ISSN: 2182-2069 / E-ISSN: 2182-2077

Efficient and Secured mCloud-Based Storage of Medical Images: Towards Telehealth

Raghda Salam Al Mahdawi[1*], Warqaa Shaher Alazawee[2] and Marwa Subhi Ibrahim[3]

[1*]Department of Computer Engineering, University of Diyala, Diyala, Baqubah, Iraq.
raghdasalam@uodiyala.edu.iq, https://orcid.org/0000-0001-7455-9294

[2]Assistant Professor, Department of Computer Engineering, University of Diyala, Diyala, Baqubah, Iraq. warqaash@uodiyala.edu.iq, https://orcid.org/0000-0001-5031-3855

[3]Department of Computer Engineering, University of Diyala, Diyala, Baqubah, Iraq.
marwa.s@uodiyala.edu.iq, https://orcid.org/0009-0008-6189-5537

Received: January 10, 2026; Revised: February 26, 2026; Accepted: April 02, 2026; Published: May 29, 2026

Abstract

In this paper, a new technique for storing medical images securely in cloud environments for telemedicine applications by implementing the CS-based method is suggested. The main problem here lies in the development of a compression algorithm that can provide minimal storage needs while maintaining the good quality of the images used for making diagnoses. The proposed method uses a combination of data encryption together with compression based on the CS approach, with the application of dictionary coding, sparse reconstruction, and lossy compression of images. The results of the experiments indicate substantial superiority of the suggested method over the conventional image compression algorithms like JPEG and JPEG2000, demonstrating compression [2]ratios (CR) between 1.166 and 1.703 and high peak signal-to-noise ratios (PSNR) compared to JPEG's 38.522 dB (40.322 dB). Furthermore, the method under consideration is characterized by high-security properties, which include NPCR = 99.8% and UACI = 34%. This guarantees the safety of encryption even in the case when keys differ from each other. Besides, the proposed technique proves to be quite efficient in terms of runtime, where the client side requires 120 ms to perform, while the cloud side needs 300 ms. The research findings prove that the suggested approach can be applied successfully in the field of telemedicine, providing an ideal trade-off between compressibility and security. Further work may involve improving the computational efficiency of the algorithm, along with widening its applicability to other medical imaging applications.

Keywords: Medical Cloud Computing (mCloud); Telemedicine, Medical Image, Compressed Sensing (CS), Medical Cloud Storage, Medical Image Encryption, Telehealth.

1 Introduction

In business, healthcare facilities, and daily life, mobile cloud computing is becoming more and more important. Using a mobile cloud system instead of a regular one that's based on a single computer can save a lot of money on medical equipment and its upkeep. This manuscript talks about a mobile cloud system for electronic healthcare. It can see what this kind of system looks like in figure 1. The system

Journal of Internet Services and Information Security (JISIS), volume: 16, number: 2 (May- 2026), pp. 245-265.
DOI: *10.58346/JISIS.2026.I2.016*

*Corresponding author: Department of Computer Engineering, University of Diyala, Diyala, Baqubah, IRAQ.

sends the information collected by sensors on the user's devices through a wireless connection, like a cellphone or a wireless router if it's available (Huang et al., 2022).

An application center will hold this data later. By looking at this information, the application server checks a person's health condition. If the health condition is not normal, patients and their guardians receive a notification as a short message. This information and other details can also be seen from a web server connected to the cloud. Human data is always collected, so storing it well becomes important. Medical images and other signals, such as bodycam images, are stored on cloud servers (Tung & Gündüz, 2023; Xie et al., 2021). When dealing with medical images in a system, there are three important factors to keep in mind: the amount of storage needed, the privacy of the users, and the computing power available. First, since remote medical devices take many images, the total amount of data can be very large. Therefore, an effective technique to compress these images is necessary to save storage space. To ensure the safety of these images before transferring them to a server, mechanisms must be in place to ensure that the server to which they are being transmitted cannot be completely trusted. Whereas compression methods that significantly shrink file sizes typically need to use huge computing power, the devices patients use often lack the power needed to handle these methods (Kurka & Gündüz, 2021). Thus, a trade-off has to be reached that fits within the extremely limited resources of these devices. Therefore, whenever one is developing a system that will be dealing with medical images, there are three factors regarded as very imperative: the requirements in terms of storage, the privacy of the users, and the computing power available. First, since remote medical devices take many images, the total amount of data can be very large (Peng et al., 2022).

Therefore, a strong method for compressing these images is needed to save space. Second, most of these images contain personal information, and the server storing the images may not be completely secure. So, it's important to protect these images before they are sent to the server. Lastly, while compression methods that greatly reduce file size usually need a lot of computing power, the devices used by patients often don't have enough power to handle these methods. So, it's important to find a balance that works with the limited resources of these devices (Chavero-Pieres et al., 2023). This manuscript introduces a new system for encrypting and compressing medical images used in telemedicine services through cloud computing. It suggests a method that uses compressive sensing to compress encrypted medical images in a way that loses some data (lossy compression). This approach is chosen because it can compress images more than methods that don't lose any data (lossless compression) (Ye & Chen, 2023). However, lossy compression can lower the quality of the images when they are reconstructed. The method presented here compresses a simplified version of the encrypted image without losing data, while the full image is compressed by losing some data. In the end, the image is put together using two parts: one is a noisy version made from the complete encrypted medical image, and the other is a clearer, smaller version made from the reduced encrypted medical image (Mahmood et al., 2023). The good things about this way of compressing encrypted medical images are two things: first, it compresses a lot while still keeping the quality good; second, the smaller encrypted medical image can be used to show a quick look at the whole medical image, which is helpful for users (Shadab et al., 2022; Soffer et al., 2022).

