Received: 31 May 2025 | Revised: 14 October 2025 | Accepted: 23 December 2025 | Published online: 30 December 2025

REVIEW

Artificial Intelligence and Applications
2025, Vol. 00(00) 1-10
DOI: 10.47852/bonviewAIA52026322

BON VIEW PUBLISHING

A Systematic Investigation of the Current State of Security in Electronic Medical Images: 2019–2024

Divya Sharma[1] and Chander Prabha[1,*]

[1] *Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India*

Abstract: Currently, there is a need to study the state of development of data-hiding techniques for securing electronic medical images (EMIs) when being transmitted or when stored on third-party storage. EMIs are large-sized and are of varying dimensions. Thus, they are commonly stored in third-party cloud storage. Because EMIs are accessed in real time, data-hiding techniques need to be lightweight and secure to ensure reduced computational time complexity. The research goal of this article is to study the state of research work that has been done to secure EMIs. A total of 147 articles were studied, focusing on e-health data and their security from 2019 to 2024. This paper focuses on the challenges that the conventional techniques face. The results found in this research article have been organized to help future researchers understand the trends in the programming language currently being used, their research goals, the achievement of these goals, the time required for these techniques, and the dataset on which the proposed techniques were evaluated. There is a tabulated study on the commonly used programming language. This research also provides an in-depth study of the currently popular performance metrics used, with a graph-based comparative analysis of their achieved results.

Keywords: privacy, security, e-health data, electronic medical images, steganography, cryptography, computational complexity

1. Introduction

Digital data [1] or multimedia data [2] are raw forms of information. Digital data exist in various types: text, image, audio, and video [2–9], as shown in Figure 1. Digital data are created, updated, modified, and deleted on a computer with the help of computer peripheral devices [10]. With the growth of Internet users, digital data can be easily accessed. Digital texts are sentences or words written in a computer word file. Popular digital text formats are PDF, DOC, TXT, etc. [11]. Digital speech or audio signals are generally represented by Motion Picture Expert Group (MPEG) Audio Layer III (MP3) [6, 12], Apple Lossless Audio Codec (ACC), waveform audio file format (WAV) [12], etc. [13–15]. Digital images are colored or grayscale. The commonly known formats are Joint Photographic Expert's Group (JPEG) [16–19], Portable Network Graphics (PNG) [6, 20], Graphics Interchange Format (GIF) [21], Tagged Image File Format (TIFF), Bitmap image format (BMP) [18, 20], etc. [5, 11]. Digital videos combine audio with images as frames. The popular video formats are Audio Video Interleave (AVI), MPEG, MPEG-4 [21], MPEG 2 [21], etc. [11].

Big data is popular as it stores vast amounts and various types of digital data [22]. The various areas of application for big data include e-health [23–25], social networking websites [26], e-commerce, weather forecasting, stock market analysis, and the Sensex. Electronic health care records (EHRs) are diverse and are saved as big data [27, 28]. EHRs are records of patient personal data such as name, Aadhar number, permanent account number (PAN), father's name, mobile number, payment details, body weight, and blood pressure [29] in the form of table records along with X-ray [30], CT-scans, etc., as medical images and laboratory reports of a blood test, test reports, etc., in the form of PDF. EHRs as big data are large and complicated [31]. The size of big data can usually range up to terabytes, exabytes [32], or even petabytes [23, 32]. Big data is classified into three types based on its structure [33, 34].

1) Structured big data: digital data in the form of tables have rows and columns, thus called structured big data, such as Excel and CSV.
2) Unstructured big data: it has no defined structure, such as social media records, e-health [35], images, and videos [23].
3) Semi-structured big data: it is a combination of structured and unstructured big data. Examples: e-mail, archive file ZIP, Extensible Markup Language (XML), etc.

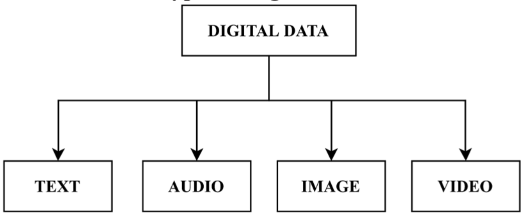
The 9 Vs [22, 25, 26], which form the major characteristics of big data [35], are depicted in Figure 2.

The various areas where big data is being used are online banking [36], online shopping, e-health care [23], stock market, government, education, transportation, energy, smart city [37, 38], applications, utilities, public sector (such as power grid, surveillance, and public welfare) social networking sites, entertainment, manufacturing industry [23], etc.

Electronic health care records (EHRs) are the records of a patient's history, doctor's prescription, lab test reports, X-rays, personal details, payment details, insurance details, etc. Because these EHRs involve more than one patient and record their entire medical history, they are large and all belong to different file formats. X-ray images are available in JPEG format, a lab test report is a PDF, and personal details are saved as part of an XLSX file. Therefore, EHRs are saved as big data, which deals with more than one file type.

***Corresponding author:** Chander Prabha, Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India. Email: chander.prabha@chitkara.edu.in

Figure 1
Types of digital data



Electronic medical images (EMIs) are commonly identified as medical images such as X-rays, CT scans, and MRIs. Usually, X-ray images are acquired from different body parts, such as the chest, legs, and arms, and from different patients of various age groups. Thus, EMIs vary in dimensions and sizes. EMIs are a part of EHRs. As the EHRs are usually large, they are usually stored by hospitals on third-party storage such as the cloud while being transferred over the Internet. The security of these EHRs when transferred or stored should be ensured. The previous articles were studied, focusing on parameters such as security, EHRs, and research work done to secure EHRs during the years 2019–2024.

Data-hiding techniques are used to ensure the security and privacy of the data. There are three types of techniques: Cryptography is the process of converting plain text into ciphertext, which is non-understandable. Cryptography involves the processes of encryption and decryption. Steganography is the art of hiding data to make them seem invisible to the reader. Watermarking leaves a mark on digital data for copyright purposes. Figure 3 presents the word cloud diagram of the popularly used data-hiding techniques. This shows that the chaotic map is currently the most popular technique used as it ensures randomness. Randomness ensures the confusion and diffusion properties of cryptography. Least significant bit (LSB) steganography is popularly used as it is simple to implement and understand and only a single bit of data is modified. Other researchers have implemented data techniques such as discrete wavelet transform (DWT), integer wavelet transform (IWT), and singular value decomposition (SVD). These data-hiding techniques implement steganography or cryptography, as shown in Figure 3.

1.1. Research contribution

1) A detailed tabulation of the currently popular data-hiding techniques used for securing EHRs or images is mentioned, with the goal that led to their research, and the objectives that they achieved.
2) A critique analysis is presented on the popular online databases used for downloading the dataset, the commonly used programming language used by researchers, and the details of the dataset (e.g., the cover and secret dataset details), performance evaluation tests, and computational time-based comparison.
3) This research also explores the challenges faced by researchers.

1.2. Article selection criteria

The article selection criteria are based on previously published articles during the period 2019–2024. They are based on keywords such as EMIs, security, privacy, cryptography, and steganography. Figure 4 presents the number of occurrences of the mentioned keywords in the studied works. The list of keywords that were used to identify the previous articles is shown in Figure 4. Most previous researchers have implemented cryptography and/or steganography as the data-hiding technique. These researchers have focused on enhancing the security of images or EMIs or on dealing with EHRs.

The data include all types of articles, such as research articles, review articles, early access, and book chapters. All articles were in the English language only. To know the research trends and security techniques in the field of EMIs, all articles from 2019 to 2024 were included. The steps are shown in Figure 5.

1.3. Structure of this paper

This article is divided into five sections. Section 2 presents a comparative tabular analysis of the work done by previous researchers based on research goals, data techniques proposed, programming languages that they used for implementing their proposed techniques, etc. In Section 3, the challenges occurring in the previous technique are highlighted. Section 4 presents the performance tests, which previous researchers have used with their formulae, and finally, in Section 5, the conclusion and future scope of this article are illustrated.

Figure 2
9 Vs of big data

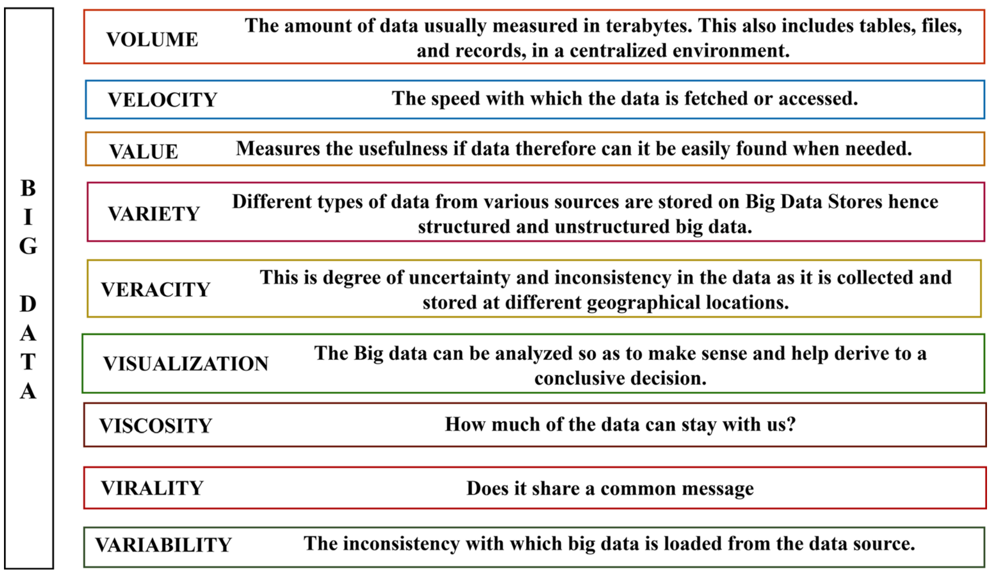
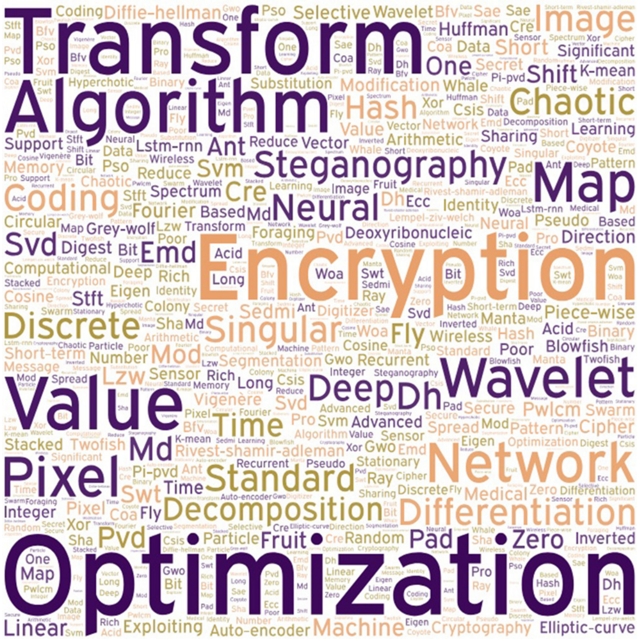


Figure 3
Popularly used data-hiding techniques



2. Comparative Analysis of the Work Done by Previous Researchers

Various papers have been studied based on the selection criteria of the articles. The tabular analysis is presented in Table 1, which studies research articles based on their research goal, techniques proposed by previous researchers, and results that they achieved.

From Table 1, it could be deduced that researchers have focused on using a hybrid technique, which is a combination of two or more conventional data-hiding techniques. The commonly used conventional techniques, such as AES and DES for encryption and LSB for steganography, have been studied based on their frequency. This has been graphically depicted in Figure 6.

Figure 6 depicts that most previous researchers used chaotic map-based encryption, while LSB steganography is commonly implemented. Then, DWT, AES, SHA, and ECC have been used. Many previous researchers have implemented hybrid steganography with cryptography or watermarking. The use of a hybrid technique will ensure the properties of both techniques. A tabulation of the programming language used by previous researchers is shown in Table 2.

MATLAB is the most widely used programming language (PL) by previous researchers, as shown in Table 2. The second most popular programming languages were Python and Java. In this article, a study on the database from which the dataset has been downloaded is shown in Table 3.

From Table 3, it is clear that Kaggle, MedPix, and USC-SIPI were the commonly used online databases for downloading datasets. A tabulated study of the dataset used by the previous researchers, based on their cover data and secret dataset details, is shown in Table 4.

From Table 4, it can be deduced that most of the previous researchers have hidden text by converting it into ASCII inside an image. Those researchers who have hidden medical images have normalized these images about their sizes. Reducing the sizes of these images will render them unreadable and non-understandable to medical professionals for medical diagnosis in case of medical emergencies.

3. Challenges in the Previous Techniques

The limitations of the conventional techniques mentioned by the above researchers in their research work are the following:

1) There is a lack of trust in third-party users. There is a need to ensure integrity and confidentiality in EHR information sharing [1].
2) LSB has less hiding capacity and is less robust against attacks. Bit plane lacks data-hiding capacity and security. Pixel value difference (PVD) is not robust against various attacks, and image visual quality is degraded. Attacks on pixel intensity modulation data render them unacceptable. IWT with a chaotic map is less robust. DFT

Figure 4
The number of occurrences of the mentioned keywords in the studied works

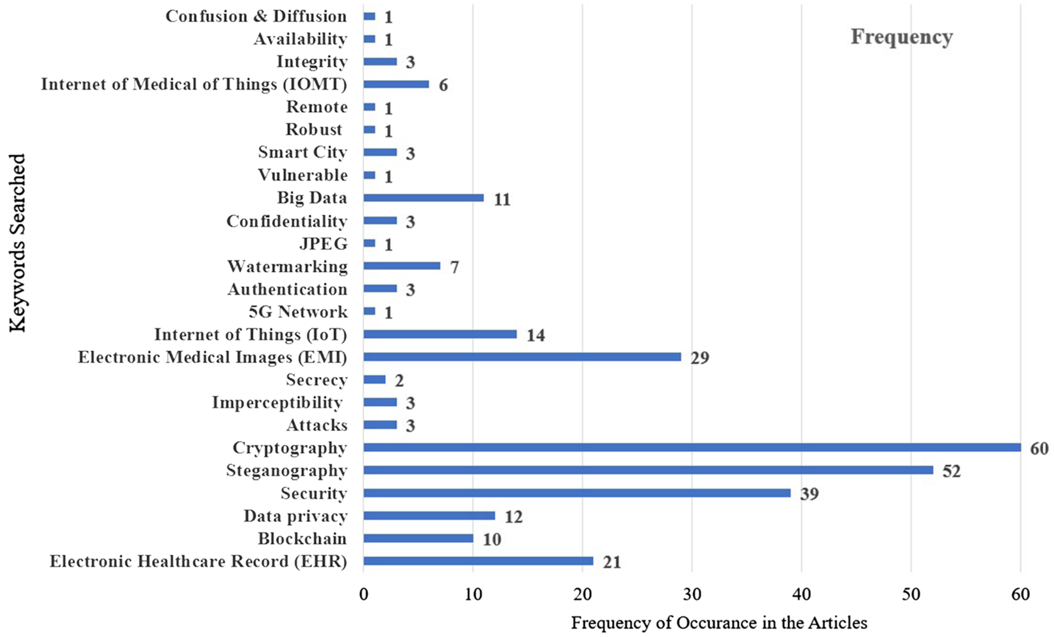


Figure 5
Article selection criteria

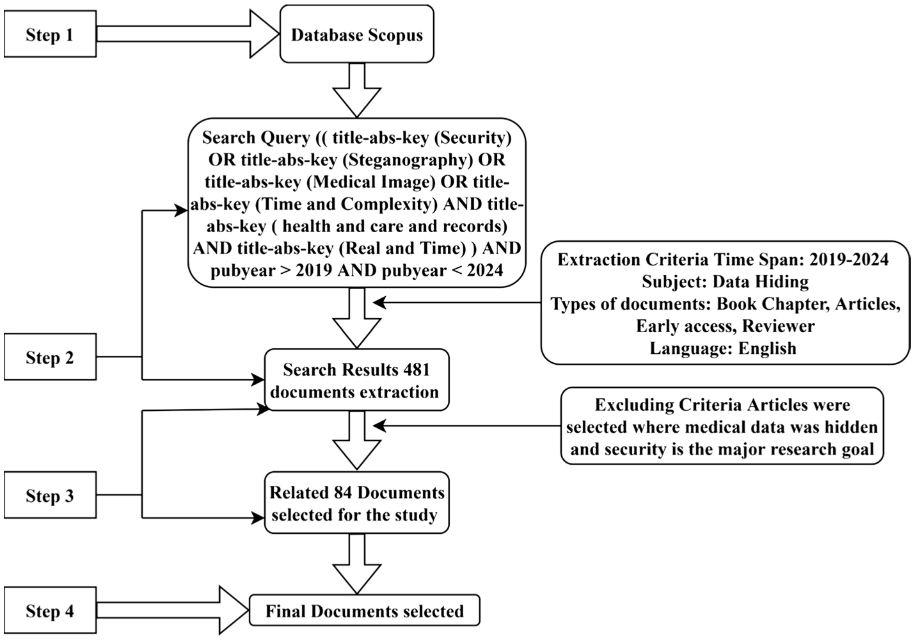


Table 1
Prevalent research work based on research goal, proposed technique, and achievement

