Computer Networks and Communications
http://ojs.wiserpub.com/index.php/CNC/

Review

Exploring Approaches for Secure Medical Image Storage and Retrieval: A Comprehensive Survey

Arun Amaithi Rajan*, Vetriselvi V

Department of Computer Science and Engineering, College of Engineering Guindy, Anna University, Chennai 600025, India
* Correspondence: arunamaithirajan@gmail.com

Received: 10 January 2026; **Revised:** 10 March 2026; **Accepted:** 17 March 2026; **Published:** 25 March 2026

Abstract: Medical images, the backbone of digital healthcare, hold critical information for accurate diagnoses and lead to advancements in medical research. However, the increasing amount of these images often entails storage on third-party cloud servers where security and privacy are major concerns. In digital healthcare operations, securely storing and retrieving medical images involves considerable difficulties. This paper investigates how existing techniques handle medical images while maintaining performance and security. It analyzes secure storage strategies like blockchain and encryption and covers secure retrieval strategies like indexing that preserve data security and effective search capabilities. The paper provides insights into the advantages, disadvantages, and applicability of current systems through an extensive evaluation. It also offers thoughtful suggestions and future research paths that could establish a trustworthy and secure medical image management.

***Keywords*:** medical images, secure storage, image encryption, secure image retrieval, encrypted indexing

1. Introduction

In today's modern landscape, images have become intrinsic to our day-to-day interactions and communication channels. Images serve as a powerful medium for conveying information and eliciting emotions everywhere from social media platforms to professional environments [1]. In domains ranging from healthcare to design, images provide key insights and help in decision-making [2]. In healthcare, medical images are critical and play an important role in the diagnosis, surgery planning, and observation of patients' conditions [3]. By using advanced imaging technologies, internal structures, and abnormalities can be visualized by healthcare professionals, and identify the progression of diseases with better clarity and precision. These images serve as invaluable diagnostic tools, enabling physicians to make informed decisions about patient care and treatment strategies [4].

Medical imaging has various techniques that generate visual representations of the body's interior parts, helping in diagnosis, and monitoring of medical conditions. Figure 1 shows the different types of medical images. Magnetic Resonance Imaging (MRI), X-ray, Computed Tomography (CT), ultrasound, and Positron Emission Tomography (PET) are among the common modalities used [5]. Each medical imaging modality owns unique advantages and applications, contributing to comprehensive patient care across various medical disciplines. X-ray and CT scans are for skeletal and structural imaging, while MRIs are good at soft tissue visualization [6]. Ultrasound provides real-time imaging without

DOI: https://doi.org/10.37256/cnc.4120269576

radiation [7], making it safe for fetal monitoring. PET, using radioactive tracers, enables functional imaging for cancer detection, neurological disorders, and cardiovascular diseases [8]. By leveraging these diverse modalities, healthcare professionals can diagnose conditions early, plan hurdles effectively, and monitor treatment responses accurately. These medical images are available in different file formats as shown in Table 1 [9]. Medical imaging technology is always developing, which propels innovation in diagnosis and treatment modalities for better patient outcomes. As a result, the sector keeps changing.

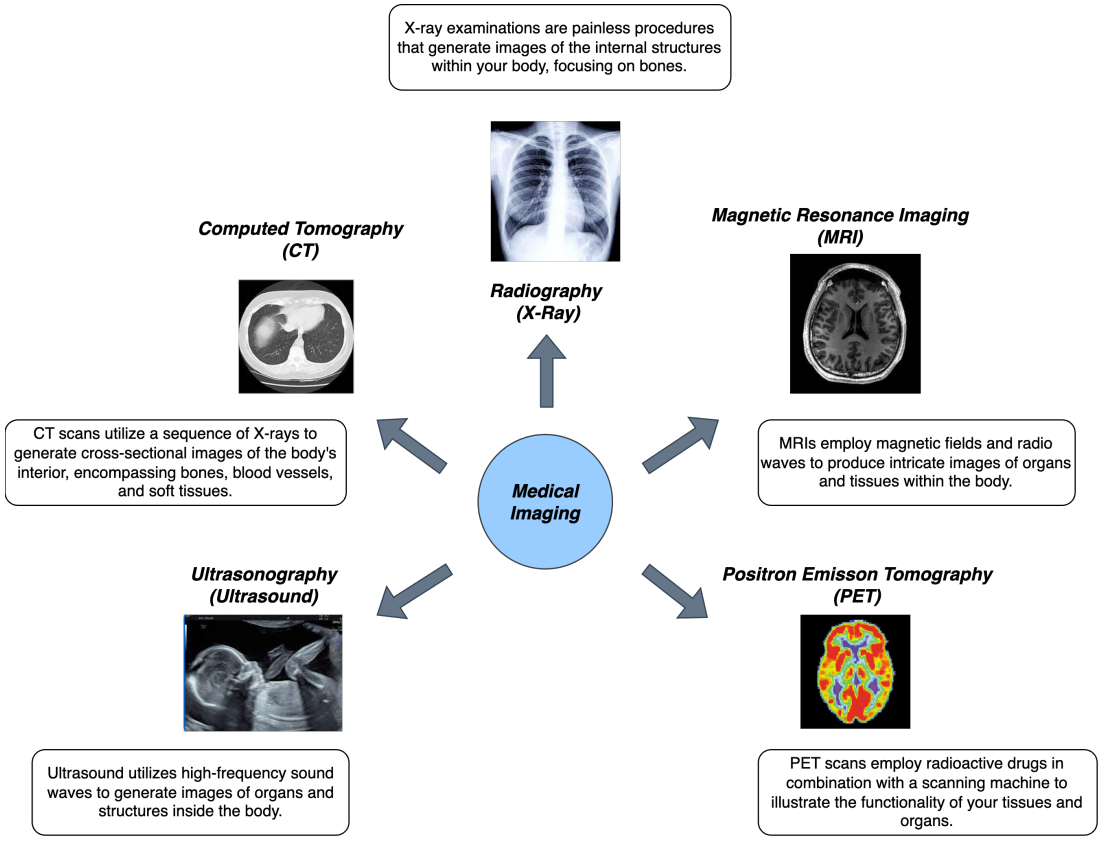

Figure 1. Different types of medical images

Table 1. General formats of medical images

Format	Extension	Header
DICOM	.dcm	Variable length binary stream
MINC	.mnc	Extensible binary stream
NIFTI	.nll	348 or 352-byte binary stream
ANALYZE	.img	348-byte binary stream

The incremental growth of medical imaging data encourages the usage of cloud storage, providing scalability, accessibility, and cost-effectiveness [10]. Issues in healthcare such as local storage systems, easing collaboration, data sharing, and remote access to medical images are overcome by utilizing cloud storage. Cloud storage offers numerous benefits. However, there exist more vulnerabilities that potentially compromise the security and privacy of stored medical images. Data breaches, where unauthorized users gain access to sensitive medical images, insider threats triggered by employees with legitimate access, and data loss because of technical failures are some of the key vulnerabilities [11]. To

establish a secure storage of medical images in the cloud, healthcare organizations need efficient security measures and better security practices. This can be achieved by encryption of medical images both during transmission and at rest, data loss prevention solutions, and granular access controls such as role-based authentication and multi-factor authentication, etc [12]. Healthcare organizations might reduce the risks associated with cloud storage and preserve the availability, integrity, and confidentiality of medical images saved in the cloud by providing a complete security strategy.

Medical image retrieval also plays a significant role in healthcare, providing evidence-based diagnostics and research [13]. Traditionally, this retrieval task is based on manual annotation through techniques like Text-based Image Retrieval (TBIR) [14]. However, because of this time-consuming manual approach, Content-based Image Retrieval (CBIR) came into the domain as a solution [15]. Content-based IR allows image search based on intrinsic image features. This method shows effectiveness, especially with medical images, modernizing the retrieval process and improving efficiency in healthcare settings. If images are encrypted, then the method of retrieving those images becomes a challenge in secure image retrieval [16]. As we know, encryption is necessary for securing sensitive medical images, but still, it introduces difficulties in retrieval mechanisms owing to the need to decrypt the images before access. It introduces additional computational overhead and latency, which heavily compromises the retrieval efficiency [17]. In the field of healthcare, where well-timed access to medical images is crucial for diagnosis and treatment planning, addressing this issue is required. Secure image retrieval methods must strike a balance between preserving the security and integrity of encrypted images while confirming speedy and efficient retrieval. This creates the need for the development of new techniques that optimize retrieval performance without compromising data security [18]. By tackling the essential question of retrieval efficiency within the framework of encrypted medical images, scholars may advance the domain of secure image retrieval and augment the efficiency of healthcare systems in regulating and accessing fundamental medical image information.

In view of above-mentioned issue, this study's main research focus is: What are the ways in which effective data security and retrieval capacity can be collectively delivered and maximized for cloud-based medical image management systems? The focus of this lead question is on the trade-off between the multiple layers of complexity associated with the cryptographic protections needed to provide secure storage of the image data, and the performance requirements of the content-based clinical search operations for both low-latency and high-accuracy operation.The principal question is a major source of analytic focus on storage strategies and retrieval methods. Several studies have focused on the secure storage and retrieval solutions of medical images from cloud repositories [19, 20]. However, the synergy between these operations is crucial for achieving a balance between security and performance.

To our knowledge, this survey represents the first attempt to comprehensively examine this domain from a secure storage and retrieval integrated perspective. Existing surveys addressing the encryption of images [21] or large scale retrieval systems [22] do not treat these essential orderings as an integrated technical silo but rather as a disparate collection of technologies. Our survey takes this integrated position by considering the complete life cycle of medical images stored in the cloud, from secure, private storage to efficient retrieval [23]. This is critical, as the type of encryption used to store images will determine the feasibility and performance of the search mechanisms that will be required to retrieve those images, thus creating a fundamental utility-security tradeoff involved in storing and retrieving images. We qualitatively study the effects of various encryption strategies, such as chaotic maps, DNA cryptography, and blockchain, on computational time and efficiency of retrieving images in order to provide timely decisions for the care of patients in hospital environments, using mean Average Precision (mAP) and retrieval time as metrics. Figure 2 depicts the framework delineating secure medical image storage and retrieval from the cloud. This study makes the following significant contributions.

(1) A thorough survey on secure cloud-based medical image storage and retrieval has been carried out.

(2) The necessity of storing medical images securely using the latest techniques has been discussed.

(3) The significance of secure medical image retrieval has been discussed using a variety of algorithms.

(4) The scope for further research on cloud-based secure medical image storage and retrieval has been delineated.

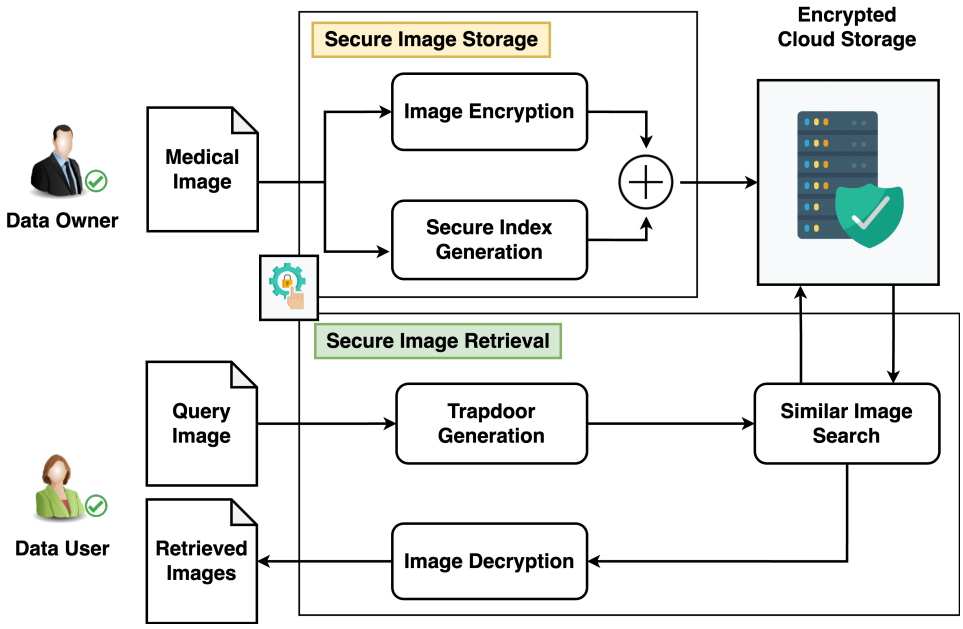

Figure 2. Framework for secure medical image storage and retrieval

The rest of the article is structured as follows: Our search methodology is detailed in Section 2. Section 3 delves into current approaches in secure medical image storage, accompanied by a comparative analysis. The existing techniques for secure medical image retrieval are scrutinized in Section 4. Section 5 is devoted to exploring unresolved issues and delineating future research directions in this domain, while Section 6 provides a comprehensive summary and conclusion for the paper.

