and Yuber Velazco-Paredes. "Chaotic-Map-Based Image Steganography Using Bernoulli and Logistic Functions." (2025).

[23]. Musa, Nura Shifa, Thangavel Murugan, Nasurudeen Ahamed N, and Nada Masood Mirza. "Research study on securing the cloud: utilizing conventional and blockchain-based access control mechanisms." Journal of Cloud Computing 14, no. 1 (2025): 88.

[24]. Ahmad, Shahnawaz, Justin Onyarin Ogala, Festus Ikpotokin, Mohd Arif, Javed Ahmad, and Shabana Mehfuz. "Enhanced cnn-dct steganography: Deep learning-based image steganography over cloud." SN Computer Science 5, no. 4 (2024): 408.

[25]. Basani, Dinesh Kumar Reddy, Sri Harsha Grandhi, and Qamar Abbas. "A Centralized Infrastructure-Aware Reliable Data Transaction Model in IoT-Enabled MANET and Cloud Using GWO and Attention Mechanism with LSTM: Attention Mechanism with LSTM." International Journal of Advanced Research in Information Technology and Management Science 1, no. 01 (2024): 110-134.

[26]. Dyavani, Narsing Rao, Charles Ubagaram, Venkat Garikipati, Bhagath Singh Jayaprakasam, Rohith Reddy Mandala, and M. Thanjaivadivel. "Adaptive Access Control in SHACS: Leveraging Markov Models and Topological Data Analysis for Enhanced Cloud Security." International Journal of Innovative Technology and Creative Engineering 14, no. 1 (2024).

[27]. Guan, Quanlong, Jiawei Lei, Chaonan Wang, Guanggang Geng, Yuansheng Zhong, Liangda Fang, Xiujie Huang, and Weiqi Luo. "BI-FERH: Blockchain-IoT based framework for securing smart hotel." Computer Science and Information Systems 20, no. 4 (2023): 1541-1568.

[28]. Ahmad, Shahnawaz, Justin Onyarin Ogala, Festus Ikpotokin, Mohd Arif, Javed Ahmad, and Shabana Mehfuz. "Enhanced cnn-dct steganography: Deep learning-based image steganography over cloud." SN Computer Science 5, no. 4 (2024): 408.

[29]. Kanimozhi, R., and P. S. Ramesh. "Deep reinforcement learning-based intrusion detection scheme for software-defined networking." Scientific Reports 15, no. 1 (2025): 38827.

[30]. Moghadasi, Hojat Allah, and Hamid Dehghani. "Assessment of a VoIP steganalysis method based on statistical analysis and deep neural network." Scientific Reports (2025).

[31]. Tiwari, Anurag, and Manuj Darbari. Emerging trends in computer science and its application. Boca Raton, FL, USA: CRC Press,2025.https://www.kaggle.com/datasets/nih-chest-xrays/data?

[32]. Alrawashdeh, Rana, Sultan Almuhammadi, Mahmood Niazi, Mufti Mahmud, and Md Mahfuzur Rahman. "Secure edge-guided adaptive image steganography using HED-based attention maps and CNN." Scientific Reports 15, no. 1 (2025): 42984.