Cited as	Research goal	Proposed technique	Achieved
[39]	Patient data security over network communication	DNN-based steganography where LSB, DCT, DWT, & binary pattern complexity	Image quality is retained
[40]	Securing medical images while being transferred	LSB steganography	Resistance to various attacks
[41]	Data security and privacy in IoT	-----	Integrity and confidentiality
[23]	Structured or unstructured big data security while retaining performance during transmission over a network	MapReduce mechanism and cluster normalization technique	Improved security, reliability, less packet size, packet loss, packet dropping, error rate, and packets are affected due to attack and congestion
[42]	Detect fingerprints in audio steganography	Study on Xiao Steganography, Invisible Secrets, deep sound audio steganography detects stego-audio across WAV files	Highly effective and practical
[43]	Reliable wireless communication safeguards health information from storage	Wireless sensor network (WSN)	Lightweight encryption technique, safety against inside & outside attacks, with patient data privacy
[44]	Data privacy and security of medical data	Homomorphic Brakerski–Fan–Vercauteren (BFV) with DL model	Secure multi-party computation
[45]	Data security and privacy on cloud computing storage with enhanced computational power	RSA, AES, and IBE algorithms alongside LSB	Flexible, efficient, secure, protection, confidentiality, privacy, and integrity from attackers
[46]	To develop a deep learning-based secure searchable blockchain as a distributed database using homomorphic encryption for secure access and search data	Novel method on blockchain allowing remote encryption to users and upload to the distributed ledger	Improved security, immutability, tamper resistance, secure data, reduced breaches to health care data, more efficient blockchain-based IoT system compared to benchmark models

Table 1
(Continued)

Cited as	Research goal	Proposed technique	Achieved
[47]	Security of sensitive patient data from hackers	Nth Degree Truncated Polynomial Ring Unit (NTRU) compression and LSB encrypted a text message into an audio file	Significantly better PSNR, MSE, and embedding capacity (EC)
[48]	IoT empowering sensitive e-health care data suffers from challenges such as security, privacy preservation, QoS, and network lifetime	Cross-layer and cryptography-based secure routing (CLCSR), which performs attack detection, privacy preservation, and secure data transmission	Stable, reliable route selection, lightweight cryptography authentication for privacy preservation, and energy-efficient
[49]	Selfie-based data hiding to reduce suspicion	Eigen-based steganography	More robust against compression attacks, JPEG compression, clipping, and scaling
[50]	Confidentiality and protection of patient information in DICOM image transmission in e-health service	Arithmetic coding with DES, then fixed LSB position hiding, followed by integer wavelet high-frequency transform	High confidentiality, quality, EC, robust, outperforms existing algorithms, lower imperceptibility, can be applied to hospitals worldwide
[51]	Good steganography ensuring privacy & secrecy of big message	Vigenère cipher and LSB steganography	Confidential, exact retrieval of hidden messages, imperceptible, and secure
[52]	Reliable, confidential Internet-based exchange of EMRs & EMIs for patient diagnosis, geographically separated	LSB of integer wavelet transform	Better PSNR, MSE, R, secure, imperceptible, and enhanced confidentiality
[53]	Confidentiality of information hiding in the ECG-TP segment	Long short-term memory recurrent neural network (LSTM-RNN) for hiding in the TP segment of ECG	Better results in the frequency domain, reduced computational complexity, more effective than LSB, and no visual distortion in the achieved ECG
[54]	Security of medical data	Logistic equation, then hyperchaotic equation, then DNA lossless computational secret image sharing (CSIS), pseudo random number (PRN), & XORed, secret sharing (SS)	Require few resources such as storage capacity, transmission bandwidth, high security against attacks, and strong key sensitivity that withstands statistical & differential attacks
[55]	Security and privacy of ECG and patient metadata over a public network	The hybrid of IWT & modified-LSB (IWT-m-LSB) in the pivotal QRS-region, while pixel inverted pixel value differentiation (PI-PVD) in the non-QRS region, then 1D combined logistic-sine (CLS) chaotic map	Large key space and high key sensitivity, yielding excellent results, a highly efficient and authentic approach
[56]	Health care systems are suffering from data breaches, & protected with privacy	LSB, with AES-256, RSA, with K-means algorithm, with segmentation	Robust encryption and high validation
[57]	Solve the centralized data island problem in the blockchain of the health care service system, protect cross-institutional EMRs sharing security while improving quantum resistance	On-chain ledger and off-chain storage (OLOS) with secure keyword-searchable attribute-based encryption (KS-ABE)	Lesser communication costs, small key sizes, security against adaptive chosen-keyword, & adaptive chosen-policy attacks in the random model while being very efficient & good performance
[58]	When a patient's medical image is transmitted between centers, to allow faster & proper diagnosis for COVID-19	EIS-SDT & manta ray foraging optimization algorithm, then double logistic chaotic map (DLCM) encryption, whale optimization algorithm (WOA), followed by gray-wolf optimization (GWO)	-----
[59]	Protect the cardiac database against unauthorized access	Daubechies wavelet transform & then conducted energy packing efficiency-based compression. Steganography followed by public key cryptography	Effective, secure, stable, potential use in telemedicine with data integrity, confidentiality, increases accuracy, & protection from unauthenticated access

Table 1
(Continued)

Cited as	Research goal	Proposed technique	Achieved
[60]	Security by chaos-based image is commonly used in telemedicine IoT while overcoming vulnerability from attackers	Stacked auto-encoder (SAE) network-based shuffling and generation of the independent chaotic sequence	Robust, reduced runtime, complexity, security, efficient, & immune to various attacks (statistical attack & noise immunity)
[61]	To secure efficient transmission, sharing, & updating of large amounts of medical information among hospitals on a communication channel while ensuring confidentiality, integrity, & data availability	The particle swarm optimization (PSO) algorithm then hashes the secret COVID-19 data LSB	Confidentiality, high embedding capacity, high image quality, security, and data availability
[62]	Efficient and secure encryption of images	2D piecewise smooth non-linear chaotic map cryptography (2DPSNCM)	Secure, fast, resistant to various attacks (correlation, sensitivity, key, noise, and chosen plaintext), & efficient encryption
[63]	Security and privacy of multimedia data transmission over the Internet of Everything (IoE) network	SVD & coyote optimization algorithm (COA) with poor and rich optimization (PRO), then multi-key homomorphic encryption with steganography approach for multimedia security (OMKHES-MS)	------
[64]	Privacy-preserving, secure, reliable health care service to legitimate patients on IoMT in TMIS with attack resilience & anonymous key exchange	Secure anonymous lightweight three-factor-based privacy preserving schema (SALS-TMIS)	Superior security, efficiency, threat resistance, prevention of attacks, scalability, mutual authentication, low computational & communication cost
[65]	Secure COVID-19 government & medical practitioners use for travelling passengers on telemedicine	Noval chaos with SHA-256 & AES-256 then Pavillier cryptosystem with Inter-Planetary File System (IPFS) & Authentication Data Table (ADT)	It is well protected against (brute force, dictionary, advanced dictionary, lookup table, & rainbow table) attacks, & privacy
[66]	Privacy & confidentiality of data with the growth of online information transfer	Secret collective agreement, counting & matrix-based secret sharing with LSB with DWT, followed by XOR encryption	Simple, intuitive, secure, robust, & no quality deterioration
[67]	Data security in mobile computing using IoT in health care	Data normalization using logistic regression & principal component analysis (LR-PCS) with genetic algorithm-based feature selection, then kernel homomorphic two-fish encryption (KHTEA) & exponential Boolean spider monkey optimization (EBSMO)	Effectively protect, high-security level, increased efficiency
[36]	Cloud medical image repository	2-tier security of medical image, 3D Lorenz chaotic attractor, then DNA, then 1D tent map	Resistance to statistical attack, integrity, & confidentiality
[68]	Safety and security of medical information while maintaining quality and efficiency	Modified AES algorithm	Outperforms existing encryption time with a small avalanche effect if the file size is large, less complex, enhanced security, & confidential
[38]	IoMT is vulnerable to attacks to provide quick, real-time analysis, secure, & private access to health care data while mitigating blockchain & fog computing	Fog & BC-based framework for IoMT	-------
[69]	Secure, confidential, and integrity transmission of massive medical data between hospitals	Virtual private network (VPN) or blockchain, hybrid cryptography where embedding, three iterations of Henon map, & inverse method, thus blocks & pixels random selection (BPRS), ElGamal EEC	Increased capacity, imperceptibility, and security while avoiding existing method problems, efficient security, robustness, & immunity against unknown attacks

Table 1
(Continued)

Cited as	Research goal	Proposed technique	Achieved
[70]	Safety, confidentiality, security & reliability of IoT health care systems from hackers & theft, from large health centers & hospitals	Blockchain-based transactional inheritance, then secure storage across multiple servers, then authorization-based access, then SHA-256, then LBSS	Decreased average processing time, rate of miners, energy consumption, end-to-end delay, and access time while increasing throughput, being lightweight
[71]	Authentication of medical image steganography	Support vector machine (SVM) & IWT steganography with circular array and shared secret key	Imperceptibility, robust, confidentiality, & more security, as it is difficult for attackers to extract patient's valuable information
[72]	While maintaining image quality and payload, robust image steganography ensures security and protects against attacks	Vigenère cipher and Huffman coding encryption, then the knight tour algorithm, then an arbitrary function with exploiting modification direction (EMD)	More efficient, robust, image quality retained, increased capacity, secure, and robust
[73]	Information security when transmitted over a public network	Pixel value differentiation (PVD)	Increased capacity, visual quality, can withstand attacks, & robust
[74]	Secure and private communication over an insecure medium for IoMT	Zero steganography with LSB/DCT transform	Robustness against filter, compression, addition of noise, 100% retrieval of payload upon extraction after low pass filter attack, & 100% payload retrieval against JPEG compression attacks, imperceptible, secure, & extraction possible from severe degradation
[75]	Protection & security of information while communicating on the Internet	Segment-based steganography in the blue layer using MOD FACTOR 4 while changing the threshold	High PSNR, low MSE, secure, resistant to statistical attacks (RS, histogram, & chi-square analysis)
[76]	Confidentiality, integrity, & availability of data on the Internet	Multi-level encryption algorithm (MLEA)	Improved strength, intangibility, security, and better performance
[77]	Implementing audio steganography to achieve more security and protection from unauthorized access	Short-time Fourier transform (STFT) & piece-wise linear chaotic map (PWLCM) based on bit-level encryption with DWT	Superior performance, confidentiality, retaining quality, more security, good restoration quality, and fewer changes
[20]	Secure classified information steganography maintains visual quality	AES-256 & then SHA-256, followed by LSB steganography	Enhanced security level, retained quality, indetectable, robust, secure from hackers, & imperceptible
[6]	Confidentiality of health care records for secure transmission	Privacy-preserving hybrid AES-128 & Diffie–Hellman encryption + LSB	Faster, minimal image distortion, and more secure
[78]	Medical data & image security during transmission health care system in telemedicine as an AI approach for RTA watermarking	SVD chaotic encryption using ECC, followed by AES & then 2D-DWT, then a fingerprint-based authentication schema	Medical image quality retained, visually secure, without secret key integrity, authentic, confidentiality, & better performance
[79]	Image security & payload capacity concerns while transmitted on the Internet	Hybrid layers of security compression using DWT & AES-128 encryption, followed by LSB	68% image quality, secure, output a distortion-free image, & good quality of stego-image
[80]	To provide security & maintain the confidentiality of medical images transmitted on an open-source network	Selective digitizer medical image encryption (SEDMI) with DNA-based cryptography & dual hyperchaotic map technique	Resistant to different various attacks, less computation time 0.236 s, suitable for RTA, good quality, efficient, & enhanced security levels
[81]	Secure data on cloud storage	Hybrid AES, then Blowfish, & MD5	Speedy, robust encryption, & efficient
[82]	Securing medical images on IoT	Hybridized visual cryptography with optimal ECC & then elliptic score-based key enumeration algorithm (ESKEA)	Confidential, reduces file size by 45.76%, 24.97%, 15.86%, 33%, and 33.86%, achieved 6.89% higher security, efficient, accurate, & optimal solution

Table 1
(Continued)

Cited as	Research goal	Proposed technique	Achieved
[25]	Mobile Internet, ensuring security, & confidentiality, allowing generation & transmission of large medical images & pathological models on public networks	Privacy-preserving recognition network, medical privacy-oriented VC-based recognition (MPVCNet), then visual cryptography blind watermarking, trusted computing environments (TEE)	Maintain trustworthiness, protection, privacy, efficient, secure, suitable smart devices, & low computing power
[83]	Security, confidentiality, integrity of medical images from malicious users for timely & successful diagnosis	Extended visual cryptography with hash-like function circular shift encryption (CRE), then LSB–MSB, then SHA-256	High hiding capacity & lower distortion in visual quality while maintaining integrity
[84]	Protecting colored medical images from intruders or penetrators	Private key-based encryption	Good encryption, a highly secure encrypted image is more distorted
[85]	Secure storage & transmission of medical data	DNN and convolution block attention module (CBAM) & then zero watermarking based on depth over parameterized VGG (DO-VGG)	Resistant to common & geometric attacks, improved security, robust, invisible, integrity, better than compared schemas, & lossless watermarking
[86]	Information security, biometric, and medical image encryption based on AI	Convolutional neural network (CNN) & batch normalization, then rectified linear unit (ReLU) & two-dimensional sine logistic modulation map (2D-SLMM), followed by tent logistic map (TLM) & then chaotic magic transform (CMT), together named Deep Enc, using the one-time pad	High-security level, efficiency, high speed, sensitivity to secret keys, & high degree of robustness against various attacks
[87]	Medical multimedia communication requires enhanced security	Deep learning-based enhanced cryptography hybrid chaotic Lorentz map diffusion, then DNA with hyper chaotic system, & MD5	More resistant to known chosen plaintext attacks, robust, secure, privacy, high level of security, & efficient performance
[88]	Securing data by encryption before transmission to the cloud over the Internet	IWT, then ant colony optimization, then ECC to enhance the security of medical image management (ACO-ECC-SMIM)	Improved performance, superiority, security, large capacity, & high level of security
[31]	To protect the confidentiality, reliability, & availability of digital images on online processing applications to storage tools, computer networks, & wireless communication	Multilayer 2D spatial convolution processing network (MCPN)-based cryptography, 2D spatial fractional-order convolutional operations, SPCM-based key generator	Satisfactory decryption performance, promising capabilities to protect the data confidentiality, secure communication, data recoverability, & data availability of digital images
[89]	Chaos-based encryption of medical images while being transmitted on TCP/IP	Discrete logistic, Arnold Cat and Baker chaotic map system based on the iterative map 3DES	Simple, speedy, efficient, secure, robust, reliable, larger key size, high performance, dependable, and feasible cryptography
[90]	IoMT security on a cloud platform for efficient storage and safe transfer of medical images	RSA-based Arnold map (RSA-AM), hostile orchestration (HO), and then obstruction bloom breeding optimization (OBBO)	Effectiveness, less memory, less ambiguity, quality control, & enhanced security level
[91]	Medical image encryption	Mean shift algorithm, then fractional order hyperchaotic system with embedding doctor-patient information SHA-256, DWT, & SVD	Robustness, security, & good performance against various attacks with key sensitivity
[92]	EHRs in cloud computing provides larger storage at a minimum cost	Obfuscation technique, then ECC	Confidential, integrity, minimum data theft, data leakage, high security level, low cost, small key size, better performance, efficiency, better computational & communication time, throughput rate, & turnaround time