2. Search methodology

As detailed in a study article by Snyder [24], we used a comprehensive literature review method to choose and evaluate studies. This section is dedicated to expressing the article collection process for this survey. We searched the standard databases like ACM, Springer, IEEE, arXiv, MDPI, and Elsevier with the standard keywords “secure medical image storage”, “secure healthcare”, “secure medical image retrieval”, and “privacy preservation in medical images”. We retrieved around 135 articles within the period 2019-2026.

The selection procedure consists of two stages: screening of the abstract and screening of the entire article. We evaluated the article’s breadth, depth of research, and originality. Based on the inclusion criteria, the majority of the papers are eliminated following the abstract screening. After a thorough screening, very few articles are eliminated. Ultimately, the chosen articles are divided into two groups to facilitate a rapid study and analysis. We removed 40 papers that are relevant to the selected topic. In the second round of filtering, we did a detailed analysis of the paper and removed around 22 papers. We end up with 73 papers in hand to start the survey. The screening process is shown in Figure 3.

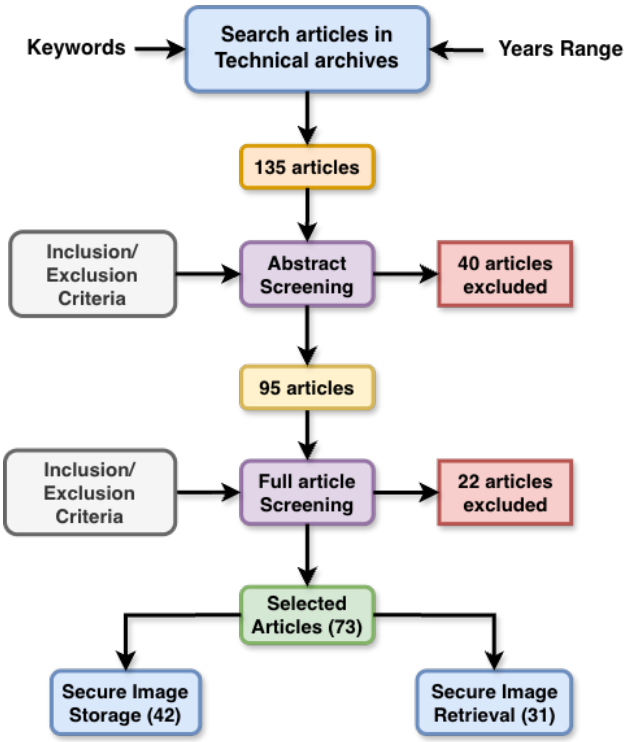

Figure 3. Articles screening process

The formal criteria adopted during abstract and full article screening are displayed in Figure 3 and are described below as the selection process:

(1) **Inclusion Criteria**

• *Thematic Relevance:* Articles must focus specifically on secure storage (e.g., encryption, blockchain, DNA cryptography) or secure retrieval (e.g., deep hashing, encrypted indexing) within the medical imaging field.

• *Technological Scope:* Research must address the problem of offloading data to third party cloud environments.

• *Temporal Relevance:* Publications must fall within the range of 2019-2026 to provide the most up to date state-of-the-art techniques including quantum resistant and AI driven methodologies.

• *Quality and Source:* Articles included in this selection will be peer-reviewed and from reputable technical archives (IEEE, Springer, Elsevier, MDPI, and ACM).

(2) **Exclusion Criteria**

• *Generic Security:* General studies on encryption that do not incorporate the specific characteristics of medical images (high resolution, ROI- requirements/characteristics, DICOM format) will be excluded from consideration.

• *Non-Secure Retrieval:* Articles focusing on standard Content-based Image Retrieval (CBIR), will not be selected for inclusion in this review unless they specifically focus on privacy preservation or security.

• *Low Technical Depth:* Articles that are poster presentations or have little experimental data content (where no metrics such as mean Average Precision (mAP), Normalized Pixel Change Rate (NPCR), or Unified Average Change Index (UACI) are provided) will not qualify for inclusion in the review.

Figure 4a shows the year-wise publications count in this domain ranging from 2019-2026, Figure 4b visualizes the research article and survey article counts in it, and finally, Figure 4c shows the publisher-wise split up of the documents selected from the standard databases. Based on our analysis, we have not identified any survey article that comprehensively addresses both secure image storage and retrieval. This observation has prompted us to undertake the present survey.

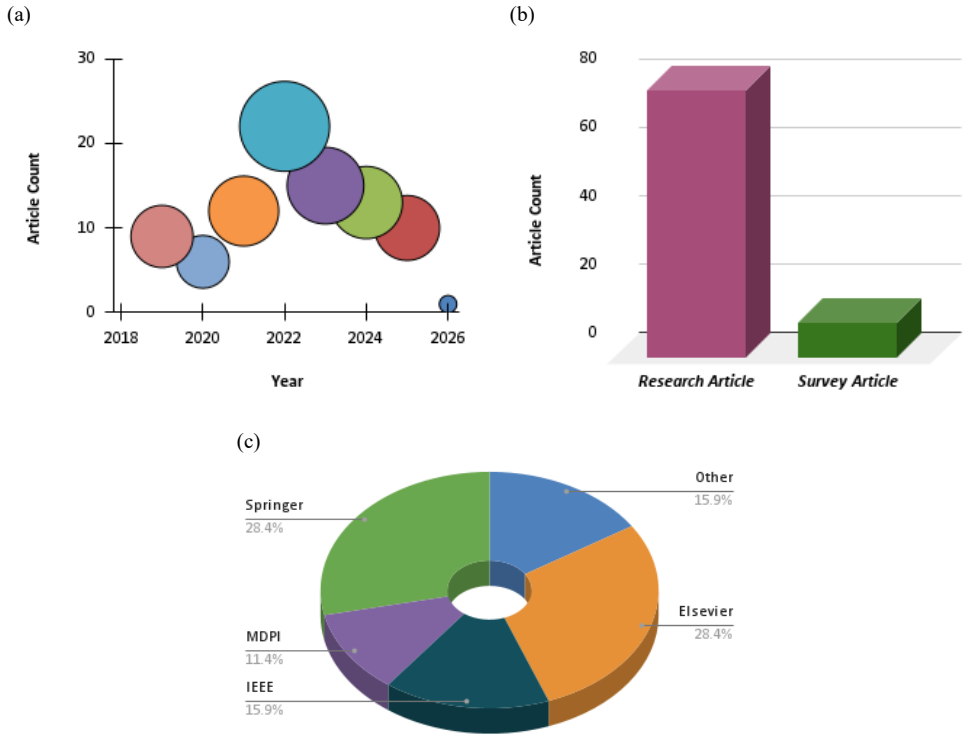

Figure 4. Analysis on collected research articles

The 63 chosen articles are methodologically sufficient as a sample base for three reasons: First, the review of the research presented in this paper adequately covers a very specific niche area of research—the integrated synergy between securing data for storage and retrieval, a research area previously identified via a more general, siloed literature review. Second, the starting pool of 135 articles was filtered using a robust process of evaluation to identify papers which contained high levels of originality and technical complexity to best provide users with high quality, "thoughtful suggestions" rather than simple "summary" statements. Third, the selected articles create a "balanced" distribution between securing data for storage (42 papers) and securing data for retrieval (31 papers) representing the full range of current methods, from Chaotic Maps and DNA Cryptography to Deep Hashing and Multimodal Indexing, therefore the selection of the articles presents a highly comprehensive, although limited, map of the current state of the 'utility-security conundrum' within the context of Digital Health Care.

3. Secure medical image storage

The medical images are used for effective diagnosis and they are very helpful for researchers to analyze and do medical findings. These images contain more critical as well as sensitive information that needs to be hidden. Nowadays, medical images are offloaded to the cloud for easy processing. So, we are relying on a third party for storage. This brings more security and privacy concerns to the healthcare sector. This can be resolved by providing security solutions in the storage. As seen in Figure 1 and Table 1, there are multiple types and formats of medical images. There are two different things, one is securing the image from the attackers which is called image encryption, and another one is hiding the information within the medical image where we do not change the image pixels [21]. Image encryption is a technique where all image pixels are encrypted with a unique key only those who have the key can decrypt the image. This provides confidentiality and authenticity. The watermarking and steogonagraphy on the other side, hides the information within the image. Watermarking mainly provides integrity. Combining image encryption with watermarking provides confidentiality,

integrity, and authenticity to the image. Figure 5 shows the different ways of secure medical image storage are possible from the bird's eye view. In this article, we only be focusing on secure image encryption techniques that are available for medical images. This can be divided into two categories: classical and quantum-based methods.

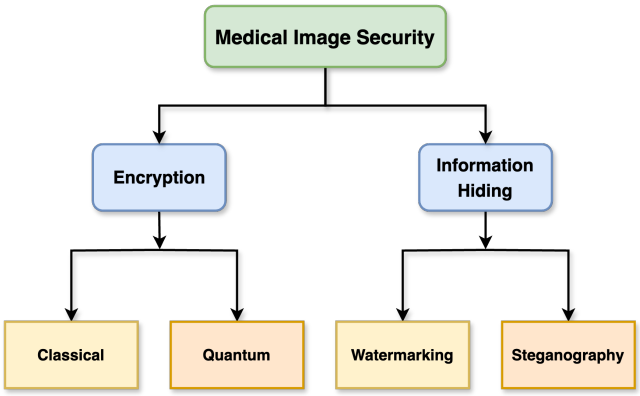

Figure 5. Secure medical image storage techniques

3.1 *Classical image encryption techniques*

Classical image encryption is a cornerstone of data security, ensuring the confidentiality and integrity of visual information across diverse domains. Employing well-established cryptographic algorithms, these techniques transform plaintext images into ciphertext, restricting access to authorized entities only. Unlike modern methods, classical image encryption relies on robust cryptographic primitives and withstand cryptanalysis [25]. This encryption addresses challenges like key management and performance overhead while tailoring encryption parameters to image characteristics like resolution and color depth.

Some survey articles already discuss medical image encryption from different aspects [20, 26]. Through classical image encryption, sensitive visual data is shielded from unauthorized access and malicious exploitation. Generally, obfuscation is text-based to improve the privacy of those data [27]. With robust primitives like substitution-permutation networks and Feistel ciphers, classical encryption methods aim to obfuscate image content and resist cryptanalysis. There are two major domains involved in classical image encryption spatial and transform domain [21]. We will be focusing on spatial domain image encryption techniques in this article. Upcoming sub-sections are dedicated to explaining the spatial domain image encryption models that exist in the medical domain. Figure 6 details the techniques in classical image encryption.

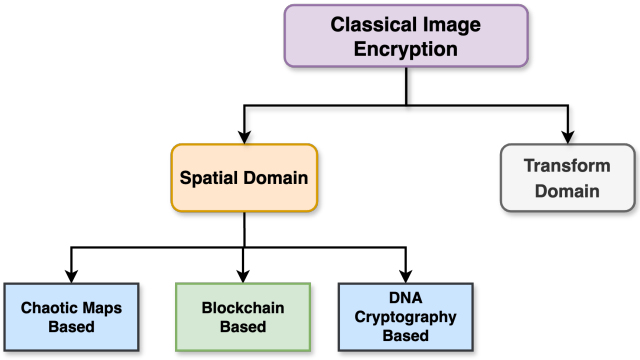

Figure 6. Classical image encryption techniques

3.1.1 *Chaotic maps-based techniques*

Chaotic maps have emerged as powerful tools for both key generation and image encryption due to their inherent properties of sensitivity to initial conditions, unpredictability, and ergodicity. In cryptography, chaotic maps offer a promising avenue for generating secure cryptographic keys by exploiting the chaotic behavior exhibited by nonlinear dynamical systems [28]. Additionally, chaotic maps serve as effective components in image encryption schemes, where they facilitate the transformation of plaintext images into ciphered forms by introducing complexity and randomness. Leveraging chaotic maps for key generation and image encryption holds significant potential in enhancing the security and robustness of cryptographic systems, paving the way for innovative approaches to securing sensitive information in digital environments. Figure 7 shows the Lorenz chaotic map bifurcation diagram.

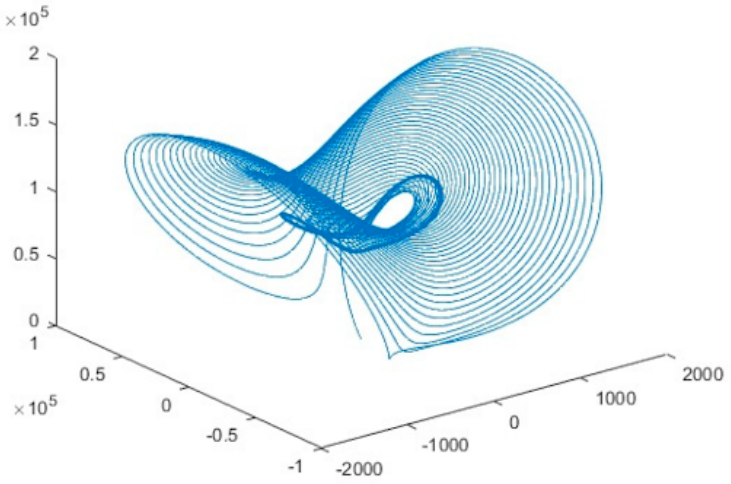

Figure 7. Bifurcation diagram of Lorenz chaotic map

Hua et al. [29] presented an encryption scheme to protect medical images, which entails introducing random data into the image's surrounding areas, carrying out high-speed scrambling and pixel adaptive diffusion to shuffle pixels, and spreading the injected data throughout the image in 2018. The proposed encryption technique shows high-security levels, speediness, and better adaptability to impulse noise and data loss interference compared to other encryption models, using both bitwise eXclusive OR (XOR) and modulo arithmetic implementations for pixel adaptive diffusion. Following by, Moafimadani et al. [30] proposed a method consisting of adaptive diffusion and a high-speed permutation task. The algorithm is found to be effective and appropriate, with good performance in terms of histogram uniformity, sensitivity to key changes, and resistance against noise and occlusion attacks [31]. Su et al. [32] introduced DERCA which is deterministic encryption based on reversible cellular automata for encrypting images. A suggested two-level granularity image encryption allows color histogram extraction for similarity search from encrypted images. The technique encrypts pixels at the pixel granularity or pixel-set -granularity to solve the utility-security conundrum. The utilization of the block-based permutation technique enhances image security and retrieval precision. Different chaotic maps are used such as logistic maps [33], 2D Arnald maps [34], Chen [35], Lorenz [36], Henon, and Tent maps [37] are used for multiple purposes like confusion, diffusion, random key generation, scrambling, and substitution.

Hyperchaotic maps are also used for medical image encryption improving the diffusion rate and providing more security [38]. To improve the performance, image compression-based encryption mechanisms are developed [39, 40]. More medical image encryption methods focus on the Region of Interest (ROI) in medical images which are key areas of medical images and try to secure the particular ROI by encryption [41–43]. Especially Meng et al. [44] use that ROI information for integrity verification. There are multi-level and multiple chaotic map-based image encryption techniques available in medical images which are expensive [45–48]. More lately, A deep learning-based image encryption model was

invented by Nadhan et al. [49]. While chaotic maps offer promising avenues for image encryption, they also present several drawbacks which include sensitivity to initial conditions, limitations in achieving diffusion and confusion, computational complexity, and lack of standardization [50, 51].

3.1.2 *Blockchain-based techniques*

The decentralized and immutable characteristics of blockchain technology present a viable way to overcome issues with medical image storage [52]. By encrypting and distributing images across a decentralized network, blockchain enhances security, enables fine-grained access control, and facilitates interoperability among healthcare providers. With blockchain, medical image storage becomes secure, transparent, and interoperable, ultimately improving patient care and outcomes in the digital age. Figure 8 depicts the basic architecture of Blockchain (BC).

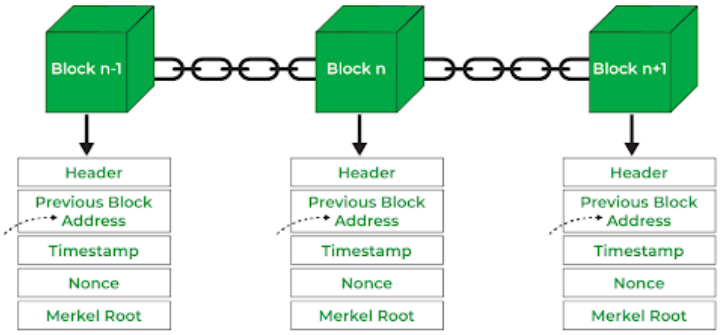

Figure 8. Structure of blockchain

A unique technique for storing sensitive medical data in the BC was proposed by Vetriselvi et al. [53]. Based on the classification of the dataset which is separated into critical and non-critical categories, it has been determined which patient needs surgery. The BC maintains such patients' comprehensive electronic health records, preventing data manipulation and preventing forgeries. BC technique was also used by Alqaralleh et al. [54] to secure Internet of Medical Things (IoMT) data. Sensitive information has been securely hashed and saved in cloud storage that supports BC, rather than being encrypted. The Deep Belief Network (DBN) is utilized for classification and disease prediction based on IoMT data, and Elliptic Curve Cryptography (ECC) is employed for encryption. The speed at which encrypted data can be retrieved from a BC acts as a benchmark for the suggested method's efficacy. Recently Jabarullah et al. [55] proposed a patient-centric distributed image management system that utilizes BC and the Inter-Planetary File System (IPFS) to ensure the secure and efficient sharing and storage of medical images within a trustless environment. To allow distributed and reliable access control, the system makes use of an Ethereum smart contract termed the patient-centric access control protocol. The evaluation results demonstrate the efficiency and feasibility of the proposed scheme. Drawbacks of blockchain-based medical image storage systems include scalability challenges because of the substantial amount of data and potential concerns regarding regulatory compliance and data privacy.

3.1.3 *DNA cryptography-based techniques*

DNA cryptography is the use of the deoxyribonucleic acid (DNA) sequence in data concealment techniques. DNA cryptography is a revolutionary technique for image encryption that combines the latest advances in molecular biology and cryptography [38]. Each letter of the alphabet is changed into a distinct combination of the four bases which are adenine (A), guanine (G), cytosine (C), and thymine (T), that make up human DNA throughout this cryptographic procedure. This method converts the pixels into scrambled and usable forms. By utilizing the internal properties of DNA molecules, such as sequence specificity and vast storage capacity, DNA cryptography introduces a novel method for securing digital images.

This approach involves encoding image data into DNA sequences, which act as cryptographic keys or ciphertexts, using techniques like DNA sequence alignment, and hybridization for encryption and decryption processes. With its potential for high-density storage, parallel processing, and resistance to conventional cyber attacks, DNA cryptography holds promise for enhancing the security and robustness of image encryption methods, paving the way for advanced applications in secure image transmission and storage across diverse domains [56–58]. DNA encoding has its benefits. Where we can work on DNA-encoded data. Table 2 shows the DNA addition.

Table 2. DNA addition sample

+	A	C	G	T
A	A	C	G	T
C	C	A	T	G
G	G	T	C	A
T	T	G	A	C

An effective and safe mutual authentication system utilizing Quark lightweight hash design and ECC with additional DNA cryptography in medical images was presented by Moosavi et al. [59]. DNA encoding has to be combined with chaotic maps to bring more diffusion in pixels [60]. Yousif et al. [35] used both Chen Lorenz 4D maps for bit replacing and DNA cryptography to come up with a new strong image encryption algorithm. This could be extended to medical images. Amaithi Rajan et al. [37] proposed a novel image encryption model for the secure storage and processing of medical images in a cloud server, utilizing hyperchaotic maps, DNA encoding, and bitplane scrambling. The model demonstrates robustness and resistance against attacks, ensuring the security and privacy of sensitive image information. Issues of DNA encoding in image encryption include limited encoding capacity for large images, and potential errors in DNA synthesis leading to data corruption. The following Table 3 summarizes the cryptography techniques discussed so far. Ch denotes chaotic, BC denotes Blockchain, and DNA denotes DNA cryptography-based technique. The comparative analysis provides the conclusion that DNA computing is effective for space-efficient encryption mechanisms. When time is the focus, chaotic and hyperchaotic-based techniques give better solutions. For tamper-proof or integrity-focused requirements, blockchain comes as the ideal solution.

Table 3. Medical image encryption models: comparative analysis

Year	Article	Category			
		Ch	BC	DNA	Other
2017	Abd El-Latif et al. [61]	✓			
2018	Hua et al. [29]	✓			
2019	Moafimadani et al. [30]	✓			
2019	Su et al. [32]				✓
2020	Vetriselvi et al. [53]		✓		
2021	Jabarullah et al. [55]		✓		
2021	Alqaralleh et al. [54]		✓		
2021	Janani et al. [62]	✓			✓
2021	Balasamy et al. [33]	✓			✓
2021	Khare et al. [34]	✓			
2022	Moosavi et al. [59]			✓	
2022	Ahmad et al. [39]	✓			✓
2022	Kiran et al. [45]	✓			
2022	Ping et al. [42]				✓

Table 3. (cont.)

Year	Article	Category			
		Ch	BC	DNA	Other
2022	Meng et al. [44]	✓			
2022	Zhang et al. [48]	✓			
2022	Yousif et al. [35]			✓	
2022	Elkandoz et al. [47]	✓			
2022	Li et al. [38]	✓		✓	
2023	Gao et al. [63]			✓	✓
2023	Amaithi Rajan et al. [37]	✓		✓	
2023	Wang et al. [46]	✓			
2024	Priyanka et al. [40]	✓			
2024	Jamal et al. [43]	✓			
2024	Nadhan et al. [49]				✓
2025	Cheng et al. [56]				✓
2025	Liao et al. [57]	✓			
2026	Erkan et al. [51]	✓			

3.2 *Quantum-based image encryption techniques*

Quantum-based image encryption represents a groundbreaking frontier in cryptographic techniques, harnessing the principles of quantum mechanics to revolutionize image security [63]. By exploiting the unique properties of quantum systems such as superposition and entanglement, quantum-based encryption methods offer unparalleled levels of security and resistance to traditional decryption techniques. In this paradigm, image data is encoded into quantum states, manipulated using quantum operations, and protected against unauthorized access through quantum key distribution protocols. With the potential to achieve unconditional security and thwart emerging threats in the era of quantum computing, quantum-based image encryption holds immense promise for safeguarding sensitive visual information in the digital age. Figure 9 shows the general quantum image encryption process. There are two ways: images are represented by qubits and then scrambling over them or generated random sequences from quantum-based chaotic maps to do pixel scrambling [64, 65].

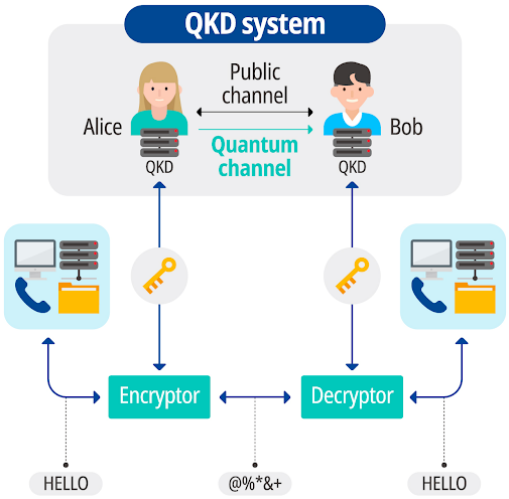

Figure 9. Quantum image encryption process: synthesized from the inputs in [63]

A framework for the chaos-based quantum encryption of healthcare images that guarantees patient safety and anonymity was presented in an article by Abd El-Latif et al. [61]. Medical professionals can securely help patients by decrypting their image content. Quantum grey code is used to disentangle the quantum image, and a quantum XOR operation based on a key generator managed by the logistic-sine map is used to encrypt it. When compared to its classical counterpart, the suggested encryption method is very efficient, attainable, and resilient. Janani et al. [62] also proposed a new technique based on quantum image representation and chaotic maps to secure medical images. More articles are using quantum-based image encryption which has to be extended to medical images to handle the security the security of healthcare in the quantum era. Drawbacks of quantum-based medical image encryption include the current limitations in scalability and practical implementation due to the complexity and cost of quantum technologies, the susceptibility to decoherence and noise, and the need for specialized expertise in quantum mechanics and cryptography for effective deployment. Additionally, the lack of mature quantum computing infrastructure and standards poses challenges for widespread adoption in healthcare settings. The performance metrics to assess the image encryption scheme are discussed in the following section which would help us to compare the proposed solutions.

3.3 *Performance measures of image encryption techniques*

There are a lot of performance metrics available to measure the security and quality of the encrypted images as shown in Figure 10. For the Image quality analyses Peak Signal to Noise Ratio (PSNR), Mean Squared Error (MSE), Mean Absolute Error (MAE), and Structural Similarity Index (SSIM) are used. For the security analysis, there are several analyses, including differential analysis which has NPCR, UACI, key space analysis, statistical Analysis which includes histogram attack analysis, and correlation analysis in all directions available [21]. Table 4 lists the formulae used to measure the metrics. Table 5 compares the metrics of some of the discussed articles in section 3.