Table 1
(Continued)

Cited as	Research goal	Proposed technique	Achieved
[93]	Secure recording and sending of IoT images	Lightweight encryption algorithm, DWT watermarking, then DCT, and then Lempel-Ziv-Welch (DCT and LZW)	Energy efficient, low hardware complexity, secure image transmission, lossless compression, & lightweight encryption
[94]	Efficient medical image watermarking	Noval medical image watermarking (MIW), homomorphic transform (HT), redundant-DWT (RDWT), SVD, & 2D chaotic Arnold transform (AT)	Better robustness, imperceptible, enhanced against various attacks, & superior performance can be implemented for RTA
[95]	Telemedicine and e-health care medical image transmission	Chen's hyper chaotic map and then Lorenz chaotic sequence, then zig-zag transform, followed by DNA cryptography & SHA-512	Better security level, efficiency, performance, integrity, confidentiality, & less complexity time
[96]	Information hiding in medical images for secure transmission on the communication medium	LSB then 1D piece-wise tent chaotic map, then 2D piece-wise smooth chaotic map (2DPSCM), followed by secret key encryption	Imperceptible, image quality retained, and resistant to chi-square attacks
[97]	Medical images include confidential data about patients; thus, efficient security is needed	DNA then 1D tent and logistic chaotic map, followed by SHA-256 and MD5, followed by XOR operation	Good encryption, resistant to chosen/known-plaintext, cropping/noise, statistical, & brute-force attacks, secure, performance, & efficient embedding for RTA
[98]	To develop a scalable, lightweight framework based on blockchain, as modern health care is complex & requires secure storage for IoMT	Merkle tree data structure for hashing & lattice-based cryptography, then homomorphic proxy re-encryption scheme, secure storage using blockchain inter-planetary file system	------
[99]	Cloud-based Healthcare 4.0 secure processing & privacy-preserving	Block chain-based edge & fog computing cloud, followed by lightweight cryptography, & then ECC with ECC-Diffie–Hellman (ECDH) & ECC-digital signature (ECDS)	High computational efficiency & security
[100]	Hiding patient medical data to protect privacy	Reed–Solomon coding	Accurate extraction, superior quality, high accuracy, image quality retained, error-free, superior performance for various densities of salt and pepper
[101]	Authenticity, integrity, and security	ECC & AES-256	Authenticity, integrity, performance, secure, & efficient
[102]	Medical images carrying sensitive patient data protection from unauthorized access over the Internet	Random phase with transposition method encrypted & phase grating as 32 cross-sectional CT-scan images	The extracted image is of good quality & robust against attacks
[103]	Security from attackers & hackers attempting to steal patients' confidential records, as the current solution lacks efficiency, as they face a high number of security breaches. Develop a more efficient algorithm that achieves authenticity, confidentiality, & integrity while resisting security threats	Hybrid optical-based DWT-based compression, then quantization process + encrypted using Rubik's cube cryptography + optical double random phase encoding (DRPE) & SHA-256 generating hash-based message authentication code value (HMAC) digest, followed by LSB	Secure transmission, high-security performance, high efficiency, robustness against channel noise & attacks, low processing speed, & low complexity
[104]	Secure transmission of medical information between medical practitioners	Cryptography using logistic map (LM) and Henon maps with SHA-256	Good performance, fast encryption, excellent resistance against differential attacks, more efficient, and secure
[105]	To develop a new, fast, & secure medical image that can withstand attacks	The 1D logistic map associated with pseudo-random numbers	Fast computational time, efficient, can withstand cropping, & noise attacks can be implemented for RTA

Table 1
(Continued)

Cited as	Research goal	Proposed technique	Achieved
[106]	Securing e-health images	LSB & key compression with six chaotic maps: Chebyshev, Gauss, Henon, Logistic, Tent, & Piecewise maps DNA	Robust
[107]	Medical image transmission and storage are quick and secure	Permutation then substitution enhanced 2D logistic chaotic map & then SHA-256	Good visual quality, high entropy, low time complexity, uniformly distributed histogram, & weak adjacent pixel correlation
[108]	Secure, authentic, & confidential transmission of medical images over the Internet faces size & privacy challenges	7zr lossless compression & then public key encryption algorithm ECC	High security, good efficiency, image quality retained, free from statistical attacks, & no addition of noise
[109]	Multiple medical image encryption	Logistic tent 1D Lyapunov exponent chaotic system, & then Fisher–Yates scrambling & diffusion algorithm	Good encryption effects, resistance to attacks, secure, faster encryption speed, performance, & time-efficient
[110]	Telemedicine transmits and stores medical images via the cloud, maintaining confidentiality, validity, & security	Chaos cryptography, fruit fly optimization algorithm (FFOA), & then two-level SWT, followed by SVD	Quick, safe, efficient encryption, high performance, & more security
[111]	Secure image communication safeguards sensitive information	Chaotic map (Arnold cat map), then ECC, then genetic algorithm	High level of confidentiality, robust, effective, efficient, safe from potential attacks, secure image transmission, privacy protection, & digital content authentication
[112]	Privacy and security of medical image transmission	Lightweight cryptography (LWC) followed by Walsh–Hadamard transform (WHT)	More successful lightweight, privacy, & security
[113]	Transmission of medical image security from cyber attacks	New progressive meaningful visual cryptography (PMVC)	Quality, high security, low complexity, random pixel replacement, quality of RSI is maintained, reduced space complexity, & minimum number of computations
[114]	Authentic data transfer in health care on the cloud	Linear feedback shift register (LFSR) image encryption	Low correlation, robust, secure transfer, secure, & efficient compared to existing
[115]	Internet-based security of medical images while reducing computational complexity	FastMIE-redundant DWT (RDWT) and then randomized-SVD (RSVD), followed by a scrambled segmented image	Reduced encryption time, 50% greater security, more appropriate for RTA
[116]	Medical diagnosis involves sensitive information, which has privacy concerns	End-to-end steganography with MedSteGAN & then security quality (S-Q) assessment, followed by a U generator network & then feature extraction capability	Protect medical image efficiency, be more effective, retain image quality, be robust, & improve security
[117]	IoT for medical image privacy devices to interconnectivity and cloud devices from cyber-attacks and unauthorized access	Key learning network based on ResNet-50 architecture, then return on investment (ROI) framework with AES	Highly reliable, powerful outcome, attack resistant, performance, high level of security, & efficient
[118]	Hand vein image	Chaos-based security then improved SURF	Secure, high accuracy rate, & reliability
[119]	Medical image protection using good chaotic properties	Sin-Arcsin-Arnold-Multi-Dynamic random non-adjacent coupled map lattice (SAMCML) & then SHA-512, followed by DNA and then 3D Fisher	Better time performance, time efficiency, robust, & secure
[120]	Enhance security and guarantee data integrity	Blind watermarking approach for medical image protection: DWT-SVD & then LSB	Imperceptible, robust against conventional attacks (JPEG compression & addition of noise attacks), high quality, & three times less computational time

Table 1
(Continued)

Cited as	Research goal	Proposed technique	Achieved
[121]	Cloud service medical image security in communication	2D information image with compressed sensing (CS) & then chaotic multi-image encryption (MIE) based on identity mutual recognition keys (IMRKs) & 3D positioning MD-5 (3DPMD5)	Cloud tamper resistance, secure, safe performance, high encryption & decryption efficiency, resistance to statistical attacks, differential attacks, & chosen plain text attacks
[122]	Safeguarding the medical image	ECC, then Blum–Goldwasser cryptosystem (BGC), then discrete logarithmic algorithm, and probabilistic encryption, followed by quadratic residuosity problem	Resilience against cyber threats such as brute-force attacks & differential cryptoanalysis, effective, computationally efficient, swift & reliable data transmission
[123]	Block cipher security in a reliable manner for medical images	S-box-based chaotic map cryptography, leaving the black background unencrypted, then the logistic map & tent map	Reduced size of data, privacy, confidentiality, resistance against common (differential & linear) attacks, high-level encryption efficiency, security, fast solution for secure medical image transmission in RTA, & secure

Figure 6
Conventional data-hiding techniques used by previous researchers

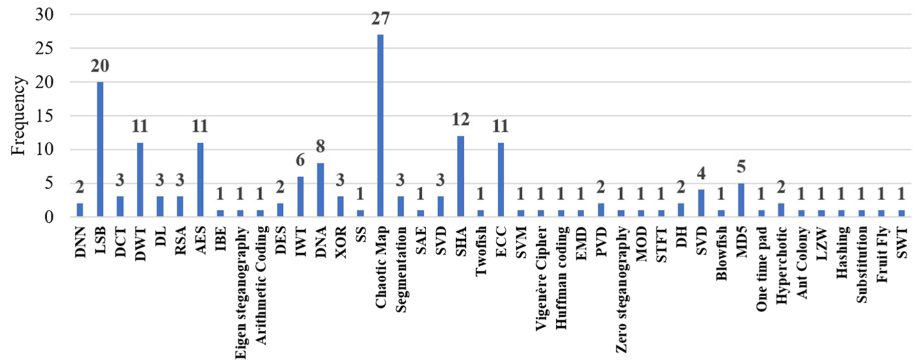


Table 2
Study based on the programming language used

Ref. No.	Programming language
[23, 31, 47, 48, 54, 62, 66, 67, 72, 75, 77, 78, 82–84, 86, 87, 89–91, 93–97, 102–107, 109, 111, 113, 115, 117, 120, 121]	MATLAB
[36, 44–46, 49, 57, 102, 108, 112, 114, 122]	Python
[48]	Network Simulator (NS2)
[59]	MATLAB + Microsoft Visual C++
[60, 116]	MATLAB + Python
[65]	Python + XAMPP+ Apache HTTP Server+ MySQL+ PHP
[68]	JavaScript + MONGO
[71]	MATLAB + Java
[79]	Visual Basic.Net language
[45, 46, 99, 124]	Java
[25]	C++ (SGX & SDK)
[98]	Ethereum platform + Python

Table 3
The online databases from which the researchers downloaded the dataset used

Ref. No.	Database
[50]	SOFTNETA-DICOM
[125]	BOSSBase
[53]	Mitdb, Pitbdb, & European ST-T database PhysioNet
[55]	ECG recordings of 47 subjects, Massachusetts Institute of Technology-Beth Israel Hospital (MIT-BIH) Arrhythmia database, MIT-BIH Normal Sinus Rhythm (MIT-BIH NSR), Beth Israel Deaconess Medical Centre Congestive Heart Failure (BIDMC-CHF), & self-recorded database
[65]	USC-SIPI, NIH, COVID-19 British Society of Thoracic Imaging database, Eurorad COVID-19 cases, & European Institute for Biomedical Imaging Research (EIBIR)
[66, 115]	Kaggle & USC-SIPI
[69, 72, 76, 122]	USC-SIPI
[71]	Sagittal T2-weighted fat-suppressed Dynamic Contrast-Enhanced Magnetic Resonance Imaging (DCE-MRI) + The Cancer Genome Atlas Breast Invasive Carcinoma Collection (TCGA-BRCA)
[74]	NIH-Clinical Center chest X-ray
[78]	Fingerprint database FVC2002
[80]	National Library of Medicine's Open Access Biomedical Images Search Engine
[25]	Diabetic Retinopathy (DR) detection & BreakHis
[83]	Instituto Mexicano del Seguro Social (IMSS)
[85, 99, 110]	Kaggle
[86]	FERET
[87]	Open-source dataset of liver CT-scans LiTS
[31]	Online Facial Expression Image Database
[94, 126, 127]	MedPix
[95]	National Library of Medicine's Open Access Biomedical Images Search Engine
[98]	Data world
[100]	European Society of Radiology database
[101]	Medical Segmentation Decathlon (MSD)
[102]	NIH
[103]	OpenMD & MedPix
[111, 117]	Publicly available databases
[112]	The Rembrandt dataset is located in the Cancer Imaging Archive (TCIA)
[114]	Metro Scans and Research Laboratory, Trivandrum
[116]	BOSSbase & iCTCF
[120]	ODIR (Ocular Disease Intelligent Recognition)
[54]	OPENi
[56]	Mini Mammographic Image Analysis Society (MIAS)

is computationally complex and less robust against manipulation attacks. DCT has low hiding capacity and not robust against attacks. DWT has less imperceptibility and lower embedding capacity or payload capacity [2].

3) LSB is used for grayscale images that are limited to a size of 24 bits. The pixel-based technique is susceptible to image processing attacks, the Blowfish technique is highly complex and requires a shared key, and spread spectrum steganography requires a chaotic encryption key [4].
4) RSA is not suitable for real-time applications as its speed is slow. LSB has low embedding capacity and is vulnerable to statistical attacks, spread spectrum requires large data capacity and is difficult to implement, and DES is not a secure encryption algorithm due to its key size [5].
5) Need to address computational time while storing EMIs while being detailed and accurate [7].
6) Need to develop an efficient encryption and scrambling technique that prevents third parties from understanding the information [8].
7) Necessary to increase the payload capacity [9] of the cover for hiding larger-sized EMIs.
8) Security challenges in the exchange of health care data [10] over a communication medium.