Empirical data found in Table 5 provides an avenue for a direct comparison of articles due to each article employing standard benchmark datasets (i.e., images of Lena and Baboon) that are typically used in the area of image encryption. Since all papers used the same reference images to arrive at Number of Pixel Change Rate (NPCR), Unified Average Changing Intensity (UACI) and Correlation, resulting scores assess performance values of each proposed cryptographic algorithm under the same testing parameters.

In Table 4, x, y are coordinates to denote the pixel position in the image. *Org* refers original image. *Enc* refers to an encrypted image. Wt, Ht are the width and height of the image. $P(Im_i)$ denotes the probability of i^{th} pixel value of image Im. n is the number of bits used to represent the pixel value. If it is a gray scale image then $n = 8$.

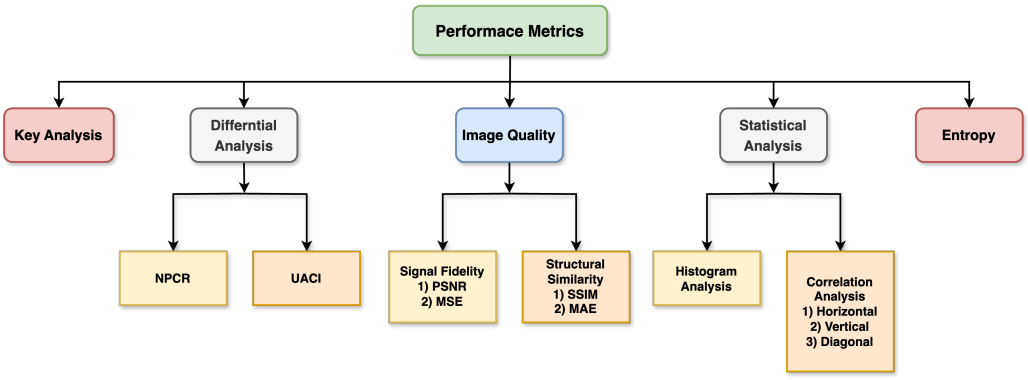

Figure 10. Performance metrics for image encryption models

Table 4. Image encryption performance metrics

Metric	Description	Formulae
Number of Pixel Change Rate (NPCR)	Determines the rate of change that occurs between the pixels of the original image and the encrypted image	$NPCR = \frac{\sum_{x,y} Diff(x,y)}{Wt*Ht} * 100$, Where $Diff(x,y) = 0$ if pixel values are same or 1.
Unified Average Changing Intensity (UACI)	Calculates the average percentage of variation between the encrypted image and the original image	$NPCR = \frac{\sum_{x,y} Org(x,y) - Enc(x,y)}{255*Wt*Ht} * 100$
Mean Squared Error (MSE)	Facilitates the comparison of an image's "true" pixel values with its decrypted counterpart. The difference between an original image's values and the decrypted image's is known as the error	$MSE = \frac{1}{Wt*Ht} \sum_{x=1}^{Wt} \sum_{y=1}^{Ht} \lvert Org(x,y) - Enc(x,y) \rvert^2$
Peak Signal to Noise Ratio (PSNR)	Used as a quality measurement between the original and decrypted images	$PSNR = 10\log_{10} \frac{(2^n-1)^2}{MSE}$
Mean Absolute Error (MAE)	Quantifies the variation between original and encrypted images	$MAE = \frac{1}{Wt*Ht} \sum_{x=1}^{Wt} \sum_{y=1}^{Ht} \lvert Org(x,y) - Enc(x,y) \rvert$
Information Entropy (IE)	Evaluate an image's average bit-by-bit information. It includes all information that could possibly be found in the provided image	$EI = -\sum_i P(Im_i) * \log_2 P(Im_i)$

Table 5. Comparative analysis of performance metrics

Year	Article	H_Corr	V_Corr	D_Corr	NPCR	UACI	IE
2017	Abd El-Latif et al. [61]	−0.0020	−0.0095	−0.0015	99.6643	28.9754	7.9878
2018	Hua et al. [29]	-	-	-	99.9974	33.2716	-
2019	Moafimadani et al. [30]	-	-	-	99.5971	33.4755	7.9997
2021	Janani et al. [62]	−0.0045	0.0103	0.0011	99.7172	33.4570	-
2021	Balasamy et al. [33]	0.5496	0.5554	0.5126	99.4100	33.5400	-
2021	Khare et al. [34]	-	-	-	99.9900	32.9500	-
2022	Kiran et al. [45]	0.5421	0.5361	0.5078	99.9820	33.1200	7.9900
2022	Ping et al. [42]	0.0032	0.0052	−0.0021	99.6121	33.4554	7.9971
2022	Meng et al. [44]	-0.0080	0.0010	−0.0074	99.9938	33.1994	7.9993
2022	Zhang et al. [48]	0.0066	−0.0049	0.0158	99.6476	33.4359	7.9995
2022	Yousif et al. [35]	−0.0215	−0.0113	0.0089	99.6100	33.7053	7.9993
2022	Elkandoz et al. [47]	0.0014	0.0079	−0.0015	99.6246	30.5681	7.9970
2023	Wang et al. [46]	0.0015	0.0011	0.0015	99.6143	33.4681	7.9994
2023	Amaithi Rajan et al. [37]	−0.0011	−0.0154	−0.0682	99.6100	33.3900	7.9971

4. Secure medical image retrieval

Medical image retrieval is essential for effective diagnosis, treatment, and research in the healthcare field. Robust systems that guarantee image retrieval and the confidentiality of sensitive patient data are imperative due to the exponential rise of security threats on medical imaging data [18]. There exist few surveys that discuss image retrieval from different perspectives. Kumar et al. [13] projected and discussed it with multidimensional and multimodality data in the medical field. Furthermore, Li et al. [66] discussed more feature engineering techniques, indexing methods, and various applications with datasets in medical image retrieval. The architecture illustrated in Figure 2 is synthesized from several representative frameworks proposed in the literature, including secure storage architectures based on encryption and indexing mechanisms described in [67–69]. These works collectively demonstrate how medical images can be securely stored in cloud environments while enabling privacy-preserving retrieval.

With digital health records and imaging modalities on the rise, secure medical image retrieval becomes paramount to safeguard patient confidentiality and prevent unauthorized access. Encryption techniques, access controls, and secure communication protocols are integrated into retrieval systems to protect data integrity and privacy. The emergence of cloud-based storage and telemedicine platforms further emphasizes the need for secure retrieval, enabling remote access while meeting regulatory standards [70]. Integrating encryption, authentication, and audit trails enhances security and fosters trust among healthcare providers and patients. As medical imaging's role expands, secure retrieval mechanisms ensure patient data protection, facilitating seamless access to critical information while upholding privacy and security standards in the digital healthcare landscape [71]. Figure 11 illustrates the general design of a secure medical image retrieval system. Figure 11 summarizes the typical architecture of secure medical image management systems derived from the surveyed literature, integrating secure storage mechanisms discussed in Section 3 and privacy-preserving retrieval techniques reviewed in Section 4.

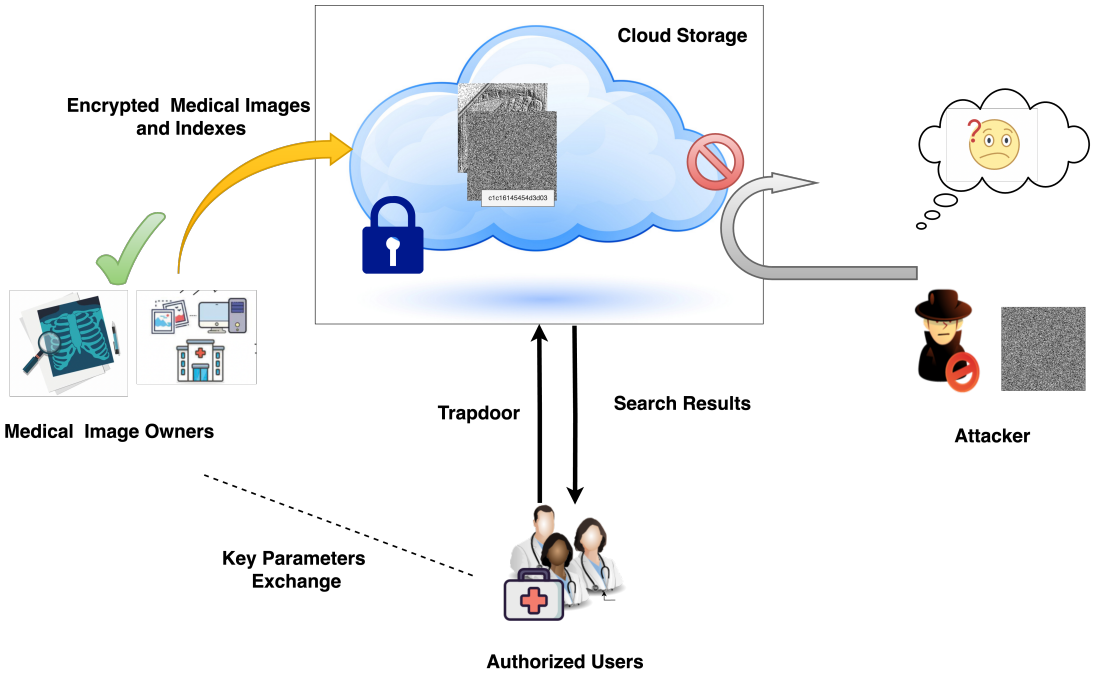

Figure 11. Secure medical image retrieval model in the cloud

The retrieval system must be constructed to ensure that only authorized users can query the cloud. While this access control measure helps mitigate attacks in the cloud, encrypting stored images is also essential for enhanced security. However, encryption can complicate the search process, necessitating the development of efficient indexing mechanisms [72]. Very recently, Ajitesh et al. [73] presented an attack-resistant privacy-enhanced image retrieval scheme called EdgeShield in the distributed environment for remote sensing images in military applications using edge computing. This kind of system can be extended to healthcare as it is also handling sensitive medical images [74]. Various medical image retrieval mechanisms exist, with some prioritizing security while others emphasize retrieval accuracy. In this survey, we categorize medical image retrieval models based on their indexing methods: Deep Hashing, Encrypted Indexing, and Multimodal-based indexing as illustrated in Figure 12.

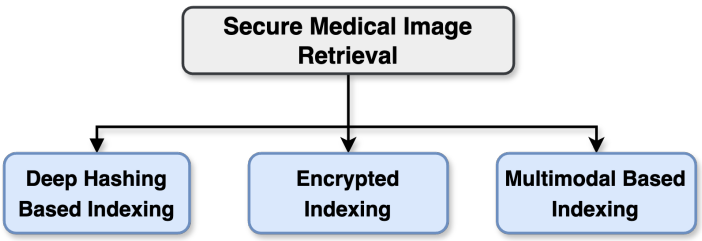

Figure 12. Secure medical image retrieval categories

4.1 *Deep hashing-based techniques*

In the realm of medical image analysis, deep hashing of images is a strategy that uses deep learning techniques to produce compact and discriminative binary codes for effective image retrieval and similarity search tasks. By harnessing the power of deep neural networks, deep hashing methods learn hierarchical representations of medical images that capture both global semantics and fine-grained features, thereby enabling the generation of hash codes that preserve meaningful information while reducing storage and computational requirements [75]. In the context of medical imaging, deep hashing techniques offer the potential to revolutionize content-based image retrieval, disease diagnosis, and treatment planning by facilitating rapid and accurate retrieval of relevant medical images from large-scale repositories. Through the integration of advanced Convolutional Neural Networks (CNNs), attention mechanisms, and optimization algorithms, deep hashing algorithms strive to address the unique issues posed by medical image data, including variability in imaging modalities, anatomical structures, and pathological conditions, thus laying the foundation for more effective and intelligent medical image analysis systems [22]. Figure 13 shows the general structure of deep hashing model.

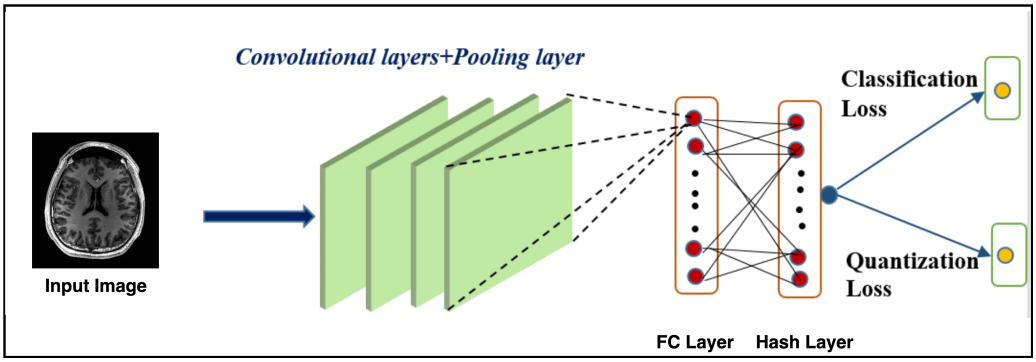

Figure 13. Basic deep hashing flow synthesized from representative works in the literature [22]

In 2021, Ozturk et al. [76] proposed a retrieval framework for medical images using deep features obtained from a CNN architecture. The goal is to produce effective and discriminant hash codes for MRI and CT image indexing and searching. Following that, To increase the retrieval accuracy of medical image retrieval, Guan et al. [77] introduced a precision medical image hash retrieval method that combines interpretability and feature fusion. To produce high-quality hash codes for retrieval, the approach uses a pre-trained DenseNet-121 network, interpretable saliency maps, and a variety of loss functions.

There exist different hashing models that focus more on advanced networks [78], explainability [79], and Federated Learning (FL) concepts [80] which help the domain to improve in different directions. Medical image deep hashing has some drawbacks: the need for large labeled datasets, high computational requirements for hashing training, overfitting risks, and limited interpretability, which might hinder its clinical relevancy and trustworthiness.

4.2 *Encrypted indexing*

Encrypted index generation for medical images involves the application of advanced cryptographic techniques such as Homomorphic Encryption (HE), secure Multiparty Computation (MPC), and Searchable Symmetric Encryption (SSE) to facilitate secure and privacy-preserving indexing of sensitive medical images. Encrypted indices can be computed on encrypted data without the need for decryption, ensuring confidentiality while enabling efficient search operations by leveraging HE [81]. While maintaining the privacy of individual datasets, secure MPC protocols manage many participants to collaborate on the computation of encrypted indices [71]. Moreover, SSE techniques enable the generation of encrypted indices that support keyword-based search queries over encrypted medical image metadata [82]. These methods focus on the need for protecting patient privacy and confidentiality while enabling efficient and secure retrieval of medical images in healthcare systems.

Kumar et al. [83] introduced a new technique with invariant feature selection of images and applying asymmetric scalar-product-preserving encryption over them to simplify the similarity search. Shen et al. [71] utilized the MPC to protect the privacy of medical images. Blockchain technology is also leveraged to store the encrypted indices which give double-layer protection [84]. Secure k-Nearest Neighbors (k-NN) is another approach to performing k-NN classification or regression while preserving the privacy and security of the data involved in the process. This secure k-NN has been combined with locality-sensitive hashing by Xia et al. [85]. Whereas, Chen et al. [72] extended it by applying the algorithm to ROIs which are selected by YOLOv5. Challenges of encrypted index generation for medical images cover increased computational overhead due to encryption and decryption processes, heavily impacting system performance and the difficulty of maintaining cryptographic keys and access control.

4.3 *Multimodal-based indexing*

Multimodal-based index generation for medical images, including imaging modalities like CT, MRI, and X-rays, represents a futuristic approach to improving medical image retrieval through the use of deep hashing techniques [86]. By integrating information from diverse imaging modalities, this technique aims to generate comprehensive representations of medical images that help efficient retrieval and analysis across modalities, including cross-modal retrieval tasks. Kitanovski et al. [86] did an elaborate survey on what are all the modalities available in healthcare and how they can be processed for image retrieval.

Multi-manifold Deep Discriminative Cross-modal Hashing (MDDCH) is a unique hashing technique that was presented by Xu et al. [87] in 2022 for large-scale medical image retrieval. It tackles the issues of weak discriminability of hash codes and weak multi-manifold structure preservation across many modalities. In order to maintain a correlation between instances, MDDCH combines several sub-manifolds defined on heterogeneous data. Additionally, it guarantees that every hash code encoded by hash functions is unique, enhancing the hash code's discriminative performance. Wang et al. [88] introduced MedCLIP, a framework for contrastive language-image pretraining that decouples medical images and texts, allowing for scalable training data and improved representation transferability.

More recently in 2024, In order to overcome the drawbacks of the current deep hashing-based techniques and enhance retrieval performance, Li et al. [89] presented a CLIP-based Knowledge Distillation Hashing (CKDH) method for cross-modal retrieval. CKDH introduces a complete similarity measurement for improved training supervision, and it makes use of CLIP for visual feature extraction and a graph attention network for textual feature enhancement. Experimental results prove that CKDH surpasses existing state-of-the-art methods consistently. The difficulties associated with multimodal medical image hashing include the semantic gap between low-level features and clinical semantics, feature fusion complexity, and modality heterogeneity. Ensuring robustness to variability, scalability, and efficiency, while preserving clinical relevance and retrieval accuracy, remains crucial.

4.4 *Comparative analysis*

Maintaining security and improving retrieval accuracy are the primary objectives of secure medical image retrieval. The most important criteria for evaluating image retrieval performance are mean Average Precision (mAP) and retrieval time. The definition of the mAP is as follows.

$$mAP = \frac{1}{Q}\sum_{q=1}^{Q} AP(q)$$

where $AP(q)$ is the average precision (AP) for a particular query, q, and Q is the number of queries in the set. The comparative comparison of the secure CBIR approaches is presented in Table 6. This comparison differentiates the techniques based on the focus (Sec, Perf) of the proposed method and the method it uses (DH, En, MM). DH means deep hashing, En means encrypted indexing, and MM means multimodal indexing. More techniques are performance-concerned where they have shown less priority in security [89, 90]. Few techniques are security-focused which has robust security but less performance [84, 85, 91]. The major goal is to strike the balance between security and performance [72]. However, these schemes can be utilized based on the requirements in the healthcare.

Table 6. Comparative analysis of secure medical image retrieval

Year	Article	Focus		Category				Technique
		Sec	Per	DH	En	MM	Other	
2017	Xia et al. [85]	✓			✓			Locality Sensitive Hashing and Secure KNN
2019	Shen et al. [84]	✓		✓			Encrypted Index in Blockchain	
2019	Aggarwal et al. [92]		✓				✓	Orthogonal Fourier-Mellin Moments method indexing
2020	Shen et al. [71]	✓			✓			Secure MPC
2021	Kumar et al. [83]	✓			✓			Asymmetric scalar-product-preserving encryption and invariant feature selection
2021	Janani et al. [91]	✓			✓			HSV Feature and ROI-based Hash Verification
2021	Bhanu Mahesh et al. [75]		✓	✓				Optimized CNN
2021	Öztürk et al. [76]		✓	✓				Class-driven hashcodes with ResNet-50
2022	Guan et al. [77]		✓	✓				Feature Fusion with DenseNet-121
2022	Sunitha et al. [93]		✓				✓	SURF Features with BoVW
2022	Duan et al. [17]	✓					✓	Light Polynomial-based Access Control
2022	Xu et al. [87]		✓	✓		✓		Discriminative Cross-Modal Hashing
2022	Wang et al. [88]		✓			✓		CLIP Model
2023	Gupta et al. [94]		✓				✓	Efficient Graph-based Index Generation
2023	Zhu et al. [95]	✓			✓			Mahalanobis Distance and Fuzzy-C-Means
2023	Tabatabaei et al. [80]		✓	✓				FL based retrieval
2023	Özbay et al. [90]		✓	✓				Feature Fusion with DenseNet-201
2023	Hu et al. [79]		✓	✓				DenseNet-121 and Explainability in Retrieval
2023	Chen et al. [72]	✓	✓	✓	✓			YOLOv5, CNN, S-kNN based retrieval
2024	Amaithi Rajan et al. [67]	✓		✓	✓			ConvNeXt based similarity-preserving hashing and Invariant Linear Transformation-based Secure Indexing
2024	Li et al. [89]		✓	✓		✓		Knowledge Distillation Hashing with CLIP
2025	Amaithi Rajan et al. [69]		✓				✓	FL based hashing with distributed encrypted image storage and retrieval

Customising a mixed storage and retrieval architecture based upon the unique business objectives associated with a specific health care organisation, while effectively addressing the current utility vs security conundrum, should dictate the most effective solution for the implementation of a mixed storage/retrieval architecture. A mixed use of chaotic maps integrated with Deep Hashing is the most viable solution for teleradiology and emergency diagnostics, as it allows for a rapid scramble of data with a quick binary code similarity search thus providing for low latency of critical diagnostic information access. For medical research and large scale clinical trial studies, DNA Cryptography integrated with Multi-Modal Indexing provides the highest density storage capabilities thus allowing for the use of space-efficient encryption methods to effectively manage a massive repository of records combined with the ability to use cross-modal frameworks to bridge the semantic gap that exists when comparing different imaging modalities (such as CT vs MRI). In contrast, long-term clinical archives require the use of a mixed storage/retrieval architecture that provides for the retention of the most secure and private records possible through the use of Blockchain storage integrated with Encrypted Indexing (by using HE or MPC). Integrating these approaches will provide for the best possible tamper-resistant audit trail and assured data confidentiality for the long-term, while securing long-term data at the expense of immediate computational performance.

5. Technical discussion

This section is dedicated to discuss the secure storage and retrieval architectures analysed so far. The comparison presented in Table 7 highlights the diverse trade-offs among different technique classes used for secure medical image storage and retrieval. Classical methods for encryption based on chaos have a low level of computational expense and are fairly common in academic research; however, they have not yet reached their full level of deployment maturity or compliance with established regulations. On the other hand, blockchain technology has been shown to provide significant protection from data manipulation and high levels of preemptive protection from internal security breaches and to offer the ability to conduct audits and trace data, all of which are necessary for proper regulatory compliance within the healthcare system. New and developing technologies, such as DNA-based encryption and quantum cryptography—can reach higher theoretical levels of security than classical methods; however, they require substantial amounts of computational resources and are yet experimental in nature, limiting their use in the clinical setting at this time. For retrieval of data, deep hash techniques provide efficient searching capabilities at around mid-level security; conversely, cryptographic methods such as Searchable Symmetric Encryption (SSE) and secure Multi-Party Computation (MPC) provide substantially more privacy than their mid-level counterparts when executing queries against encrypted data, albeit with considerably higher computational resource requirements. Hybrid systems that achieve a compromise in security, scalability and retrieval performance through the combination of efficient indexing technologies and strong cryptographic protections may provide the best solution for future healthcare systems in terms of security and retrieval performance through the use of multiple modalities to enhance the diagnostic relevance of the resulting information retrieved while simultaneously providing additional challenges related to data fusion privacy.

From the evaluation perspective, Table 8 categorizes the evaluation metrics commonly used in secure medical image storage and retrieval systems into four major groups: cryptographic security metrics, retrieval performance metrics, system performance metrics, and storage and infrastructure metrics.The statistical and brute force attacks against the strengths of encryption algorithms used to secure the confidentiality of sensitive medical images can be quantified by several different types of metrics. These metrics include the cryptographic metrics of NPCR, UACI, entropy, and key space; retrieval performance metrics of precision, recall, mAP, and F1-score; system-level performance metrics of latency, throughput, and response time; and storage/infrastructure performance metrics of storage overhead and computational complexity. These metrics form a comprehensive evaluation for both security and practical performance of secure medical image management systems. Each metric provides a unique perspective toward quantifying the efficacy of secure medical image management systems.