Table 4
Dataset details used by researchers

Ref. No.	Secret data type & size	Cover type & size
[39]	Chest X-ray image	Natural scene image
[44]	1000 records	-----
[45]	Text: "Rose Adee encrypted files"	Three images sized: 1.2, 2.9, & 7.2 MB
[49]	Convert RGB to grayscale images size 18, 37, 87, 174, & 370 byte	202,598 facial images of celebrities (70 × 109)
[50]	Medical report: 1000, 5000, 10000 up to 20000 characters	10 MRI & CT-scan images size 512 × 512 & 16-bit depth grayscale
[125]	Medical JPEG images	10,000 grayscale cover images (512 × 512)
[52]	Text with up to 8 and 192 digits	512 × 512 Bitmap grayscale images reduced to (256 × 256) 1 kHz, 360 Hz, and 250 Hz frequency with 11-bit data resolution
[53]	----	48 ECG records, 222 records, 1 kHz, 360 Hz, and 250 Hz frequency with 11-bit data resolution
[55]	Information, 4996 bits	2D ECG of 1 min having ECG record 100, 3000 samples of record 100
[59]	Block length 1024, 2048, and 4096 samples, watermark length of 32, 64, 128, 256, & 526	Real ECG, photoplethysmographic, and Holter cardio data, recorded for up to 72 h, 24 PPG signals (of 2 h recording), 12 cardio records
[60]	----	5 different medical grayscale images
[61]	Medical data	Grayscale image
[62]	Message block	Image: Lena (128 × 128, 256 × 256, 512 × 512), cameraman (256 × 256, 512 × 512), Barbara (512 × 512), boat (512 × 512), & mandrill (512 × 512)
[63]	-----	Peppers, Isabe, house, foreman, boat, Barbara colored images (100 × 100)
[65]	Plain password	20 images: Lena, chest X-ray, girl face, clown, tank, truck, cameraman, chest-1, chest, b-f00163, b-f00175, b-f00181, b-m00167, b-m00169, b-m00171, e-17524-1-1, e-17543-1-1, e-17605-1-1, e-17611-1-1, e-17637-1-1, e-17531-1-1 (512 × 512)
[66]	1 & 2 bit	50 images: baboon, deer, flower, fruit (32 bits, 64 bits)
[36]	320-bit hash algorithm	DICOM image
[68]	EHRs as PDF (202, 270, 461, 540 kB, 0.99, 1.93, 2.14, 2.91, 3.41, 4.09, 6.38 MB)	EHRs as Excel file (128 B, 5, 10, 15, 20, 30, 40 kB, 1, 2 4, 8 MB), output is a text file
[38]	-----	EEG signals, ECG, blood sugar levels, blood pressure levels, & other conditions
[69]	Payload capacity = 16384 bytes, 16384, 32768, 49152, 65536 bytes, text: "ElGamal," (512 × 512)/8 = 32768 bits	Lena, pepper cover image, colored and grayscale images (512 × 512), 8 × 8 block thus 64 blocks, 64 × 64 (4096 pixels)
[70]	------	Block of 1 MB
[71]	500 DCE-MRI slices of 50 women patients, 165 × 165 logo image = 65536 pixels	100 grayscale images of size (165 × 165), 10 images of size (256 × 256), 10 images (256 × 256)
[72]	Message "University of Mosul"	6 images size (512 × 512), Lena, man, baboon, airplane F16, pepper, & Tiffany
[73]	------	10 grayscale images (512 × 512): Lena, pepper, baboon, airplane, Tiffany, boat, truck, tank, Barbara, Gold Hill
[74]	16 × 16-bit pseudo-random matrix	112121 X-ray PNG images (1024 × 1024), 30,805 patients having 14 disease labels
[75]	Character message of 2547, 2881, 4287, 8192 bytes	Images (256 × 256): boat, bird, Flintstone, Lena, pepper, & baboon
[76]	Text of 8 kB, different sizes of text 2, 4, 6, & 8 kB	50 edgy and smooth colored images (128 × 128, 256 × 256, 512 × 512, & 1024 × 1024): Lena, baboon, pepper, house, scene, splash, F-16, & building

Table 4
(Continued)

Ref. No.	Secret data type & size	Cover type & size
[77]	4 medical images	4 audio
[20]	Data of 196608 bits (i.e., 24576 bytes), 264 bits	Butterfly (176 kB, 386 × 395), Mario (22.1 kB, 219 × 150), penguin (47.1 kB, 386 × 395), images (256 × 256), 24-BMP & PNG images
[6]	Text "this is the test string"	BMP images in PNG and WAV files
[78]	------	EMIs, EHRs, 6 medical images (512 × 512): lungs, pelvic, head, skin, breast, kidney; 6 images (1024 × 1024): Lena, baboon, girl, pepper, Barbara, & airplane
[79]	Lena image, 65536 bits	40 different-sized cover landscape images, 393216 bytes
[80]	500 medical images each 100 of type (512 × 512), ECG, MRI, CT-scan, X-ray, & ultrasound	------
[81]	File sizes: 1, 3, 5, 7, 9, & 10 MB	------
[82]	Brain, eye, lung, kidney, & pancreas images	File sizes: 2000, 4000, 6000, 8000, 10000 kB
[25]	-----	35126 DR images (786 × 512)
[83]	10 images DICOM file hiding, medical images in grayscale: head & brain, 4095 depth 12 bits/pixel	Patient identification photo (255 × 255), 255 × 255 × 12 bit depth = 7,80,300 bits for colored images 255 × 255 × 8 bit × 3 = 15,60,600 bits
[84]	151 × 333 × 3	10 images (256 × 256) sizes: 150849, 77976, 518400, 4326210, 122265, 518400, 150975, 150975, 151353, 1890000
[85]	Watermark images resized 64 × 64	Different body parts & organs: brain, lungs, eyes (128 × 128)
[86]	Facial image	CT-scan images, input data 224 × 224 × 3
[87]	Originally 256 × 256	131 scans of CT-scan images (224 × 224)
[88]	-----	RGB medical images: MRI images
[31]	JPEG images of 227 × 227 pixels: headshots of 100 children's facial expression images, 100 children's, 10 hand X-rays, self-created, 10 standard images	10 medical images: hand X-ray, self-created in JPEG (227 × 227), resolution of 96 × 96 dots per inch and 24 bits per pixel (colored image)
[89]	Grayscale & colored photos	Grayscale medical images: head, ultrasound, X-ray, feet, hand, 500 × 500, 512 × 512, 600 × 600, 612 × 612, 900 × 900, & 1024 × 1024
[90]	------	Brain, lung, EEG, & other images, glaucoma, cancer
[91]	Doctor-patient information	5 ultrasound images & textual metadata, including over 12,000 patient case scenarios, 9000 topics, & 59,000 images
[92]	Character text file sizes: 0.1, 0.5, 1, 10, 50, 100, & 500 MB	-----
[93]	Human eye, X-ray images, encrypted watermark size of 23 kB, compressed to 18.01 kB	Lena, chest, baby, logo, baboon, 9 JPEG images, head chronometer, face, dental X-ray, Einstein (128 × 128)
[94]	Bladder stone	Medical images: knee X-ray, abdomen CT-scan, lung X-ray, spinal disk, thorax CT-scan, leg X-ray, hand X-ray, ankle X-ray, brain CT-scan, throat, Lena, cameraman, mandrill, pepper, pancreas, cervix, skull, lake, house, clock (64 × 64, 128 × 128, 256 × 256, 512 × 512); 7 images: knee X-ray, abdomen CT-scan, lung X-ray, leg X-ray, hand X-ray, ankle X-ray, brain CT-scan, & spinal
[95]	256 × 256, 512 × 512, 1024 × 1024	500 medical images (512 × 512): 100 medical images: MRI, CT-scan, ultrasound, X-ray, & ECG
[96]	-----	Lena, baboon, pepper, airplane (512 × 512)
[97]	Lena, cameraman (256 × 256, 512 × 512)	DICOM medical images: MRI, US, X-ray (256 × 256, 512 × 512, 1024 × 1024)
[99]	100 chest X-ray images: 700	X-ray, CT-scan, MRI (512 × 512)
[100]	Patient information: grayscale logo of Kocaeli University (45 × 45, 64 × 64)	Head scan, CT scan, MRI, US, and X-ray images (480 × 480)
[101]	Text file sizes: 559, 636, & 910 kB	Cover image

Table 4
(Continued)

Ref. No.	Secret data type & size	Cover type & size
[102]	32 high-resolution CT-scan images 677 × 598, size of 364.2 kB, size of 32 images: 11.3 MB (677 × 598)	CT-scan images (4100 × 2050), marked spot (480 × 480; 677 × 598) 364.2 kB, 32 images size: 11.3 MB
[103]	Gray & RGB images (256 × 256)	256 × 256
[104]	880 × 660: pelvic & thorax, 256 × 256: leg, eye, thorax, pelvis	Lena, baboon, Barbara, cameraman images
[105]	Brain, MRI, lungs: 50 grayscale & 50 RGB images 512 × 512	Lena, 50 gray & 50 RGB images
[106]	Patient information (a text file containing 100 characters, including patient name, age, gender, address, and patient's medical diagnosis, was stored in a text file with a size of 107 bytes.)	6 medical images chest X-rays, body X-rays, abdominal CT, heart CT, brain MRI, and neck MRI with different dimensions (chest X-ray, 174 × 290; body X-ray, 483 × 626; abdominal CT-scan, 335 × 400; heart CT-scan, 412 × 800; brain-MRI, 1175 × 1332; neck-MRI, 315 × 560)
[107]	Foot X-ray, 512 × 512; brain CT, 256 × 256; head MRI, 256 × 256; fetal ultrasound, 512 × 512; brain PET, 256 × 256; COVID-19 virus, 512 × 512; Lena normal image, 512 × 512; pepper normal image, 256 × 256	Output size 2.45 Mbps
[109]	Four CT images 512 × 512, two MRI images of size 320 × 320	Different sizes
[110]	Logo in RGB (128 × 128, 200 × 256)	3205 DICOM: CT-scan, X-rays, MRI (512 × 512, 430 MB)
[111]	- ----	Baboon, Lena, Barbara, cameraman, pepper (512 × 512)
[112]	400 images	100 images: normal & tumor MRI in JPEG (256 × 256, 512 × 512)
[113]	4 grayscale images: Medical_image1, Medical_image2, QR code, Lena (256 × 256)	4 grayscale images: pepper, girl, Image 3, baboon (256 × 256)
[114]	CT-scan images	5 DICOM images
[115]	Medical dataset (105 images), non-medical dataset (50 images)	Grayscale images: MRI, 512 × 512; kidney stone, 512 × 512; X-ray, 512 × 512; colon MRI, 724 × 839; head CT-scan, 512 × 512; cameraman, 512 × 512; cell, 512 × 512; rice, 510 × 510; Zelda, 256 × 256; Lena, 350 × 350 (512 × 512)
[116]	JPEG	CT-scan (256 × 256)
[117]	----	Chest X-rays and MRI (256 × 256, 512 × 512)
[118]	Text: "Personal Name: Fernando Tureng Sex: M Birth Date: 05.11.1990 ID Number: 12986278161 Blood Type: 0 rh –" size = 1, 10, 20, 40, 80	Vein pattern image, 500 healthy adults (256 × 256)
[119]	-----	Medical images: brain, knee, chest X-ray (480 × 512)
[120]	5,000 patients, 200 images, 238 characters, concealing 2546 bits	Retinal image (512 × 512)
[121]	ASCII code for: "Patient ID code = 230520854070565, Date of admission to hospital = 20230810, Department = Neurosurgery, Name = Jack Smith, Gender = Male, Age = 37, Brain, Right foot, Cervical, Lung, Head, Pathological Tissue Sections, Skull, Left hand"	3D medical images: brain, 512 × 512 × 3; right foot, 256 × 256 × 3; cervix, 256 × 256 × 3; lung, 256 × 256 × 3; head, 256 × 256 × 3; pathological tissue sections, 512 × 512 × 3; 3D model: skull (vertices: 42440 × 3; faces: 84666 × 3), left hand (vertices: 94998 × 3; faces: 190667 × 3) (256 × 256)
[122]	-----	Dental X-ray (720 × 330), mandrill (512 × 512)
[123]	Flower	4 DICOM images: US, axial, CT-scan, X-ray of feet, & brain CT-scan (512 × 4, 2048-bit blocks)
[51]	"battista" converted to ASCII	BMP image
[54]	Cameraman, peppers, Barbara, aerial	18 images: X-ray, CT-scan images (256 × 256)
[56]	322 mammogram images (1024 × 1024)	Breast cancer patient's data, PNG image RGB
[58]	4 cover and 4 secret images	CT scan and X-ray images

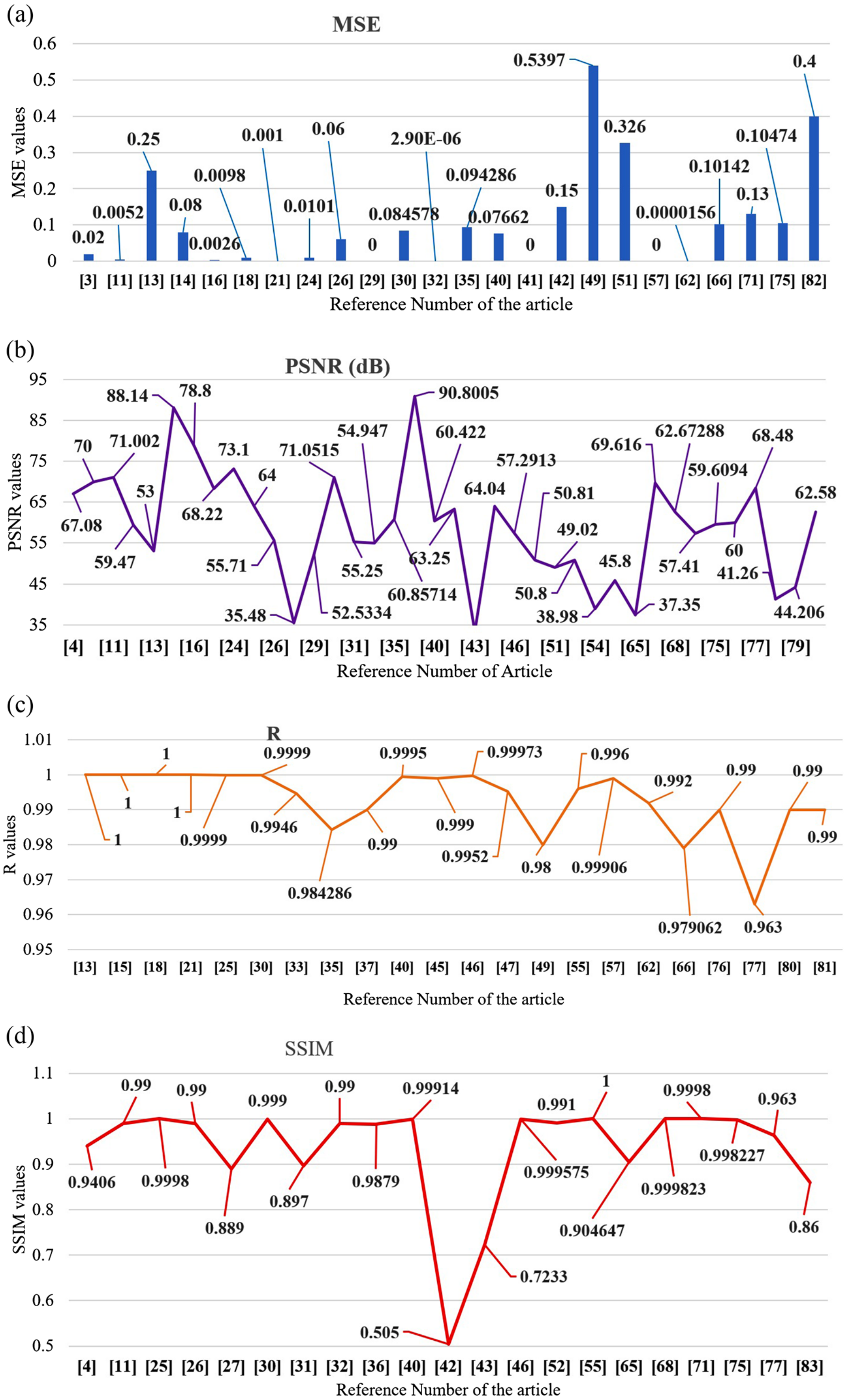
Table 5
Various performance test formulas