Table 7. Comparative analysis of major technique classes for secure medical image storage and retrieval

Technique class	Threat model	Security level	Comp. cost	Impl. maturity	Regulatory compatibility
Chaos-based Encryption	External attackers, statistical attacks	Medium–High	Low	Research prototypes widely explored in academia	Moderate
Blockchain-based Systems	Data tampering, insider attacks	High	Medium–High	Emerging healthcare deployments	High (supports traceability)
DNA-based Encryption	Cryptanalytic attacks	High	High	Mostly experimental	Low–Moderate
Quantum Cryptography	Advanced computational adversaries	Very High	Very High	Early-stage research	Uncertain
Deep Hashing Retrieval	Feature leakage, inference attacks	Medium	Medium	Mature in CBMIR research	High
Searchable Symmetric Encryption (SSE)	Honest-but-curious cloud provider	High	Medium	Increasing industry adoption	High
Secure Multi-Party Computation (MPC)	Multi-party privacy threats	Very High	High	Limited deployments	High
Multimodal Retrieval	Data fusion leakage	Medium	Medium	Growing research adoption	Moderate

Table 8. Comparison of evaluation metrics in secure medical image storage and retrieval systems

Metric category	Metrics	Purpose	Application relevance
Cryptographic Security Metrics	NPCR, UACI, Entropy, Key Space	Measure encryption strength and resistance to statistical and brute-force attacks	Critical for protecting patient privacy and ensuring secure storage of medical images
Retrieval Performance Metrics	Precision, Recall, Mean Average Precision (mAP), F1-score	Evaluate the accuracy and effectiveness of medical image retrieval algorithms	Important for clinical decision support and medical research databases
System Performance Metrics	Latency, Throughput, Response Time	Measure system efficiency and responsiveness in real-time environments	Critical for time-sensitive applications such as emergency diagnosis and teleradiology
Storage & Infrastructure Metrics	Storage Overhead, Computational Complexity	Evaluate storage requirements and computational resource consumption	Important for large-scale hospital archives and cloud-based healthcare infrastructures

6. Clinical integration and deployment consideration

The literature evaluated shows that the articles are secure in their operation, have efficient ways of retrieving data, and can withstand attacks from their adversaries. For them to be adopted into practice, however, clinical workflow and the integrated nature of Health Information Technology (HIT) across organizations must be carefully considered. To accomplish this, facilities must comply with and integrate into their existing Picture Archiving and Communication Systems (PACS) as well as comply with DICOM (Digital Imaging and Communications in Medicine) standards governing metadata schema, formats for images, and methods of transmitting data [96].

To ensure compatibility with Radiology Information Systems (RIS) and Electronic Health Records (EHR), the encrypted Hash Codes and Secure Indexes that result from using our proposed models would need to be encapsulated in DICOM-compatible tags and linked through the Fast Healthcare Interoperability Resources (FHIR) Application Programming Interface (API) [97]. In addition, if deployed in the cloud using services such as Google Cloud Medical Imaging Suite or Amazon Web Services (AWS) HealthLake Imaging, they would also require HIPAA/GDPR compliant storage, Key Management System (KMS) through Cloud Native Hardware Security Module (HSM) and strict access controls based upon clinical roles. The methods can be integrated as a Back-End Service(s) that can interface with PACS via DICOMweb, allowing Encrypted Domain Search without disrupting existing workflows. Federated and fault-

tolerant systems are highly compatible with Multi-Hospital collaborations, but real-world implementations need to plan for Asynchronous Nodes, Different Bandwidths, and Institutional Data Governance Policy.

Quantum-based encryption and retrieval rely on both state-of-the-art computer technologies and physical sciences that use quantum information to be implemented and used in real-life applications, i.e., hospitals or doctor's offices. Until recently, research had encompassed theoretical quantum cryptography; however, practical implementations of quantum encryption remain constrained due to numerous technical and economic factors, including the cost, complexity, size, ability of quantum hardware and susceptibility of quantum systems to decoherence and noise. As such, even though quantum cryptography has the potential to be unconditionally secure, the high costs and complexity of quantum hardware and lack of quantum infrastructure indicate that widespread clinical adoption of quantum-based solutions is unlikely for the next several years. With further development of proper standards for quantum-based technology and the introduction of more accessible quantum computing environments, quantum-based methods will remain mostly in their experimental stages, with the timeline for realistic clinical implementation left to the implementation of global standards and greater availability of quantum computers. The next critical step in translating this research into deployable healthcare solutions is validating the clinical use cases, including Radiologist User-Centered Studies, Workflow Impact Analysis and Interpretability Assessment.

Table 9 presents practical deployment guidelines for selecting appropriate techniques in secure medical image storage and retrieval systems across different healthcare scenarios. Lightweight solutions, such as AES encryption and deep hashing, balance security with an easy way to implement them in a small hospital. Whereas, larger healthcare providers, who use the cloud, can benefit from using scalable methods like SSE and encrypted indexing, to enable efficient searching of their encrypted medical records, similarly to collaborative medical research databases, where the use of privacy-preserving methods such as MPC can support the joint analysis of data while keeping patient data confidential. In a long-term medical database, strong encrypted storage will have to be used along with blockchain based data verification systems to maintain integrity, authenticity and traceability for a long time. Lastly, lightweight encryption and deep feature indexing can be used in support of time sensitive applications, such as teleradiology services, as they allow for low latency retrieval of data, enabling remote clinical diagnosis.

Table 9. Practical deployment guidelines for secure medical image storage and retrieval systems

Deployment scenario	Recommended techniques	Advantages
Small hospital system	AES-based encryption + deep hashing retrieval	Low implementation complexity and fast retrieval
Large cloud healthcare provider	Searchable Symmetric Encryption (SSE) + encrypted indexing	Scalable and secure cloud search
Medical research repositories	Secure Multi-Party Computation + privacy-preserving retrieval	Enables collaborative data analysis while preserving privacy
Long-term medical archives	Blockchain-based integrity verification + strong encryption	High data integrity, traceability, and auditability
Teleradiology services	Lightweight encryption + deep feature indexing	Low latency retrieval suitable for remote diagnosis

7. Open issues and future work

In the digital era, especially in healthcare secure medical image storage and retrieval are the prevalent operations in medical professional's day-to-day life. As medical images contain sensitive information, privacy and security of the data are more concern. More research works are being done in this area. We have also discussed more of the techniques proposed in the domain. Yet, there are more challenges and open issues that exist in the domain which has to be addressed in the future. The major challenge is maintaining the balance between security and retrieval performance.

In secure medical image storage, more quantum-based secure schemes are anticipated as we move towards the quantum era. More encryption algorithms are required with a focus on handling medical images as they have more intrinsic features than other images. Recent GenAI techniques can be brought in to generate more precise medical images from the

existing medical images which might resolve the data scarcity issue while training. Homomorphic-enabled DNA encoding could be introduced to achieve both searchability and efficient spacing in a single solution. Encryption techniques with access control capabilities could be useful in the medical field.

In secure medical image retrieval, robust adversarial training could be introduced in the deep hashing network to prevent adversarial attacks on the model. Quantum-based hashing is also a major challenge in the future. More modalities could be brought into the hashcode generation of image retrieval which could improve the retrieval accuracy. Enhanced encrypted indexing is on demand which improves the retrieval time and retrieval accuracy. Secure medical image retrieval as a service could be introduced as a potential service. Confidential computation requires encryption for cloud-side computations.

8. Summary and conclusion

Secure medical image storage and retrieval is the major focus in digital healthcare which relies on third-party cloud. This survey has addressed the fundamental research question of how to jointly optimize robust data security and high retrieval efficiency within cloud-based medical image management systems. This paper discusses the issues of secure storage and retrieval of medical images in digital healthcare. It explores techniques like classical and quantum encryption with chaotic maps, DNA cryptography, and blockchain for secure storage. In secure medical image retrieval, indexing for efficient search capabilities covers deep hashing, encrypted indexing, and multimodal-based indexing are discussed. Our study provides a comprehensive analysis of existing approaches, including their strengths, limitations, performance comparisons, and applicability insights. The paper also discusses challenges and future research directions to ensure secure and efficient medical image management. The major objective of secure medical image retrieval is to maintain both security and better retrieval accuracy. For practical deployments, hybrid approaches combining strong encryption techniques with efficient deep feature indexing appear to provide the most promising balance between security, scalability, and retrieval performance. For researchers, it is imperative to move past silod optimizations towards investigating the potential of homomorphic-enabled DNA encoding for simultaneous searching and efficiency, as well as quantum-resistant hashing to create a durable infrastructure for healthcare. Figure 14 summarizes the survey.

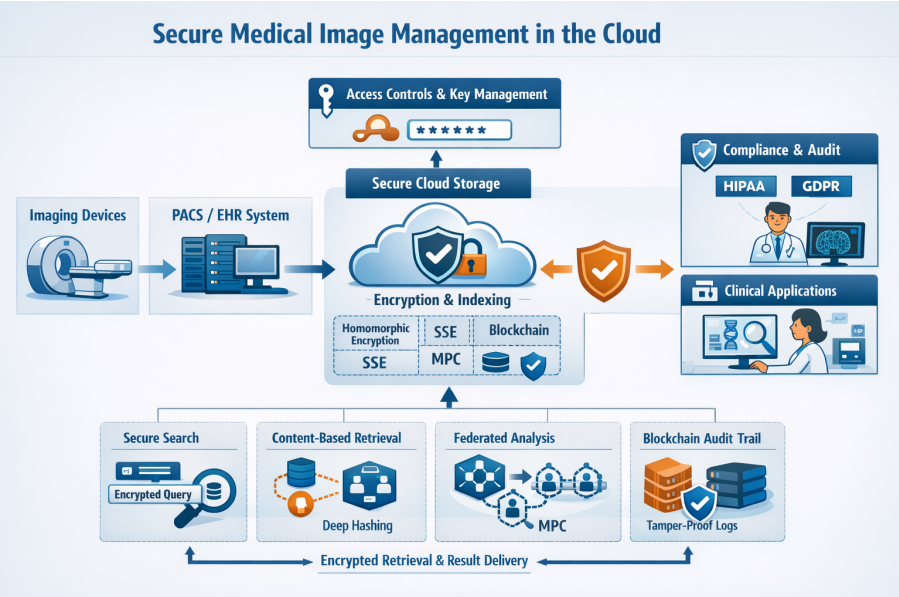

Figure 14. Summary of the survey

Author contributions

Conceptualization: A.A.R. and V.V; methodology and development: A.A.R. and V.V; formal analysis and investigation: A.A.R. and V.V; writing—original draft preparation: A.A.R. and V.V; writing—review, and editing: A.A.R. and V.V; supervision: V.V.

Confilict of interest

The authors declare no competing financial interest.

References

[1] T. Schweiger, "The digital image-history, use in social media, and its power to influence," 2019. [online]. Available: https://tinaschweiger.medium.com/the-digital-image-history-use-in-social-media-and-its-power-to-influence-249a2e0d0d1c. [Accessed Mar. 11, 2024].

[2] W. H. L. Pinaya, P. D. Tudosiu, R. Gray, G. Rees, P. Nachev, S. Ourselin, et al., "Unsupervised brain imaging 3d anomaly detection and segmentation with transformers," *Medical Image Analysis*, vol. 79, p. 102475, 2022. https://doi.org/10.1016/j.media.2022.102475.

[3] J. H. Moon, H. Lee, W. Shin, Y.-H. Kim, and E. Choi, "Multi-modal understanding and generation for medical images and text via vision-language pre-training," *IEEE Journal of Biomedical and Health Informatics*, vol. 26, no. 12, pp. 6070-6080, 2021. https://doi.org/10.1109/JBHI.2022.3207502.

[4] F. Mercaldo, L. Brunese, F. Martinelli, A. Santone, and M. Cesarelli, "Object detection for brain cancer detection and localization," *Applied Sciences*, vol. 13, no. 16, p. 9158, 2023. https://doi.org/10.3390/app13169158.

[5] G. Litjens, T. Kooi, B. E. Bejnordi, A. A. A. Setio, F. Ciompi, M. Ghafoorian, J. A. W. M. van der Laak, B. van Ginneken, and C. I. Sánchez, "A survey on deep learning in medical image analysis," *Medical Image Analysis*, vol. 42, pp. 60-88, 2017. https://doi.org/10.1016/j.media.2017.07.005.

[6] C. Xiong, X. Xu, H. Zhang, and B. Zeng, "An analysis of clinical values of mri, ct and x-ray in differentiating benign and malignant bone metastases," *American Journal of Translational Research*, vol. 13, no. 6, pp. 7335-7341, 2021.

[7] A. Anitha and S. Balaji, "A survey on genetic disorder prediction of fetus from ultrasound-based computer-aided diagnosis," In Proc. 2022 6th International Conference on Electronics, Communication and Aerospace Technology, Coimbatore, India, Dec. 1-3, 2022, pp. 575-583. https://doi.org/10.1109/ICECA55336.2022.10009264.

[8] H. P. Sigurdsson, L. Alcock, M. Firbank, R. Wilson, P. Brown, R. Maxwell, et al., "Developing a novel dual-injection fdg-pet imaging methodology to study the functional neuroanatomy of gait," *NeuroImage*, vol. 288, p. 120531, 2024. https://doi.org/10.1016/j.neuroimage.2024.120531.

[9] M. Larobina and L. Murino, "Medical image file formats," *Journal of Digital Imaging*, vol. 27, no. 2, pp. 200-206, 2014. https://doi.org/10.1007/s10278-013-9657-9.

[10] S. Ebadinezhad and T. E. Mobolade, "A novel cloud-based iot framework for secure health monitoring," *Sustainability*, vol. 16, no. 3, p. 1349, 2024. https://doi.org/10.3390/su16031349.

[11] D. Lakshmi and A. K. Tyagi, "Emerging technologies and security in cloud computing," in *Advances in Information Security, Privacy, and Ethics*, IGI Global, 2024. https://doi.org/10.4018/979-8-3693-2081-5.

[12] A. Amaithi Rajan and V. V., "Systematic survey: Secure and privacy-preserving big data analytics in cloud," *Journal of Computer Information Systems*, vol. 61, no. 1, pp. 136-156, 2023. https://doi.org/10.1080/08874417.2023.2176946.

[13] A. Kumar, J. Kim, W. Cai, M. Fulham, and D. Feng, "Content-based medical image retrieval: A survey of applications to multidimensional and multimodality data," *Journal of Digital Imaging*, vol. 26, no. 6, pp. 1025-1039, 2013. https://doi.org/10.1007/s10278-013-9619-2.

[14] A. Safaei, "Text-based multi-dimensional medical images retrieval according to the features-usage correlation," *Medical & Biological Engineering & Computing*, vol. 59, pp. 1993-2017, 2021. https://doi.org/10.1007/s11517-021-02392-0.

[15] V. S. Mahalle, N. M. Kandoi, and S. B. Patil, "A powerful method for interactive content-based image retrieval by variable compressed convolutional info neural networks," *The Visual Computer*, vol. 40, pp. 5259-5285, 2023. https://doi.org/10.1007/s00371-023-03104-5.

[16] J.-S. Li, I.-H. Liu, C.-J. Tsai, Z.-Y. Su, C.-F. Li, and C.-G. Liu, "Secure content-based image retrieval in the cloud with key confidentiality," *IEEE Access*, vol. 8, pp. 114940-114952, 2020. https://doi.org/10.1109/ACCESS.2020.3003928.

[17] Y. Duan, Y. Li, L. Lu, and Y. Ding, "A faster outsourced medical image retrieval scheme with privacy preservation," *Journal of Systems Architecture*, vol. 122, p. 102356, 2022. https://doi.org/10.1016/j.sysarc.2021.102356.

[18] S. Kumar, S. K. Agarwal, and S. S. Ahmad, "A secure medical image retrieval technique using encrypted query image," In Proc. 2022 2nd International Conference on Emerging Frontiers in Electrical and Electronic Technologies (ICEFEET), Patna, India, Jun. 24-25, 2022. https://doi.org/10.1109/ICEFEET51821.2022.9847826.

[19] U. Zia, M. McCartney, B. Scotney, J. Martinez, M. AbuTair, J. Memon, and A. Sajjad, "Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains," *International Journal of Information Security*, vol. 21, no. 4, pp. 917-935, 2022. https://doi.org/10.1007/s10207-022-00588-5.

[20] Priyanka and A. K. Singh, "A survey of image encryption for healthcare applications," *Evolutionary Intelligence*, vol. 16, pp. 801-818, 2022. https://doi.org/10.1007/s12065-021-00683-x.

[21] M. Kaur and V. Kumar, "A comprehensive review on image encryption techniques," *Archives of Computational Methods in Engineering*, vol. 27, no. 1, pp. 15-43, 2020. https://doi.org/10.1007/s11831-018-9298-8.

[22] X. Luo, H. Wang, D. Wu, C. Chen, M. Deng, J. Huang, and X.-S. Hua, "A survey on deep hashing methods," *ACM Transactions on Knowledge Discovery from Data*, vol. 17, no. 1, pp. 1-50, 2023. https://doi.org/10.1145/3532624.

[23] A. Amaithi Rajan and V. V., "Privacy or performance? towards secure and scalable medical image storage and retrieval management in the cloud," In Proc. 18th Innovations in Software Engineering Conference, Kurukshetra, India, Feb. 20-22, 2025, pp. 1-4. https://doi.org/10.1145/3717383.3717398.

[24] H. Snyder, "Literature review as a research methodology: An overview and guidelines," *Journal of Business Research*, vol. 104, pp. 333-339, 2019. https://doi.org/10.1016/j.jbusres.2019.07.039.

[25] Y. Liu, X. Qu, and G. Xin, "A roi-based reversible data hiding scheme in encrypted medical images," *Journal of Visual Communication and Image Representation*, vol. 39, pp. 51-57, 2016. https://doi.org/10.1016/j.jvcir.2016.05.008.

[26] M. Magdy, K. M. Hosny, N. I. Ghali, and S. Ghoniemy, "Security of medical images for telemedicine: a systematic review," *Multimedia Tools and Applications*, vol. 81, no. 18, pp. 25101-25145, 2022. https://doi.org/10.1007/s11042-022-11956-7.

[27] A. A. Rajan and A. A. Rajan, "Data anonymization techniques for preserving privacy in public release data model: a technical review," *International Journal of Scientific Research in Computer Sciences and Engineering*, vol. 8, no. 1, pp. 58-62, 2020. https://doi.org/10.26438/ijsrcse/v8i1.5862.

[28] O. M. Al-Hazaimeh, M. F. Al-Jamal, N. Alhindawi, and A. Omari, "Image encryption algorithm based on lorenz chaotic map with dynamic secret keys," *Neural Computing and Applications*, vol. 31, no. 7, pp. 2395-2405, 2019. https://doi.org/10.1007/s00521-017-3195-1.

[29] Z. Hua, S. Yi, and Y. Zhou, "Medical image encryption using high-speed scrambling and pixel adaptive diffusion," *Signal Processing*, vol. 144, pp. 134-144, 2018. https://doi.org/10.1016/j.sigpro.2017.10.004.

[30] S. S. Moafimadani, Y. Chen, and C. Tang, "A new algorithm for medical color images encryption using chaotic systems," *Entropy*, vol. 21, no. 6, p. 577, 2019. https://doi.org/10.3390/e21060577.

[31] Y. Lin, Z. Xie, T. Chen, X. Cheng, and H. Wen, "Image privacy protection scheme based on high-quality reconstruction dct compression and nonlinear dynamics," *Expert Systems with Applications*, vol. 257, p. 124891, 2024. https://doi.org/10.1016/j.eswa.2024.124891.

[32] Y. Su, Y. Wo, and G. Han, "Reversible cellular automata image encryption for similarity search," *Signal Processing: Image Communication*, vol. 72, pp. 134-147, 2019. https://doi.org/10.1016/j.image.2018.12.008.

[33] K. Balasamy and S. Suganyadevi, "A fuzzy based roi selection for encryption and watermarking in medical image using dwt and svd," *Multimedia Tools and Applications*, vol. 80, no. 5, pp. 7167-7186, 2021. https://doi.org/10.1007/s11042-020-09981-5.

[34] P. Khare and V. K. Srivastava, "A secured and robust medical image watermarking approach for protecting integrity of medical images," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 2, 2021. https://doi.org/10.1002/ett.3918.

[35] S. F. Yousif, A. J. Abboud, and R. S. Alhumaima, "A new image encryption based on bit replacing, chaos and dna coding techniques," *Multimedia Tools and Applications*, vol. 81, no. 19, pp. 27453-27493, 2022. https://doi.org/10.1007/s11042-022-12762-x.

[36] K. Singh, O. Singh, A. K. Singh, and A. K. Agrawal, "Eimol: A secure medical image encryption algorithm based on optimization and the lorenz system," *ACM Transactions on Multimedia Computing, Communications, and Applications*, vol. 19, no. 2s, pp. 1-19, 2023. https://doi.org/10.1145/3561513.

[37] A. Amaithi Rajan, V. Vetrian, and A. Gladys, "Secure image encryption model for cloud-based healthcare storage using hyperchaos and dna encoding," in *Secure Image Encryption Model for Cloud-Based Healthcare Storage Using Hyperchaos and DNA Encoding*, Springer, Cham, 2023, pp. 89-103. https://doi.org/10.1007/978-3-031-38296-3_8.

[38] M. Li, S. Pan, W. Meng, W. Guoyong, Z. Ji, and L. Wang, "Medical image encryption algorithm based on hyper-chaotic system and dna coding," *Cognitive Computation and Systems*, 2022. https://doi.org/10.1049/ccs2.12070.

[39] I. Ahmad and S. Shin, "Encryption-then-compression system for cloud-based medical image services," In Proc. 2022 International Conference on Information Networking (ICOIN), Jeju-si, Korea, Jan. 12-15, 2022, pp. 30-33. https://doi.org/10.1109/icoin53446.2022.9687214.

[40] Priyanka, N. Baranwal, K. N. Singh, and A. K. Singh, "Yolo-based roi selection for joint encryption and compression of medical images with reconstruction through super-resolution network," *Future Generation Computer Systems*, vol. 150, pp. 1-9, 2024. https://doi.org/10.1016/j.future.2023.08.018.

[41] K. Balasamy, N. Krishnaraj, and K. Vijayalakshmi, "Improving the security of medical image through neuro-fuzzy based roi selection for reliable transmission," *Multimedia Tools and Applications*, vol. 81, no. 10, pp. 14321-14337, 2022. https://doi.org/10.1007/s11042-022-12367-4.

[42] P. Ping, X. Zhang, X. Yang, and Y. A. A. Hashems, "A novel medical image encryption based on cellular automata with roi position embedded," *Multimedia Tools and Applications*, vol. 81, no. 5, pp. 7323–7343, 2022. https://doi.org/10.1007/s11042-021-11799-8.

[43] S. S. Jamal, M. M. Hazzazi, M. F. Khan, Z. Bassfar, A. Aljaedi, and Z. ul Islam, "Region of interest-based medical image encryption technique based on chaotic s-boxes," *Expert Systems with Applications*, vol. 238, p. 122030, 2024. https://doi.org/10.1016/j.eswa.2023.122030.

[44] X. Meng, J. Li, X. Di, Y. Sheng, and D. Jiang, "An encryption algorithm for region of interest in medical dicom based on one-dimensional eλ-cos-cot map," *Entropy*, vol. 24, no. 7, p. 901, 2022. https://doi.org/10.3390/e24070901.

[45] P. Kiran and B. D. Parameshachari, "Resource optimized selective image encryption of medical images using multiple chaotic systems," *Microprocessors and Microsystems*, vol. 91, p. 104546, 2022. https://doi.org/10.1016/j.micpro.2022.104546.

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

[47] M. T. Elkandoz and W. Alexan, "Image encryption based on a combination of multiple chaotic maps," *Multimedia Tools and Applications*, vol. 81, no. 18, pp. 25497-25518, 2022. https://doi.org/10.1007/s11042-022-12595-8.

[48] Y. Zhang, H. Xie, J. Sun, and H. Zhang, "An efficient multi-level encryption scheme for stereoscopic medical images based on coupled chaotic system and otsu threshold segmentation," *Computers in Biology and Medicine*, vol. 146, p. 105542, 2022. https://doi.org/10.1016/j.compbiomed.2022.105542.

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

[50] Z. Xie, W. Xie, X. Cheng, Z. Yuan, W. Cheng, and Y. Lin, "Image privacy protection communication scheme by fibonacci interleaved diffusion and non-degenerate discrete chaos," *Entropy*, vol. 27, no. 8, p. 790, 2025. https://doi.org/10.3390/e27080790.

[51] U. Erkan, F. Toktas, A. Toktas, Q. Lai, S. Zhou, Y. Lin, and S. Gao, "Multi-layer and multi-directional image encryption algorithm based on hyperchaotic 3d xin-she yang map," *Expert Systems with Applications*, vol. 304, p. 130808, 2026. https://doi.org/10.1016/j.eswa.2025.130808.

[52] A. A. Rajan and B. J. Yamuna, "Secure E-Health System using Blockchain Technology in IoT Environment," in *Blockchain Intelligent Systems*, E. G. Julie, Y. H. Robinson, J. V. Nayahi, and T. Vaiyapuri, Eds. Boca Raton: CRC Press, 2024. https://doi.org/10.1201/9781003313441.

[53] V. Vetriselvi, S. Pragatheeswaran, V. Thirunavukkarasu, and A. R. Arun, "Preventing forgeries by securing healthcare data using blockchain technology," *Advances in Intelligent Systems and Computing*, vol. 933, pp. 151-159, 2020. https://doi.org/10.1007/978-981-13-7166-0_15.

[54] B. A. Y. Alqaralleh, T. Vaiyapuri, V. S. Parvathy, D. Gupta, A. Khanna, and K. Shankar, "Blockchain-assisted secure image transmission and diagnosis model on internet of medical things environment," *Personal and Ubiquitous Computing*, vol. 28, pp. 17-27, 2024. https://doi.org/10.1007/s00779-021-01543-2.

[55] M. Y. Jabarulla and H. N. Lee, "Blockchain-based distributed patient-centric image management system," *Applied Sciences*, vol. 11, no. 1, pp. 1-20, 2021. https://doi.org/10.3390/app11010196.