Performance test	Formula	Equation number
Mean square error (MSE)	$\mathrm{MSE} = \sum_{i=1}^{M}\sum_{j=1}^{N}\frac{(\mathrm{I(i,j)-SI(i,j)})^2}{\mathrm{M\times N}}$	(1)
Peak signal-to-noise ratio (PSNR)	$\mathrm{PSNR} = 10\ log_{10}\frac{\mathrm{max}^2}{\mathrm{MSE}}$	(2)
Root mean square error (RMSE)	$RMSE = \sqrt{MSE}$	(3)
Structural similarity index metrics (SSIM)	$\mathrm{SSIM(x,y)} = \frac{(2\mu_{Ac}\mu_{Re}+c_1)(2\sigma_{AcRe}+c_2)}{(\mu_{Ac}^2+\mu_{Re}^2+c_1)(\sigma_{Ac}^2+\sigma_{Re}^2+c_2)}$	(4)
Embedding ratio (ER)	$ER = \frac{p}{M\times N}$	(5)
Pearson coefficient (R)	$\mathrm{R(Ac,\ Re)} = \frac{\mathrm{Cov\ (Ac,\ Re)}}{\sigma_{Ac}\sigma_{Re}}$	(6)
Coefficient of variation (CV)	$\sigma_{Ac} = \sqrt{\frac{(\sum(\mathrm{Ac}-\mu))^2}{\mathrm{L}}}$	(7)
	$\mu_{Ac} = \frac{\sum \mathrm{Ac}}{\mathrm{L}}$	(8)
	$\mathrm{Cov(Ac,\ Re)} = \frac{\sum(Ac-\mu_{Ac})\times(Re-\mu_{Re})}{L}$	(9)
Number of pixel changing rate (NPCR)	$\mathrm{NPCR} = \frac{\sum_{i,j}^{N,M}\mathrm{D(i,j)}}{\mathrm{M\times N}}\times 100$	(10)
	$\mathrm{D(i,j)} = \begin{cases}0 & \text{if } c_1(i,j) = c_2(i,j)\\ 1 & \text{otherwise}\end{cases}$	(11)
Unified average changing intensity (UACI)	$\mathrm{UACI} = \frac{1}{\mathrm{M\times N}}\left(\sum_{i,j}^{N,M}\frac{\lvert c_1(i,j)-c_2(i,j)\rvert}{255}\times 100\right)$	(12)
Edge differential ratio (EDR)	$EDR = \frac{\sum_{i,j=1}^{N}\lvert c_1(i,j)-c_2(i,j)\rvert}{\sum_{i,j=1}^{N}\lvert c_1(i,j)-c_2(i,j)\rvert}$	(13)
Entropy (E)	$E = -\sum_{i=1}^{N}P(Re)\ log_2\ P\ (Re)$	(14)
Kullback–Leibler divergence (KLD)	$KLD = \int c_2(x)\times log\frac{c_1(x)}{c_2(x)}d(x)$	(15)
Bit error rate (BER)	$BER = \frac{\sum_{i,j}^{N,M}I(i,j)\otimes S(i,j)}{L}$	(16)
Mean absolute percentage error (MAPE)	$\mathrm{MAPE} = \frac{1}{\mathrm{L}}\sum_{i=1}^{L}\left(\frac{\lvert c_1(i)-c_2(i)\rvert}{c_1(i)}\right)\times 100\%$	(17)
Signal-to-noise ratio (SNR)	$SNR = 10\ log_{10}\frac{\sum_{i=1}^{L}(c_1(i)-c_2(i))^2}{\sum_{i=1}^{L}(c_1(i))^2}$	(18)
Percentage residual difference (PRD)	$PRD = \sqrt{\frac{\sum_{i=1}^{L}(c_1(i)-c_2(i))^2}{\sum_{i=1}^{L}(c_1(i))^2}}\times 100\%$	(19)

9) RSA, AES, DES, and DNA security techniques reduce network performance, thus resulting in slow speed [23].
10) Traditional techniques are ineffective and computationally infeasible [32].
11) DES, 3DES, Blowfish, and AES techniques were found to be inefficient [47] when dealing with EMIs.
12) The AES technique is secure, suffers from the avalanche effect, and needs improvement in computational cost [68] as it needs more resources to implement.
13) Traditional security techniques are not enough to provide high security for medical images [80]. Thus, there is a need for implementing a lightweight security technique.
14) Conventional encryption techniques such as RSA, DES, AES, and IDEA are not convenient for encrypting bulky or large images [79] such as EMIs.
15) AES is a complex algorithm, takes more execution time, and requires more resources for implementing [101].
16) RC5 provides less security level. DES has poor security levels, making it vulnerable to several attacks. RC6 is not suitable for practical implementations. The two-fish algorithm is relatively slow. Blowfish has complex key management, and time consumption for decryption is high [117].
17) Conventional techniques such as LSB, PVD, DCT, and EMD have limited hiding capacity for secret data, and if the size of the secret data is increased, this would result in distortion [124] of the secret image upon extraction.
18) Conventional techniques such as DES and IDEA are not suitable for large medical images [128].
19) Traditional techniques suffer from reliability issues, while these cryptography techniques are complex to implement [129].
20) Computational complexity to implement a technique is a cause of concern [68, 130, 131].

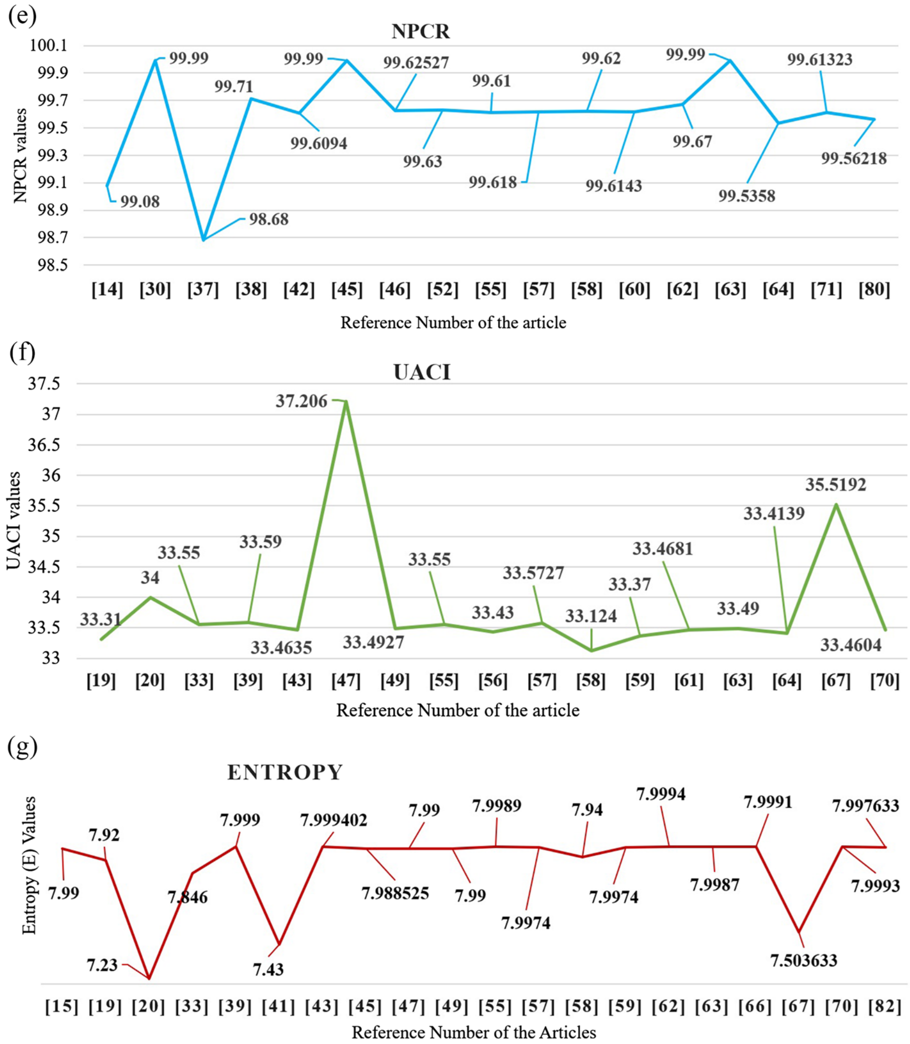
Hence, spatial domain-based binary steganography needs more space for hiding, even for a smaller payload, and is prone to statistical

Figure 7
Performance test: (a) MSE, (b) PSNR, (c) R, (d) SSIM, (e) NPCR, (f) UACI, and (g) entropy



attacks [2]. Kataria et al. [5] suggested the need for integrity and authenticity of medical images as e-diagnosis requires them to be shared over the Internet [13] or storage on third-party insecure medium while being prone to data breaches [9]. Patient's personal data such as personal details and medical history also need to be protected [7], ensuring confidentiality [10]. Spatial domain methods such as LSB steganography are prone to stego-attacks [14], pixel value difference (PVD) and exploiting modification direction (EMD) are vulnerable to distortion and compression, and transformation techniques such as discrete cosine transform (DCT), DWT, and fast Fourier transform (FFT) are computationally expensive [10]. Due to the limited key space, the 2D chaotic map is not resistant to brute force attacks, while the chaotic encryption algorithm is prone to exhaustive search attacks [31]. Modified Advanced Encryption Standard (AES) has a

Figure 7
(Continued)



higher avalanche effect than simple AES. AES uses the same key for encryption and decryption; thus, the key is highly vulnerable [30]. The genetic algorithm (GA) requires more computational time [25]. It can be concluded that conventional techniques such as DES, AES, and MD are facing challenges and have not addressed the computational time-based complexity. Therefore, a new data-hiding technique needs to be developed, which can hide larger and varying-sized EMIs such that they are accessible in real time through real-time applications.

4. Result Analysis and Prevalently Used Performance Test

A few commonly used performance tests and their formulas are shown in Table 5. These test results are found by comparing the decrypted images with their originals. Tests such as mean square error (MSE), peak signal-to-noise Ratio (PSNR), root mean square error (RMSE), structural similarity index metrics (SSIM), and correlation (R) help in measuring the quality of the distortion in the image upon retrieval. These test formulas are shown in Equation (1), Equation (2), Equation (3), Equation (4), and Equation (6). The formulas for tests such as embedding ratio (ER), standard deviation (σ), mean value (μ), Cov, NPCR, coefficient of correlation (D), UACI, EDR, E, KLD, BER, MAPE, SNR, and PRD are shown in Equation (5) and Equations (7)–(19).

Using the formula quoted in Equation (1) to Equation (19) as in Table 5, the previous research evaluated their proposed techniques. The preferred MSE test values are low. Some of these values are shown in Figure 7(a). PSNR values should be above 33. The plot of the previously achieved PSNR values is depicted in Figure 7(b). The ideal R value is 1, indicating a high correlation between the original and decrypted images, graphically shown in Figure 7(c). Figure 7(d) depicts SSIM values. The preferred value of SSIM is 1, indicating a similarity between the decrypted images and their originals. NPCR and UACI are shown in Figures 7(e) and (f). Figure 7(g) shows entropy (E), which should be close to 8.

As shown in Figure 7(a)–(g), most of the researchers have achieved the preferred values for the tests. Table 6 shows the test values for R, MSE, SSIM, UACI, E, PSNR, and NPCR, which are not close to the ideal values. Table 6 also shows the values for FSIM, KLD, root mean square error (RMSE), MAPE, PRD, MAE, bit error ratio (BER), signal-to-noise ratio (SNR), compression ratio (CR), MCE, image fidelity (IF), and payload capacity (PC).

Table 6 presents a few values of the various performance tests. The PSNR values shown here were either infinite or below the required

Table 6
Some performance test values achieved by researchers

Ref. No.	R
[3]	0
[36]	0.00286
[59]	0.036
[85]	0.002
[90]	0
[102]	0.03097
[105]	0.02392
[106]	0.00278
[108]	0.0011
[114]	0.00298
[121]	0.001

Ref. No.	UACI
[31]	80.24
[76]	0.00747
[93]	28.0645
[119]	0.00016

Ref. No.	SNR
[52]	81.3
[54]	48.27
[58]	36.4
[76]	14.8761
[109]	35.4

Ref. No.	MSE
[3]	7.93
[36]	14800
[48]	8.561
[51]	0.25
[62]	0.22
[79]	739.098
[89]	0.15
[94]	5178.38
[95]	0.5397
[98]	509.71
[99]	0.326
[105]	13743
[112]	1.73757
[132]	1.28
[133]	6.05
[134]	4.09
[113]	0.10142
[117]	0.17864
[119]	0.13
[127]	0.10474
[135]	0.4

Ref. No.	Entropy
[95]	0.00029

Ref. No.	NPCR
[136]	0.011048

Ref. No.	PSNR (dB)
[“[25]”]	27.87
[31]	105.25
[36]	14.87,6
[48]	161.02
[59]	7.98
[61]	16.95
[65]	132.47
[79]	5.72
[84]	15.46
[83]	∞3 14.4
[88]	∞8 100
[94]	5.4954
[96]	7.21833
[102]	9.33, ∞
[104]	7.4232, ∞
[105]	26.7
[110]	24.06541
[121]	8.6138, ∞
[128]	32
[133]	42,611

Ref. No.	CR
[58]	4.16
[92]	21.66%
[128]	28.50%

Ref. No.	SSIM
[25]	5.47
[59]	0.0046
[85]	0.00585
[105]	0.0067

Ref. No.	FSIM
[59]	0.34
[85]	0.35
[102]	0.4105,1

Ref. No.	KLD
[137]	957.82
[54]	9.42E-06
[58]	0.002

Ref. No.	PRD
[52]	0.02
[54]	0.066
[58]	0.113

Ref. No.	BER
[58]	0.119
[81]	0.002857
[101]	6.16 (%)
[138]	7.76

Ref. No.	RMSE
[3]	2.702
[49]	0.072
[52]	0.05
[58]	0.21
[75]	0.01096
[92]	0.16161
[95]	2.6465

Ref. No.	MAPE
[3]	2.1793
[52]	0.53
[58]	0.068
[62]	0.00045
[133]	0.89
[112]	3.37172

Ref. No.	MCE
[133]	0.34

Ref. No.	IF
[127]	0.9994

Ref. No.	PC
[74]	8160

range of 30 similar values for R, MSE, SSIM, UACI, NPCR, and entropy mentioned. Table 6 also shows the test values for other evaluation tests.

4.1. Computational complexity

Computational complexity is a measure of encryption time (ET). ET is the time taken to encrypt the original image, while the decryption time (DT) is the time taken to retrieve the image. The total time is the sum of ET and DT. The values achieved for ET, DT, and total time are shown in Table 7. From Table 7, it is clear that the encryption time is a measure of the time taken to secure the images by implementing the proposed data-hiding technique. The minimum encryption time taken is 9.06E-07 by Peng et al. [116], while the minimum decryption time taken is 9.05E-06 by Elkamchouchi et al. [87]. Decryption time is the time taken to decrypt the image back into its original form. To make the EMI accessible in real time, the time taken to secure the image, ET and the time taken to extract the image should be less. This will make the data-hiding technique accessible in real time, thus ensuring the light weight of the technique. Prevalently, a hybrid and lightweight technique is needed to secure EMIs, which are large and have varying dimensions. Therefore, the hybrid lightweight technique should be independent of the data size and should not modify the data such that they are non-understandable for medical diagnosis.