[56] X. Cheng, T. Cheng, X. Yang, W. Cheng, and Y. Lin, "A face image encryption scheme based on nonlinear dynamics and rna cryptography," *Cryptography*, vol. 9, no. 3, p. 57, 2025. https://doi.org/10.3390/cryptography9030057.

[57] Y. Liao, Y. Lin, Z. Xing, Q. Li, G. Huang, D. Chen, and X. Yuan, "Using 3d-lmm-based encryption to secure digital images with 3-d s-box and fibonacci q-matrix," *IEEE Internet of Things Journal*, vol. 12, no. 24, pp. 55182-55195, 2025. https://doi.org/10.1109/jiot.2025.3624032.

[58] L. Yunlong, L. Yiting, X. Zheng, and Y. Xiaochen, "Privacy image secrecy scheme based on chaos-driven fractal sorting matrix and fibonacci q-matrix," *The Visual Computer*, vol. 41, no. 9, pp. 6931-6941, 2025. https://doi.org/10.1007/s00371-025-04014-4.

[59] S. R. Moosavi and A. Izadifar, "End-to-end security scheme for e-health systems using dna-based ecc," *Communications in Computer and Information Science*, pp. 77-89, 2022. https://doi.org/10.1007/978-3-030-96057-5_6.

[60] Y. Liao, Y. Lin, Q. Li, Z. Xing, and X. Yuan, "Lightweight image encryption algorithm using 4d-nds: Compound dynamic diffusion and single-round efficiency," *IEEE Access*, vol. 13, pp. 74656-74666, 2025. https://doi.org/10.1109/access.2025.3560686.

[61] A. A. Abd El-Latif, B. Abd-El-Atty, and M. Talha, "Robust encryption of quantum medical images," *IEEE Access*, vol. 6, pp. 1073-1081, 2017. https://doi.org/10.1109/ACCESS.2017.2777869.

[62] T. Janani and M. Brindha, "A secure medical image transmission scheme aided by quantum representation," *Journal of Information Security and Applications*, vol. 59, p. 102832, 2021. https://doi.org/10.1016/j.jisa.2021.102832.

[63] J. Gao, Y. Wang, Z. Song, and S. Wang, "Quantum image encryption based on quantum dna codec and pixel-level scrambling," *Entropy*, vol. 25, no. 6, p. 865, 2023. https://doi.org/10.3390/e25060865.

[64] W. W. Hu, R. G. Zhou, J. Luo, S. X. Jiang, and G. F. Luo, "Quantum image encryption algorithm based on arnold scrambling and wavelet transforms," *Quantum Information Processing*, vol. 19, no. 3, 2020. https://doi.org/10.1007/s11128-020-2579-9.

[65] H. Liu, B. Zhao, and L. Huang, "A novel quantum image encryption algorithm based on crossover operation and mutation operation," *Multimedia Tools and Applications*, vol. 78, no. 14, pp. 20465-20483, 2019. https://doi.org/10.1007/s11042-019-7186-3.

[66] Z. Li, X. Zhang, H. Müller, and S. Zhang, "Large-scale retrieval for medical image analytics: A comprehensive review," *Medical Image Analysis*, vol. 43, pp. 66-84, 2018. https://doi.org/10.1016/j.media.2017.09.007.

[67] A. Amaithi Rajan, V. Vetriselvi, M. Raikwar, and R. Balaraman, "Smedir: secure medical image retrieval framework with convnext-based indexing and searchable encryption in the cloud," *Journal of Cloud Computing*, vol. 13, no. 1, 2024. https://doi.org/10.1186/s13677-024-00702-z.

[68] A. Amaithi Rajan, V. Vetriselvi, M. Raikwar, and M. F. H., "Esecmedir: Efficient and secure dual-level transformer based medical image retrieval framework in the cloud," *Computers and Electrical Engineering*, vol. 126, p. 110519, 2025. https://doi.org/10.1016/j.compeleceng.2025.110519.

[69] A. Amaithi Rajan, V. Vetriselvi, A. M, and P. K. R, "Secure and fault tolerant cloud based framework for medical image storage and retrieval in a distributed environment," *Scientific Reports*, vol. 15, no. 1, 2025. https://doi.org/10.1038/s41598-025-16903-8.

[70] B. Ferreira, J. Rodrigues, J. Leitão, and H. Domingos, "Practical privacy-preserving content-based retrieval in cloud image repositories," *IEEE Transactions on Cloud Computing*, vol. 7, no. 3, pp. 784-798, 2019. https://doi.org/10.1109/TCC.2017.2669999.

[71] M. Shen, G. Cheng, L. Zhu, X. Du, and J. Hu, "Content-based multi-source encrypted image retrieval in clouds with privacy preservation," *Future Generation Computer Systems*, vol. 109, pp. 621-632, 2020. https://doi.org/10.1016/j.future.2018.04.089.

[72] Y.-H. Chen and M.-C. Huang, "Fine-grained encrypted image retrieval in cloud environment," *Mathematics*, vol. 12, no. 1, p. 114, 2023. https://doi.org/10.3390/math12010114.

[73] M. Ajitesh, M. Deekshith, A. Amaithi Rajan, V. V., and D. Hemanth, "EdgeShield: Attack resistant secure and privacy-aware remote sensing image retrieval system for military and geological applications using edge computing," *Earth Science Informatics*, vol. 17, pp. 2275-2302, 2024. https://doi.org/10.1007/s12145-024-01256-z.

[74] A. Amaithi Rajan, V. V., A. R., and A. Amaithi Rajan, "Efficient and lightweight framework for confidential medical image search using edge computing," In Proc. 2024 International Conference on Computational Intelligence and Network Systems, Dubai, United Arab Emirates, Nov. 28-29, 2024, pp. 1-7. https://doi.org/10.1109/CINS63881.2024.10864435.

[75] D. Bhanu Mahesh, G. Satyanarayana Murty, and D. Rajya Lakshmi, "Optimized local weber and gradient pattern-based medical image retrieval and optimized convolutional neural network-based classification," *Biomedical Signal Processing and Control*, vol. 70, p. 102971, 2021. https://doi.org/10.1016/j.bspc.2021.102971.

[76] Ş. Öztürk, "Class-driven content-based medical image retrieval using hash codes of deep features," *Biomedical Signal Processing and Control*, vol. 68, p. 102601, 2021. https://doi.org/10.1016/j.bspc.2021.102601.

[77] A. Guan, L. Liu, X. Fu, and L. Liu, "Precision medical image hash retrieval by interpretability and feature fusion," *Computer Methods and Programs in Biomedicine*, vol. 222, p. 106945, 2022. https://doi.org/10.1016/j.cmpb.2022.106945.

[78] E. Özbay and F. Altunbey Özbay, "Interpretable features fusion with precision mri images deep hashing for brain tumor detection," *Computer Methods and Programs in Biomedicine*, vol. 231, p. 107387, 2023. https://doi.org/10.1016/j.cmpb.2023.107387.

[79] B. Hu, B. Vasu, and A. Hoogs, "X-MIR: Explainable medical image retrieval," In Proc. IEEE/CVF Winter Conference on Applications of Computer Vision (WACV), Waikoloa, HI, USA, Jan. 3-8, 2022. https://doi.org/10.1109/WACV51458.2022.00161.

[80] Z. Tabatabaei, Y. Wang, A. Colomer, J. Oliver Moll, Z. Zhao, and V. Naranjo, "Wwfedcbmir: World-wide federated content-based medical image retrieval," *Bioengineering*, vol. 10, no. 10, p. 1144, 2023. https://doi.org/10.3390/bioengineering10101144.

[81] N. Wang, W. Zhou, J. Wang, Y. Guo, J. Fu, and J. Liu, "Secure and efficient similarity retrieval in cloud computing based on homomorphic encryption," *IEEE Transactions on Information Forensics and Security*, vol. 19, 2024. https://doi.org/10.1109/TIFS.2024.3350909.

[82] F. Li, J. Ma, Y. Miao, X. Liu, J. Ning, and R. H. Deng, "A survey on searchable symmetric encryption," *ACM Computing Surveys*, vol. 56, no. 5, pp. 1-42, 2023. https://doi.org/10.1145/3617991.

[83] S. Kumar, A. K. Pal, S. H. Islam, and M. Hammoudeh, "Secure and efficient image retrieval through invariant features selection in insecure cloud environments," *Neural Computing and Applications*, vol. 35, pp. 4855-4880, 2021. https://doi.org/10.1007/s00521-021-06054-y.

[84] M. Shen, Y. Deng, L. Zhu, X. Du, and N. Guizani, "Privacy-preserving image retrieval for medical iot systems: A blockchain-based approach," *IEEE Network*, vol. 33, no. 5, pp. 27-33, 2019. https://doi.org/10.1109/MNET.001.1800503.

[85] Z. Xia, N. N. Xiong, A. V. Vasilakos, and X. Sun, "Epcbir: An efficient and privacy-preserving content-based image retrieval scheme in cloud computing," *Information Sciences*, vol. 387, pp. 195-204, 2017. https://doi.org/10.1016/j.ins.2016.12.030.

[86] I. Kitanovski, G. Strezoski, I. Dimitrovski, G. Madjarov, and S. Loskovska, "Multimodal medical image retrieval system," *Multimedia Tools and Applications*, vol. 76, no. 2, pp. 2955-2978, 2017. https://doi.org/10.1007/s11042-016-3261-1.

[87] L. Xu, X. Zeng, B. Zheng, and W. Li, "Multi-manifold deep discriminative cross-modal hashing for medical image retrieval," *IEEE Transactions on Image Processing*, vol. 31, pp. 3371-3385, 2022. https://doi.org/10.1109/TIP.2022.3171081.

[88] Z. Wang, Z. Wu, D. Agarwal, and J. Sun, "Medclip: Contrastive learning from unpaired medical images and text," 2022. [Online]. Available: https://arxiv.org/abs/2210.10163. [Accessed Mar. 10, 2026].

[89] J. Li, W. K. Wong, L. Jiang, X. Fang, S. Xie, and Y. Xu, "Ckdh: Clip-based knowledge distillation hashing for cross-modal retrieval," *IEEE Transactions on Circuits and Systems for Video Technology*, 2024. https://doi.org/10.1109/TCSVT.2024.3350695.

[90] E. Özbay and F. A. Özbay, "Interpretable pap-smear image retrieval for cervical cancer detection with rotation invariance mask generation deep hashing," *Computers in Biology and Medicine*, vol. 154, p. 106574, 2023. https://doi.org/10.1016/j.compbiomed.2023.106574.

[91] T. Janani, Y. Darak, and M. Brindha, "Secure similar image search and copyright protection over encrypted medical image databases," *IRBM*, vol. 42, no. 2, pp. 83-93, 2021. https://doi.org/10.1016/j.irbm.2020.02.005.

[92] A. Aggarwal, S. Sharma, K. Singh, H. Singh, and S. Kumar, "A new approach for effective retrieval and indexing of medical images," *Biomedical Signal Processing and Control*, vol. 50, pp. 10-34, 2019. https://doi.org/10.1016/j.bspc.2019.01.009.

[93] T. Sunitha and T. S. Sivarani, "Novel content based medical image retrieval based on bovw classification method," *Biomedical Signal Processing and Control*, vol. 77, p. 103678, 2022. https://doi.org/10.1016/j.bspc.2022.103678.

[94] D. Gupta, R. Loane, S. Gayen, and D. Demner-Fushman, "Medical image retrieval via nearest neighbor search on pre-trained image features," *Knowledge-Based Systems*, vol. 278, p. 110907, 2023. https://doi.org/10.1016/j.knosys.2023.110907.

[95] D. Zhu, H. Zhu, X. Wang, R. Lu, and D. Feng, "An accurate and privacy-preserving retrieval scheme over outsourced medical images," *IEEE Transactions on Services Computing*, vol. 16, no. 2, pp. 913-926, 2023. https://doi.org/10.1109/TSC.2022.3149847.

[96] B. Anand, A. Amaithi Rajan, and V. V., "A_2RS: Adversarial attack resistant steganography technique for medical images in digital healthcare," in *Computational Intelligence in Data Science*, E. Mercier-Laurent, B. Jayaraman, P. Ravisankar, A. D. S., and A. Jayasimhan, Eds. Cham, Switzerland: Springer Nature Switzerland, 2025, pp. 339-353. https://doi.org/10.1007/978-3-031-98364-1_26.

[97] R. Elizabeth Kuriyan, R. Sudeep, A. Amaithi Rajan, and V. V., "PCMedIR: Privacy-enhancing cross-modal medical information retrieval system in cloud," in *Communication and Intelligent Systems*, H. Sharma, V. Shrivastava, A. K. Tripathi, L. Wang, Eds. Singapore: Springer Nature Singapore, 2025, pp. 361-376. https://doi.org/10.1007/978-981-96-5732-2_27.