4.2. Discussion

Many researchers have clearly quoted computational time-based complexity in their articles, which helps in concluding the feasibility of their proposed techniques, as mentioned in Table 7. Reduced time-based complexity ensures the suitability of these techniques for real-time applications. Previous researchers have performed the following data-hiding techniques: DNN, LSB, AES, RSA, DES, chaotic map, and/or a combination of more than one data-hiding technique, as shown in Table 1. Table 2 shows that MATLAB is the most commonly used programming language. Table 3 helps in understanding that most of the researchers have used an online database to download their dataset. As shown in Table 4, most of the previous researchers in their articles cited as [6, 20, 44, 45, 50, 52, 55, 59, 61, 62, 66, 68, 69, 72, 75, 76, 81, 91, 92, 100, 101, 116, 118, 121] have hidden text data in the cover image. This is achieved by converting the text into ASCII and then hiding it in the images. In general, researchers [50, 80, 95, 99, 105, 110, 111, 115, 120, 121, 125] have normalized the dimensions 512 × 512 of the medical

Table 7
The encryption, decryption, and total times taken by researchers for their proposed techniques

Encryption time (ET)

Cited as	ET (s)	Cited as	ET (s)
[6]	2	[94]	4.50E-05
[31]	0.065	[96]	3.7
[36]	0.176	[97]	3.56E-06
[44]	34.43	[98]	12.47
[52]	5.36E-06	[100]	0.028
[59]	2.25	[103]	0.73
[66]	60	[104]	0.033
[67]	0.00129	[105]	8.35
[77]	13.72	[106]	0.49
[78]	4.6	[109]	4.07
[79]	0.24	[110]	0.86
[80]	1.27	[111]	9.79
[81]	0.0029	[114]	0.175
[84]	1.36	[116]	9.06E-07
[85]	0.23	[120]	20.86
[87]	1.17E-05	[121]	0.077
[88]	4.73	[122]	0.00074
[91]	0.15	[130]	0.001998
[93]	4.28	[139]	0.005
		[140]	102.16

Decryption time (DT)

Cited as	DT (s)	Cited as	DT (s)
[6]	0	[93]	4.26
[31]	0.107	[97]	1.00E-05
[59]	2.25	[98]	8.31
[66]	63	[100]	0.029
[67]	0.0014	[105]	10.03
[77]	14.16	[106]	0.59
[79]	0.25	[109]	1.02
[80]	1.006	[110]	0.86
[81]	0.0018	[111]	96.38
[84]	1.36	[114]	0.00898
[85]	0.44	[116]	7.08E-05
[87]	9.05E-06	[120]	21.49
[88]	4.4	[121]	0.069
[91]	0.023	[130]	0.001
		[139]	0.006
		[140]	97.84

Total time (in s)

Cited as	Total time	Cited as	Total time	Cited as	Total time	Cited as	Total time
[22]	0.4	[54]	0.15	[94]	37.8	[128]	5.9
[35]	0.001	[72]	4.9	[102]	1.735	[130]	0.003001
[43]	599.17	[89]	1.5 min	[117]	0.099	[141]	83.26
[44]	1.31	[91]	0.5	[138]	-0.00542	[142]	7.50E-05
						[138]	0.04

images, rendering them unclear for understanding and future diagnosis. Similarly, Hachaj et al. [49] used a medical image with dimensions of 70 × 109; work by Olvera-Martinez et al. [83], 255 × 255; works by Huang et al. [85] and Nazari et al. [93], 128 × 128; work by Abdellatef et al. [86], 224 × 224 × 3; work by Elkamchouchi et al. [87], 224 × 224; work by Lin et al. [31], 227 × 227; work by Hussain and Khodher [89], 500 × 500; work by Khare and Srivastava [94], 64 × 64; works [54, 97, 104, 107, 112, 113, 116, 117, 118, 121], 256 × 256; work by Konyar and Öztürk [100], 480 × 480; work by Peng et al. [116], 174 × 290; work by Wang and Wang [109], 320 × 320; work by Zermi et al. [119], 480 × 512; work by Jamal et al. [122], 720 × 330; and work by Khalifeh et al. [56], 1024 × 1024. Medical images have various sizes as they belong to patients of various age groups and during the various phases of their disease. Security and privacy need to be enhanced while dealing with large and varied-sized images, ensuring timely access to them.

5. Conclusions and Future Scope

This study has shown that the security of EMIs is a cause of concern. Hence, EMIs need to be secured using data-hiding techniques. The lack of conventional techniques has been highlighted in this article. EMIs, which are in the form of digital images in JPEG format, have various sizes and dimensions and are accessed by their users on their devices through the Internet. It was found in this study that not much work has been done to develop a data-hiding technique for EMIs, which would hide large and various sizes of EMIs to secure them while they are being transmitted over the Internet on third-party storage. Because EMIs are accessed in real time by the patients and doctors, they should be accessible in real time for real-time applications. Computational time-based complexity is an important aspect that needs to be addressed. Most of the previous researchers have failed to mention them. Thus, it can be concluded that in the future, researchers could propose a lightweight hybrid technique that would reduce the computational time-based complexity of the data-hiding techniques. Hybrid means that a combination of two or more data-hiding techniques is applied on EMIs, ensuring the properties of both data-hiding techniques. Future research could focus on larger and varying-size datasets of EMIs while ensuring security and privacy by implementing a hybrid technique that emphasizes the reduction of computational time-based complexity, thereby making it lightweight.

Ethical Statement

This study does not contain any studies with human or animal subjects performed by any of the authors.

Conflicts of Interest

The authors declare that they have no conflicts of interest to this work.

Data Availability Statement

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

Author Contribution Statement

Divya Sharma: Conceptualization, Methodology, Software, Validation, Formal analysis, Investigation, Resources, Writing – original draft. **Chander Prabha:** Data curation, Writing – review & editing, Visualization, Supervision, Project administration.

References

[1] Puneeth, R. P., & Parthasarathy, G. (2023). Survey on security and interoperability of electronic health record sharing using blockchain technology. *Acta Informatica Pragensia*, *12*(1), 160–178. https://doi.org/10.18267/j.aip.187

[2] Kaur, S., Singh, S., Kaur, M., & Lee, H.-N. (2022). A systematic review of computational image steganography approaches. *Archives of Computational Methods in Engineering*, *29*(7), 4775–4797. https://doi.org/10.1007/s11831-022-09749-0

[3] Yildirim, M. (2021). Steganography-based voice hiding in medical images of COVID-19 patients. *Nonlinear Dynamics*, *105*(3), 2677–2692. https://doi.org/10.1007/s11071-021-06700-z

[4] S, S. K., Hegde, S., P, S., & P, V. R. (2023). Exploring the effectiveness of steganography techniques: A comparative analysis. In *2023 3rd International Conference on Smart Data Intelligence*, 181–186. https://doi.org/10.1109/ICSMDI57622.2023.00042

[5] Kataria, M., Jain, K., & Subramanian, N. (2023). Exploring advanced encryption and steganography techniques for image security. In *2023 11th International Symposium on Digital Forensics and Security,* 1–6. https://doi.org/10.1109/ISDFS58141.2023.10131890

[6] Lishomwa, K., & Zimba, A. (2023). A privacy-preserving scheme for medical diagnosis records based on encrypted image steganography. *Zambia ICT Journal*, *7*(1), 23–28. https://doi.org/10.33260/zictjournal.v7i1.151

[7] Sharma, D., & Prabha, C. (2024). Hybrid security of EMI using edge-based steganography and three-layered cryptography. In J. Singh, S. Goyal, R. Kumar Kaushal, N. Kumar, & S. Singh Sehra (Eds.), *Applied data science and smart systems* (pp. 278–290). CRC Press. https://doi.org/10.1201/9781003471059-37

[8] Mahalingam, H., Veeramalai, T., Menon, A. R., S., S., & Amirtharajan, R. (2023). Dual-domain image encryption in unsecure medium—A secure communication perspective. *Mathematics*, *11*(2), 457. https://doi.org/10.3390/math11020457

[9] Abed, M. K., Kareem, M. M., Ibrahim, R. K., Hashim, M. M., Kurnaz, S., & Ali, A. H. (2021). Secure medical image steganography method based on pixels variance value and eight neighbors. In *2021 International Conference on Advanced Computer Applications*, 199–205. https://doi.org/10.1109/ACA52198.2021.9626807

[10] Dhar, S., Khare, A., & Singh, R. (2023). Advanced security model for multimedia data sharing in Internet of Things. *Transactions on Emerging Telecommunications Technologies*, *34*(11), e4621. https://doi.org/10.1002/ett.4621

[11] Kumar, M., Soni, A., Shekhawat, A. R. S., & Rawat, A. (2022). Enhanced digital image and text data security using hybrid model of LSB steganography and AES cryptography technique. In *2022 Second International Conference on Artificial Intelligence and Smart Energy*, 1453–1457. https://doi.org/10.1109/ICAIS53314.2022.9742942

[12] Mahmoud, M. M., & Elshoush, H. T. (2022). Enhancing LSB using binary message size encoding for high capacity, transparent and secure audio steganography–An innovative approach. *IEEE Access*, 10, 29954–29971. https://doi.org/10.1109/ACCESS.2022.3155146

[13] AlSabhany, A. A., Ali, A. H., Ridzuan, F., Azni, A. H., & Mokhtar, M. R. (2020). Digital audio steganography: Systematic review, classification, and analysis of the current state of the art. *Computer Science Review*, *38*, 100316. https://doi.org/10.1016/j.cosrev.2020.100316

[14] Salem, O., & Mehaoua, A. (2023). Ephemeral elliptic curve Diffie–Hellman to secure data exchange in Internet of Medical Things. In K. Daimi, A. Alsadoon, C. Peoples, & N. El Madhoun (Eds.), *Emerging trends in cybersecurity applications* (pp. 3–20). Springer International Publishing. https://doi.org/10.1007/978-3-031-09640-2_1

[15] Alhaddad, M. J., Alkinani, M. H., Atoum, M. S., & Alarood, A. A. (2020). Evolutionary detection accuracy of secret data in audio steganography for securing 5G-enabled Internet of Things. *Symmetry*, *12*(12), 2071. https://doi.org/10.3390/sym12122071

[16] Nagaraju, C., Parthasarathy, S., & Subramanya, M. B. (2014). Embedding patient information in medical images augmented with compression by rotation technique. In *Emerging Research in Electronics, Computer Science and Technology: Proceedings of International Conference*, 703–712. https://doi.org/10.1007/978-81-322-1157-0_72

[17] Ayuba, S., & Zainon, W. M. N. W. (2023). Medical image watermarking: A survey on applications, approach and performance requirement compliance. *International Journal of Multimedia Information Retrieval*, *12*(2), 33. https://doi.org/10.1007/s13735-023-00290-9

[18] Ayub, N., & Selwal, A. (2020). An improved image steganography technique using edge based data hiding in DCT domain. *Journal of Interdisciplinary Mathematics*, *23*(2), 357–366. https://doi.org/10.1080/09720502.2020.1731949

[19] Ahmad, I., & Shin, S. (2022). A perceptual encryption-based image communication system for deep learning-based tuberculosis diagnosis using healthcare cloud services. *Electronics*, *11*(16), 2514. https://doi.org/10.3390/electronics11162514

[20] Singhal, V., Shukla, Y. K., & Prakash, N. (2020). Image steganography embedded with Advance Encryption Standard (AES) securing with SHA-256. *International Journal of Innovative Technology and Exploring Engineering*, *9*(8), 641–648. https://doi.org/10.35940/ijitee.H6442.069820

[21] Kadhim, I. J., Premaratne, P., Vial, P. J., & Halloran, B. (2019). Comprehensive survey of image steganography: Techniques, evaluations, and trends in future research. *Neurocomputing*, *335*, 299–326. https://doi.org/10.1016/j.neucom.2018.06.075

[22] Kuri, J. L. (2020). Securing data in Internet of Things (IoT) using cryptography and steganography techniques. *International Journal for Research in Applied Science and Engineering Technology*, *8*(7), 1933–1939. https://doi.org/10.22214/ijraset.2020.30485

[23] Bansal, B., Jenipher, V. N., Jain, R., Dilip, R., Kumbhkar, M., Pramanik, S., …, & Gupta, A. (2022). Big data architecture for network security. In S. Pramanik, D. Samanta, M. Vinay, & A. Guha (Eds.), *Cyber security and network security* (pp. 233–267). Wiley. https://doi.org/10.1002/9781119812555.ch11

[24] Alabdulatif, A., Thilakarathne, N. N., & Kalinaki, K. (2023). A novel cloud enabled access control model for preserving the security and privacy of medical big data. *Electronics*, *12*(12), 2646. https://doi.org/10.3390/electronics12122646

[25] Zhang, D., Ren, L., Shafiq, M., & Gu, Z. (2023). A privacy protection framework for medical image security without key dependency based on visual cryptography and trusted computing. *Computational Intelligence and Neuroscience*, *2023*(1), 6758406. https://doi.org/10.1155/2023/6758406

[26] Venkatraman, S., Parvin, S., Mansoor, W., & Gawanmeh, A. (2023). Big data analytics and Internet of Things for personalised healthcare: Opportunities and challenges. *International Journal of Electrical and Computer Engineering*, *13*(4), 4306–4316. https://doi.org/10.11591/ijece.v13i4.pp4306-4316

[27] Subrahmanya, S. V. G., Shetty, D. K., Patil, V., Hameed, B. M. Z., Paul, R., Smriti, K., …, & Somani, B. K. (2022). The role of data science in healthcare advancements: Applications, benefits, and future prospects. *Irish Journal of Medical Science*, *191*(4), 1473–1483. https://doi.org/10.1007/s11845-021-02730-z

[28] Rabanal, F., & Martínez, C. (2020). Cryptography for big data environments: Current status, challenges, and opportunities. *Computational and Mathematical Methods*, *2*(1), 1–12. https://doi.org/10.1002/cmm4.1075

[29] Marichamy, V. S., & Natarajan, V. (2023). Blockchain based securing medical records in big data analytics. *Data & Knowledge Engineering*, *144*, 102122. https://doi.org/10.1016/j.datak.2022.102122

[30] Kumar, M., Kumar, A., Verma, S., Bhattacharya, P., Ghimire, D., Kim, S., & Hosen, A. S. M. S. (2023). Healthcare Internet of Things (H-IoT): Current trends, future prospects, applications, challenges, and security issues. *Electronics*, *12*(9), 2050. https://doi.org/10.3390/electronics12092050

[31] Lin, C.-H., Wen, C.-H., Lai, H.-Y., Huang, P.-T., Chen, P.-Y., Li, C.-M., & Pai, N.-S. (2023). Multilayer convolutional processing network based cryptography mechanism for digital images infosecurity. *Processes*, *11*(5), 1476. https://doi.org/10.3390/pr11051476

[32] Srivastava, D., Pandey, H., & Agarwal, A. K. (2023). Complex predictive analysis for health care: A comprehensive review. *Bulletin of Electrical Engineering and Informatics*, *12*(1), 521–531. https://doi.org/10.11591/eei.v12i1.4373

[33] Rajaprakash, S., Bagath Basha, C., Muthuselvan, S., Jaisankar, N., & Singh, R. P. (2020). RBJ25 cryptography algorithm for securing big data. *Journal of Physics: Conference Series*, *1706*(1), 012146. https://doi.org/10.1088/1742-6596/1706/1/012146

[34] Sharma, D., & Kawatra, R. (2023). Security techniques implementation on big data using steganography and cryptography. In *ICT Analysis and Applications: Proceedings of ICT4SD*, 279–302. https://doi.org/10.1007/978-981-19-5224-1_30

[35] Jacob, T. P., Pravin, A., & Kumar, R. R. (2022). A secure IoT based healthcare framework using modified RSA algorithm using an artificial hummingbird based CNN. *Transactions on Emerging Telecommunications Technologies*, *33*(12), e4622. https://doi.org/10.1002/ett.4622

[36] Chidambaram, N., Thenmozhi, K., Raj, P., & Amirtharajan, R. (2024). DNA-chaos governed cryptosystem for cloud-based medical image repository. *Cluster Computing*, *27*(4), 4127–4144. https://doi.org/10.1007/s10586-024-04391-w

[37] Roy, M., Chakraborty, S., Mali, K., Banerjee, A., Ghosh, K., & Chatterjee, S. (2020). Biomedical image security using matrix manipulation and DNA encryption. In *Proceedings of International Ethical Hacking Conference 2019*, 49–60. https://doi.org/10.1007/978-981-15-0361-0_4

[38] Alam, S., Shuaib, M., Ahmad, S., Jayakody, D. N. K., Muthanna, A., Bharany, S., & Elgendy, I. A. (2022). Blockchain-based solutions supporting reliable healthcare for fog computing and internet of medical things (IoMT) integration. *Sustainability*, 14(22), 15312. https://doi.org/10.3390/su142215312

[39] Desai, S. D., Patil, N., Nirmala, S. R., Kulkarni, S., Desai, P. D., & Shinde, D. (2022). Deep neural network based medical image steganography. In *2022 International Conference on Smart Technologies and Systems for Next Generation Computing*, 1–5. https://doi.org/10.1109/ICSTSN53084.2022.9761321

[40] Abikoye, O. C., & Ogundokun, R. O. (2021). Efficiency of LSB steganography on medical information. *International Journal of Electrical and Computer Engineering*, *11*(5), 4157–4164. https://doi.org/10.11591/ijece.v11i5.pp4157-4164

[41] R, V. C., & Madhavan, P. (2022). A comprehensive analysis of IoT security using various cryptographic methods. In *2022 8th International Conference on Smart Structures and Systems*, 1–4. https://doi.org/10.1109/ICSSS54381.2022.9782268

[42] Gong, C., Zhang, J., Yang, Y., Yi, X., Zhao, X., & Ma, Y. (2020). Detecting fingerprints of audio steganography software. *Forensic Science International: Reports*, *2*, 100075. https://doi.org/10.1016/j.fsir.2020.100075

[43] Saxena, A., Misra, D., Ganesamoorthy, R., Arias Gonzales, J. L., Almashaqbeh, H. A., & Tripathi, V. (2022). Artificial intelligence wireless network data security system for medical records using cryptography management. In *2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering*, 2555–2559. https://doi.org/10.1109/ICACITE53722.2022.9823615

[44] Wibawa, F., Catak, F. O., Sarp, S., & Kuzlu, M. (2022). BFV-based homomorphic encryption for privacy-preserving CNN models. *Cryptography*, *6*(3), 34. https://doi.org/10.3390/cryptography6030034

[45] Adee, R., & Mouratidis, H. (2022). A dynamic four-step data security model for data in cloud computing based on cryptography and steganography. *Sensors*, *22*(3), 1109. https://doi.org/10.3390/s22031109

[46] Ali, A., Pasha, M. F., Ali, J., Fang, O. H., Masud, M., Jurcut, A. D., & Alzain, M. A. (2022). Deep learning based homomorphic secure search-able encryption for keyword search in blockchain healthcare system: A novel approach to cryptography. *Sensors*, *22*(2), 528. https://doi.org/10.3390/s22020528

[47] Boukari, S., & Bobbo, J. (2020). An improved cybersecurity model using cryptography and steganography with NTRU-LSB algorithm. *SAR Journal - Science and Research*, *3*(2), 71–78. https://doi.org/10.18421/SAR32-04

[48] Kore, A., & Patil, S. (2022). Cross layered cryptography based secure routing for IoT-enabled smart healthcare system. *Wireless Networks*, *28*(1), 287–301. https://doi.org/10.1007/s11276-021-02850-5

[49] Hachaj, T., Koptyra, K., & Ogiela, M. R. (2021). Eigenfaces-based steganography. *Entropy*, *23*(3), 273. https://doi.org/10.3390/e23030273

[50] Ahmad, M. A., Elloumi, M., Samak, A. H., Al-Sharafi, A. M., Alqazzaz, A., Kaid, M. A., & Iliopoulos, C. (2022). Hiding

patients' medical reports using an enhanced wavelet steganography algorithm in DICOM images. *Alexandria Engineering Journal*, *61*(12), 10577–10592. https://doi.org/10.1016/j.aej.2022.03.056

[51] Voleti, L., Balajee, R. M., Vallepu, S. K., Bayoju, K., & Srinivas, D. (2021). A secure image steganography using improved LSB technique and Vigenere cipher algorithm. In *2021 International Conference on Artificial Intelligence and Smart Systems*, 1005–1010. https://doi.org/10.1109/ICAIS50930.2021.9395794

[52] AlEisa, H. N. (2022). Data confidentiality in healthcare monitoring systems based on image steganography to improve the exchange of patient information using the Internet of Things. *Journal of Healthcare Engineering*, *2022*(1), 7528583. https://doi.org/10.1155/2022/7528583

[53] Banerjee, S., & Singh, G. K. (2021). A new approach of ECG steganography and prediction using deep learning. *Biomedical Signal Processing and Control*, *64*, 102151. https://doi.org/10.1016/j.bspc.2020.102151

[54] Sarosh, P., Parah, S. A., Bhat, G. M., & Muhammad, K. (2021). A security management framework for big data in smart healthcare. *Big Data Research*, *25*, 100225. https://doi.org/10.1016/j.bdr.2021.100225

[55] Soni, N., Saini, I., & Singh, B. (2021). An integer wavelet transform and pixel value differencing based feature specific hybrid technique for 2D ECG steganography with high payload capacity. *Multimedia Tools and Applications*, *80*(6), 8505–8540. https://doi.org/10.1007/s11042-020-09856-9

[56] Khalifeh, S., Georgi, J., & Shakhatreh, S. (2022). Design and implementation of a steganography-based system that provides protection for breast cancer patient's data. In *2022 56th Annual Conference on Information Sciences and Systems*, 19–24. https://doi.org/10.1109/CISS53076.2022.9751183

[57] Li, C., Dong, M., Li, J., Xu, G., Chen, X.-B., Liu, W., & Ota, K. (2022). Efficient medical big data management with keyword-searchable encryption in healthchain. *IEEE Systems Journal*, *16*(4), 5521–5532. https://doi.org/10.1109/JSYST.2022.3173538

[58] Alkhliwi, S. (2021). Encryption-based image steganography technique for secure medical image transmission during the COVID-19 pandemic. *International Journal of Computer Science and Network Security*, *21*(3), 83–93. https://doi.org/10.22937/IJCSNS.2021.21.3.12

[59] Georgieva-Tsaneva, G., Bogdanova, G., & Gospodinova, E. (2022). Mathematically based assessment of the accuracy of protection of cardiac data realized with the help of cryptography and steganography. *Mathematics*, *10*(3), 390. https://doi.org/10.3390/math10030390

[60] El-Shafai, W., Khallaf, F., El-Rabaie, E.-S. M., & Abd El-Samie, F. E. (2022). Proposed neural SAE-based medical image cryptography framework using deep extracted features for smart IoT healthcare applications. *Neural Computing and Applications*, *34*(13), 10629–10653. https://doi.org/10.1007/s00521-022-06994-z

[61] Mohsin, A. H., Zaidan, A. A., Zaidan, B. B., Mohammed, K. I., Albahri, O. S., Albahri, A. S., & Alsalem, M. A. (2021). PSO–blockchain-based image steganography: Towards a new method to secure updating and sharing COVID-19 data in decentralised hospitals intelligence architecture. *Multimedia Tools and Applications*, *80*(9), 14137–14161. https://doi.org/10.1007/s11042-020-10284-y

[62] Elghandour, A., Salah, A., & Karawia, A. (2022). A new cryptographic algorithm via a two-dimensional chaotic map. *Ain Shams Engineering Journal*, *13*(1), 101489. https://doi.org/10.1016/j.asej.2021.05.004

[63] Abunadi, I., Abdullah Mengash, H., S. Alotaibi, S., Asiri, M. M., Ahmed Hamza, M., Zamani, A. S., …, & Yaseen, I. (2022). Optimal multikey homomorphic encryption with steganography approach for multimedia security in Internet of Everything environment. *Applied Sciences*, *12*(8), 4026. https://doi.org/10.3390/app12084026

[64] Yu, S., & Park, K. (2022). SALS-TMIS: Secure, anonymous, and lightweight privacy-preserving scheme for IoMT-enabled TMIS environments. *IEEE Access*, *10*, 60534–60549. https://doi.org/10.1109/ACCESS.2022.3181182

[65] Falmari, V. R., Brindha, M., & Ko, S. (2022). Secure COVID-19 electronic health records management for telediagnosis and travel ticket assistant system using cryptographic approaches. *SN Computer Science*, *3*(5), 403. https://doi.org/10.1007/s42979-022-01284-w

[66] Al-Shaarani, F., & Gutub, A. (2022). Securing matrix counting-based secret-sharing involving crypto steganography. *Journal of King Saud University - Computer and Information Sciences*, *34*(9), 6909–6924. https://doi.org/10.1016/j.jksuci.2021.09.009

[67] Kaushal, R. K., Bhardwaj, R., Kumar, N., Aljohani, A. A., Gupta, S. K., Singh, P., & Purohit, N. (2022). Using mobile computing to provide a smart and secure Internet of Things (IoT) framework for medical applications. *Wireless Communications and Mobile Computing*, *2022*(1), 8741357. https://doi.org/10.1155/2022/8741357

[68] Adeniyi, A. E., Abiodun, K. M., Awotunde, J. B., Olagunju, M., Ojo, O. S., & Edet, N. P. (2023). Implementation of a block cipher algorithm for medical information security on cloud environment: Using modified advanced encryption standard approach. *Multimedia Tools and Applications*, *82*(13), 20537–20551. https://doi.org/10.1007/s11042-023-14338-9

[69] Sameer Jabbar, M., & Saeed Issa, S. (2023). A crypto-steganography healthcare management: Towards a secure communication channel for data COVID-19 updating. *Indonesian Journal of Electrical Engineering and Computer Science*, *29*(2), 1102–1112. https://doi.org/10.11591/ijeecs.v29.i2.pp1102-1112

[70] Said, O. (2022). LBSS: A lightweight blockchain-based security scheme for IoT-enabled healthcare environment. *Sensors*, *22*(20), 7948. https://doi.org/10.3390/s22207948

[71] Chowdhuri, P., Pal, P., & Si, T. (2023). A novel steganographic technique for medical image using SVM and IWT. *Multimedia Tools and Applications*, *82*(13), 20497–20516. https://doi.org/10.1007/s11042-022-14301-0

[72] Younus, Z. S., & Hussain, M. K. (2022). Image steganography using exploiting modification direction for compressed encrypted data. *Journal of King Saud University - Computer and Information Sciences*, *34*(6), 2951–2963. https://doi.org/10.1016/j.jksuci.2019.04.008

[73] Huang, C.-T., Shongwe, N. S., & Weng, C.-Y. (2023). Enhanced embedding capacity for data hiding approach based on pixel value differencing and pixel shifting technology. *Electronics*, *12*(5), 1200. https://doi.org/10.3390/electronics12051200

[74] Abdul, W. (2022). Security of medical images over insecure communication channels using zero-steganography. *International Journal of Distributed Sensor Networks*, *18*(2), 155014772110063. https://doi.org/10.1177/15501477211006347

[75] Abdelbar, M. S., Ali, A. A., & Hasabala, M. (2021). A technique for increasing payload capacity of RGB images steganography based on mod factor and segmentation. *International Journal of Computer Applications*, *183*(13), 29–35. https://doi.org/10.5120/ijca2021921439

[76] Rahman, S., Masood, F., Ullah Khan, W., Ullah, N., Qudus Khan, F., Tsaramirsis, G., …, & Ashraf, M. (2020). A novel approach of image steganography for secure communication based on LSB substitution technique. *Computers, Materials & Continua*, *64*(1), 31–61. https://doi.org/10.32604/cmc.2020.09186

[77] Nasr, M. A., El-Shafai, W., Abdel-Salam, N., El-Rabaie, E.-S. M., El-Fishawy, A. S., & El-Samie, F. E. A. (2023). Efficient information hiding in medical optical images based on piecewise linear chaotic maps. *Journal of Optics*, *52*(4), 1852–1866. https://doi.org/10.1007/s12596-023-01128-7

[78] Castro, F., Impedovo, D., & Pirlo, G. (2023). A medical image encryption scheme for secure fingerprint-based authenticated transmission. *Applied Sciences*, *13*(10), 6099. https://doi.org/10.3390/app13106099

[79] Awadh, W. A., Alasady, A. S., & Hamoud, A. K. (2022). Hybrid information security system via combination of compression, cryptography, and image steganography. *International Journal of Electrical and Computer Engineering*, *12*(6), 6574–6584. https://doi.org/10.11591/ijece.v12i6.pp6574-6584

[80] Akkasaligar, P. T., & Biradar, S. (2020). Selective medical image encryption using DNA cryptography. *Information Security Journal: A Global Perspective*, *29*(2), 91–101. https://doi.org/10.1080/19393555.2020.1718248

[81] Bermani, A. K., Murshedi, T. A. K., & Abod, Z. A. (2021). A hybrid cryptography technique for data storage on cloud computing. *Journal of Discrete Mathematical Sciences and Cryptography*, *24*(6), 1613–1624. https://doi.org/10.1080/09720529.2020.1859799

[82] Kumar, L. A., Srivastava, S., R., B. S., H Shajin, F., & Rajesh, P. (2022). Hybrid visual and optimal elliptic curve cryptography for medical image security in IoT. *ECTI Transactions on Computer and Information Technology*, 16(3), 324–337. https://doi.org/10.37936/ecti-cit.2022163.246991

[83] Olvera-Martinez, L. A., Cedillo-Hernandez, M., Diaz-Rodriguez, C. A., & Jimenez-Borgonio, E. T. (2022). Secure exchange of medical images via extended visual cryptography. *Revista Mexicana de Ingenieria Biomedica*, *43*(2), 64–77. https://doi.org/10.17488/RMIB.43.2.5

[84] Alqadi, Z. (2022). Secure, based on pixel value encoding-decoding method for medical color image cryptography. *International Journal of Computer Science and Mobile Computing*, *11*(4), 25–35. https://doi.org/10.47760/ijcsmc.2022.v11i04.005

[85] Huang, T., Xu, J., Tu, S., & Han, B. (2023). Robust zero-watermarking scheme based on a depthwise overparameterized VGG network in healthcare information security. *Biomedical Signal Processing and Control*, *81*, 104478. https://doi.org/10.1016/j.bspc.2022.104478

[86] Abdellatef, E., Naeem, E. A., & El-Samie, F. E. A. (2024). DeepEnc: Deep learning-based CT image encryption approach. *Multimedia Tools and Applications*, *83*(4), 11147–11167. https://doi.org/10.1007/s11042-023-15818-8

[87] Elkamchouchi, D. H., D. Algarni, A., M. Ghoniem, R., & G. Mohamed, H. (2022). A deep learning signed medical image based on cryptographic techniques. *Indonesian Journal of Electrical Engineering and Computer Science*, *29*(1), 481–495. https://doi.org/10.11591/ijeecs.v29.i1.pp481-495

[88] Karthikeyini, S., Sagayaraj, R., Rajkumar, N., & Pillai, P. K. (2023). Security in medical image management using ant colony optimization. *Information Technology and Control*, *52*(2), 276–287. https://doi.org/10.5755/j01.itc.52.2.32532

[89] Hussain, A. Z., & Khodher, M. A. A. (2023). Medical image encryption using multi chaotic maps. *TELKOMNIKA Telecommunication Computing Electronics and Control*, *21*(3), 556. https://doi.org/10.12928/telkomnika.v21i3.24324

[90] Selvaraj, J., Lai, W.-C., Kavin, B. P., C., K., & Seng, G. H. (2023). Cryptographic encryption and optimization for Internet of Things based medical image security. *Electronics*, *12*(7), 1636. https://doi.org/10.3390/electronics12071636

[91] Xie, H., Zhang, Y., Li, Z., & Zhang, H. (2023). Color medical image cryptography technology based on segmentation and fractional-order hyperchaotic system. *Medical & Biological Engineering & Computing*, *61*(1), 109–127. https://doi.org/10.1007/s11517-022-02700-2

[92] V, S. V. H., & K, R. (2022). Augmented security for healthcare data using obfuscation and elliptic curve cryptography algorithm in health cloud environment. *Concurrency and Computation: Practice and Experience*, *34*(26), e7275. https://doi.org/10.1002/cpe.7275

[93] Nazari, H., Bidgoli, M. M., & Ghasvari, H. (2023). Integration of lightweight cryptography and watermarking with compression for high speed and reliable communication of digital images in IoT. *IET Image Processing*, *17*(10), 2984–3001. https://doi.org/10.1049/ipr2.12849

[94] Khare, P., & Srivastava, V. K. (2021). A secured and robust medical image watermarking approach for protecting integrity of medical images. *Transactions on Emerging Telecommunications Technologies*, *32*(2), e3918. https://doi.org/10.1002/ett.3918

[95] Akkasaligar, P. T., Biradar, S., & Biradar, S. (2022). Multilevel security for medical image using heterogeneous chaotic map and deoxyribonucleic acid sequence operations. *Concurrency and Computation: Practice and Experience*, *34*(24), e7222. https://doi.org/10.1002/cpe.7222

[96] Karawia, A. A. (2021). Medical image steganographic algorithm via modified LSB method and chaotic map. *IET Image Processing*, *15*(11), 2580–2590. https://doi.org/10.1049/ipr2.12246

[97] Aouissaoui, I., Bakir, T., & Sakly, A. (2021). Robustly correlated key-medical image for DNA-chaos based encryption. *IET Image Processing*, *15*(12), 2770–2786. https://doi.org/10.1049/ipr2.12261

[98] Avula Gopalakrishna, C., & Basarkod, P. I. (2023). An efficient lightweight encryption model with re-encryption scheme to create robust blockchain architecture for COVID-vula *GopaTransactions on Emerging Telecommunications Technologies*, *34*(1), e4653. https://doi.org/10.1002/ett.4653

[99] Mahajan, H. B., & Junnarkar, A. A. (2023). Smart healthcare system using integrated and lightweight ECC with private blockchain for multimedia medical data processing. *Multimedia Tools and Applications*, *82*(28), 44335–44358. https://doi.org/10.1007/s11042-023-15204-4

[100] Konyar, M. Z., & Öztürk, S. (2020). Reed Solomon coding-based medical image data hiding method against salt and pepper noise. Symmetry, 12(6), 899. https://doi.org/10.3390/sym12060899

[101] Y. Shakor, M. Y., Surameery, N. M. S., & N. Khlaif, Z. (2023). Hybrid security model for medical image protection in cloud. *Diyala Journal of Engineering Sciences*, *16*(1), 68–77. https://doi.org/10.24237/djes.2023.16107

[102] Patra, A., Saha, A., & Bhattacharya, K. (2023). Efficient storage and encryption of 32-slice CT scan images using phase grating. *Arabian Journal for Science and Engineering*, *48*(2), 1757–1770. https://doi.org/10.1007/s13369-022-06986-0

[103] El-Shafai, W., Almomani, I., Ara, A., & Alkhayer, A. (2023). An optical-based encryption and authentication algorithm for color and grayscale medical images. *Multimedia Tools and*

Applications, *82*(15), 23735–23770. https://doi.org/10.1007/s11042-022-14093-3

[104] Yepdia, L. M. H., & Tiedeu, A. (2021). Secure transmission of medical image for telemedicine. *Sensing and Imaging*, *22*(1), 17. https://doi.org/10.1007/s11220-021-00340-8

[105] Kumar, M., & Gupta, P. (2021). A new medical image encryption algorithm based on the 1D logistic map associated with pseudo-random numbers. *Multimedia Tools and Applications*, *80*(12), 18941–18967. https://doi.org/10.1007/s11042-020-10325-6

[106] Elamir, M. M., Al-atabany, W. I., & Mabrouk, M. S. (2021). Hybrid image encryption scheme for secure e-health systems. *Network Modeling Analysis in Health Informatics and Bioinformatics*, *10*(1), 35. https://doi.org/10.1007/s13721-021-00306-6

[107] Zhang, B., Rahmatullah, B., Wang, S. L., & Liu, Z. (2023). A plain-image correlative semi-selective medical image encryption algorithm using enhanced 2D-logistic map. *Multimedia Tools and Applications*, *82*(10), 15735–15762. https://doi.org/10.1007/s11042-022-13744-9

[108] Ratheesh, T. K., & Paul, V. (2021). An effective mechanism for the secure transmission of medical images using compression and public key encryption mechanism. In *Smart Computing Techniques and Applications: Proceedings of the Fourth International Conference on Smart Computing and Informatics*, 2, 317–325. https://doi.org/10.1007/978-981-16-1502-3_32

[109] Wang, X., & Wang, Y. (2023). Multiple medical image encryption algorithm based on scrambling of region of interest and diffusion of odd-even interleaved points. *Expert Systems with Applications*, *213*, 118924. https://doi.org/10.1016/j.eswa.2022.118924

[110] R, A., & C, M. (2024). Medical image security by crypto watermarking using enhanced chaos and fruit fly optimization algorithm with SWT and SVD. *Multimedia Tools and Applications*, *83*(27), 70451–70476. https://doi.org/10.1007/s11042-024-19019-9

[111] Kumar, S., & Sharma, D. (2024). A chaotic based image encryption scheme using elliptic curve cryptography and genetic algorithm. *Artificial Intelligence Review*, *57*(4), 87. https://doi.org/10.1007/s10462-024-10719-0

[112] Kasim, Ö. (2022). Secure medical image encryption with Walsh–Hadamard transform and lightweight cryptography algorithm. *Medical & Biological Engineering & Computing*, *60*(6), 1585–1594. https://doi.org/10.1007/s11517-022-02565-5

[113] Yan, M., Hu, Y., & Zhang, H. (2023). Progressive meaningful visual cryptography for secure communication of grayscale medical images. *Multimedia Tools and Applications*, *83*(11), 33639–33652. https://doi.org/10.1007/s11042-023-16960-z

[114] John, S., & Kumar, S. N. (2023). IoT based medical image encryption using linear feedback shift register – Towards ensuring security for teleradiology applications. *Measurement: Sensors*, *25*, 100676. https://doi.org/10.1016/j.measen.2023.100676

[115] Priyanka, & Kumar Singh, A. (2022). FastMIE: Faster medical image encryption without compromising security. *Measurement*, *196*, 111175. https://doi.org/10.1016/j.measurement.2022.111175

[116] Peng, Y., Fu, C., Zheng, Y., Tian, Y., Cao, G., & Chen, J. (2024). Medical steganography: Enhanced security and image quality, and new S-Q assessment. *Signal Processing*, *223*, 109546. https://doi.org/10.1016/j.sigpro.2024.109546

[117] Nadhan, A. S., & Jeena Jacob, I. (2024). Enhancing healthcare security in the digital era: Safeguarding medical images with lightweight cryptographic techniques in IoT healthcare applications. *Biomedical Signal Processing and Control*, *88*, 105511. https://doi.org/10.1016/j.bspc.2023.105511

[118] Boyraz, O. F., Guleryuz, E., Akgul, A., Yildiz, M. Z., Kiran, H. E., & Ahmad, J. (2022). A novel security and authentication method for infrared medical image with discrete time chaotic systems. *Optik*, *267*, 169717. https://doi.org/10.1016/j.ijleo.2022.169717

[119] Zermi, N., Khaldi, A., Kafi, R., Kahlessenane, F., & Euschi, S. (2021). A DWT-SVD based robust digital watermarking for medical image security. *Forensic Science International*, *320*, 110691. https://doi.org/10.1016/j.forsciint.2021.110691

[120] Zhang, Z., Zhou, N., Sun, B., Banerjee, S., & Mou, J. (2024). Multimedia healthcare cloud personal archives security system based on compressed sensing and multi-image encryption. *Journal of the Franklin Institute*, *361*(8), 106844. https://doi.org/10.1016/j.jfranklin.2024.106844

[121] Ningthoukhongjam, T. R., Devi Heisnam, S., & Singh Khumanthem, M. (2024). Medical image encryption through chaotic asymmetric cryptosystem. *IEEE Access*, *12*, 73879–73888. https://doi.org/10.1109/ACCESS.2024.3404088

[122] Jamal, S. S., Hazzazi, M. M., Khan, M. F., Bassfar, Z., Aljaedi, A., & Ul Islam, Z. (2024). Region of interest-based medical image encryption technique based on chaotic S-boxes. *Expert Systems with Applications*, *238*, 122030. https://doi.org/10.1016/j.eswa.2023.122030

[123] Girardi, F., De Gennaro, G., Colizzi, L., & Convertini, N. (2020). Improving the healthcare effectiveness: The possible role of EHR, IoMT and blockchain. *Electronics*, *9*(6), 884. https://doi.org/10.3390/electronics9060884

[124] Subramanian, N., Elharrouss, O., Al-Maadeed, S., & Bouridane, A. (2021). Image steganography: A review of the recent advances. *IEEE Access*, *9*, 23409–3423. https://doi.org/10.1109/ACCESS.2021.3053998

[125] Sharma, S., & Mehrotra, S. (2022). Cryptographic techniques for data processing. In *Proceedings of the 5th Joint International Conference on Data Science & Management of Data (9th ACM IKDD CODS and 27th COMAD)*, 344–347. https://doi.org/10.1145/3493700.3493771

[126] Subbiah, V. (2023). The next generation of evidence-based medicine. *Nature Medicine*, *29*(1), 49–58. https://doi.org/10.1038/s41591-022-02160-z

[127] Ramapriya, B., & Kalpana, Y. (2023). A competent medical image steganography using improved optimization algorithm with Huffman encoding techniques. In *2023 7th International Conference on Computing Methodologies and Communication*, 1065–1073. https://doi.org/10.1109/ICCMC56507.2023.10083698

[128] Al-Chaab, W., Abduljabbar, Z. A., Abood, E. W., Nyangaresi, V. O., Mohammed, H. M., & Ma, J. (2023). Secure and low-complexity medical image exchange based on compressive sensing and LSB audio steganography. *Informatica*, *47*(6), 65–74. https://doi.org/10.31449/inf.v47i6.4628

[129] Sodhro, A. H., Awad, A. I., Beek, J. V. D., & Nikolakopoulos, G. (2022). Intelligent authentication of 5G healthcare devices: A survey. *Internet of Things*, *20*, 100610. https://doi.org/10.1016/j.iot.2022.100610

[130] Senthilkumar, M., Suthendran, K., & Ravi, V. (2024). Enhancing medical image security through a novel framework: Crypto-aware elliptic curve Diffie–Hellman with key derivation function. *The Open Bioinformatics Journal*, *17*(1), e18750362303634. https://doi.org/10.2174/0118750362303634240624112446

[131] Priyanka, & Singh, A. K. (2023). A survey of image encryption for healthcare applications. *Evolutionary Intelligence*, *16*(3), 801–818. https://doi.org/10.1007/s12065-021-00683-x

[132] Sharma, S., Malik, M., Prabha, C., Al-Rasheed, A., Alduailij, M., & Almakdi, S. (2023). Robust image watermarking using LWT and stochastic gradient firefly algorithm. *Computers, Materials & Continua*, *75*(1), 393–407. https://doi.org/10.32604/cmc.2023.033536

[133] Takaoğlu, M., Özyavaş, A., Ajlouni, N., & Takaoğlu, F. (2023). Highly secured hybrid image steganography with an improved key generation and exchange for one-time-pad encryption method. *Afyon Kocatepe University Journal of Sciences and Engineering*, *23*(1), 101–114. https://doi.org/10.35414/akufemubid.1128075

[134] Pramanik, S., Samanta, D., Dutta, S., Ghosh, R., Ghonge, M., & Pandey, D. (2020). Steganography using improved LSB approach and asymmetric cryptography. In *2020 IEEE International Conference on Advent Trends in Multidisciplinary Research and Innovation*, 1–5. https://doi.org/10.1109/ICATMRI51801.2020.9398408

[135] Mothi, R., & Karthikeyan, M. (2019). Protection of bio medical iris image using watermarking and cryptography with WPT. *Measurement*, *136*, 67–73. https://doi.org/10.1016/j.measurement.2018.12.030

[136] Lingamallu, N. S., & Veeramani, V. (2021). Secure and covert communication using steganography by wavelet transform. *Optik*, *242*, 167167. https://doi.org/10.1016/j.ijleo.2021.167167

[137] Suganthi, S., Gupta, V., Sisaudia, V., & Poongodi, T. (2021). Data analytics in healthcare systems – Principles, challenges, and applications. In H. Bansal, B. Balusamy, T. Poongodi, & F. Khan Kp (Eds.), *Machine learning and analytics in healthcare systems: Principles and applications* (pp. 1–22). CRC Press. https://doi.org/10.1201/9781003185246-1

[138] Zeenath, DurgaDevi, K., & Carey M, J. W. (2024). An efficient image encryption scheme for medical image security. *International Journal of Electrical and Electronics Research*, *12*(3), 964–976. https://doi.org/10.37391/ijeer.120330

[139] Senthilkumar, M., Suthendran, K., Aparna, S. V. S., Kotha, M., Kirubakaran, S., Dharmireddi, S., & Kumar, V. N. (2024). A novel encryption framework to improve the security of medical images. In *Proceedings of Fifth International Conference on Computer and Communication Technologies*, *1*, 145–159. https://doi.org/10.1007/978-981-99-9704-6_13

[140] Maata, R. L. R., Cordova, R. S., & Halibas, A. (2020). Performance analysis of twofish cryptography algorithm in big data. In *Proceedings of the 2020 9th International Conference on Software and Information Engineering*, 56–60. https://doi.org/10.1145/3436829.3436838

[141] Al Hamid, H. A., Rahman, S. M. M., Hossain, M. S., Almogren, A., & Alamri, A. (2017). A security model for preserving the privacy of medical big data in a healthcare cloud using a fog computing facility with pairing-based cryptography. *IEEE Access*, *5*, 22313–22328. https://doi.org/10.1109/ACCESS.2017.2757844

[142] Ali, A., Rahim, H. A., Ali, J., Pasha, M. F., Masud, M., Rehman, A. U., …, & Baz, M. (2021). A novel secure blockchain framework for accessing electronic health records using multiple certificate authority. *Applied Sciences*, *11*(21), 9999. https://doi.org/10.3390/app11219999

How to Cite: Sharma, D., & Prabha, C. (2025). A Systematic Investigation of the Current State of Security in Electronic Medical Images: 2019–2024. *Artificial Intelligence and Applications*. https://doi.org/10.47852/bonviewAIA52026322