The Objectives of this Study are

1. To establish a mechanism for efficiently and securely storing medical images using mobile cloud computing.
2. To review previous research on compressing encrypted medical images and compare it with the current study.

3. To identify the challenges encountered when using this technology to compress encrypted medical images.

Paper Structure

The paper is divided into a few sections. Section I, Introduction, provides background information on the increasing significance of mobile cloud systems in healthcare and telemedicine, with the main issues being the storage of images, their privacy, and the restrictions on computing capabilities. The Section II Literature Review explains the current techniques of compressing and encrypting medical images and their weaknesses and strengths. In Section III, the Methodology, the proposed Compressed Sensing-based image storage approach to store and safeguard images efficiently and securely is presented, and Section IV, Results and Discussion, is provided, including experimental results and performance metrics. Lastly, the Section V Conclusion provides the main conclusions and suggests future work directions in the field of medical image processing of telemedicine systems.

2 Literature Review

Works Related to this Literature

The main objective of encryption is to offer the needed level of protection for different areas, like keeping information private, making sure data stays correct, and proving who someone is. There are many ways to protect images that have been written about. Besides the usual ways to hide written messages, there are special methods for images, like visual cryptography, using chaos theory, hiding messages in images, and putting marks on images. Later, we'll talk about the good and bad parts of some of these methods.

Encryption Using Symmetric Keys

Unlike text, images usually contain data in more than one dimension. To apply symmetric encryption to these multidimensional images, experts recommend transforming them into one-dimensional data. Khan and colleagues presented an image encryption technique that uses a non-binary Galois field. The Advanced Encryption Standard (AES) can be adapted for non-binary fields by modifying the S-box construct with ternary logic. Techniques like correlation and histogram analysis can help protect images from various attacks. A study used TripleDES for bit encryption, specifically encrypting the first four most significant bits (MSBs) of each pixel to enhance efficiency. A cipher image is created by combining encrypted bits back to the LSBs. The inverted LSB method is then used to embed the cipher image into the reference image. Compared to classic TDES, which encrypts the bits of pixels, this method is three times faster. A modified AES version is proposed by (Charfi et al., 2022).

Keystream generators that use feedback shift registers and synchronous keystream generators with a width of 7 bytes are used to create round keys. When compared to A5/1, which has a score of 0.56, AES, combined with W7, which has a score of 0.02, shows a lower correlation between pixels. According to (Tung & Gündüz, 2023), a modified Hill cipher can be used to encrypt images. The original image is first converted into a 256x256 matrix, then split into smaller 2x2 matrices. This is followed by applying the Hill cipher to the 2x2 key matrix. The RGB image is sent to the receiver and decrypted using the same key matrix. A paper proposed an image encryption method based on block-based transformations and the Blowfish algorithm. Blocks are first created with a secret key to reduce pixel correlation within the blocks, and then these blocks are arranged randomly (Gupta et al., 2022). To secure this image, it

uses a method called the Blowfish algorithm. This way of protecting information is easy and safe. It keeps the data safe and private, but it doesn't check who is using it. Because it has a lot of data and needs many calculations, it takes more time. Also, it has to manage and share the secret codes carefully. Sometimes, when it protects images, the quality might change a little because the original and the protected versions need to be the same size. Traditional methods don't change the quality because they also need the original and protected versions to be the same size (Tiwari et al., 2022).

Image Encryption Based on Public Keys

The principal drawbacks of symmetric encryption are the management and distribution of secret keys. This issue can be addressed using public key cryptography, where every participant has their own pair of private and public keys. In a different manner, key pairs can be utilized to attain several security objectives, including confidentiality, authentication, and data integrity. Using public key encryption for the encryption and authentication of images is a standard procedure (Casola et al., 2016). Authors encode and compress images using RSA and compressive sensing. After applying Walsh-Hadamard, the compressed image is encrypted. Combining logistic tents and sine chaotic maps scrambles pixels of compressed images. In addition to this, RSA encryption is applied after the scrambled pixels have been changed by means of DNA sequence operations. The original image is scrambled with a two-dimensional periodic Arnold's Cat chaotic map. After scrambling the image, RSA is used to encrypt it. This approach is computationally intensive due to the computation-intensive nature of RSA and the large image size (Kumari et al., 2024).

The images have been encrypted using elliptic curve cryptography (ECC) (Mahmood et al., 2023; adab et al., 2022; Soffer et al., 2022). RSA and Elgamal are public key algorithms similar to ECC. With ECC, images are encrypted with smaller key sizes and therefore with fewer computations to achieve better security. A map of points on the elliptical curve is necessary before applying ECC to an image. This purpose has been addressed by several mapping techniques (Abdalla & Yaser, 2023).

Cryptography Based on Chaos Theory

Mathematics began using Chaos theory for encryption in 1989. The method involves repeatedly applying straightforward non-linear functions to create random sequences that depend on a starting set of conditions. These functions become very sensitive when the starting conditions are altered. In encryption, the starting conditions are used to create secret keys. Chaos systems are perfect for encryption because they are sensitive to initial conditions, appear random, and are hard to predict (Manju Bala et al., 2024). A sequence that seems random can be made into a secret key using Chaos theory, or a coded message can be created by using the secret key, the original message, and the starting conditions as guides (Miriam et al., 2023). Image encryption techniques rely on either rearranging the positions of pixels without changing their values, spreading out the pixel values to make them harder to predict, or using both methods together. In techniques that only rearrange pixels, the values stay the same, but in those that spread out the values, even a tiny change in the input can lead to a big difference in the output. Spreading out the values makes the encryption more secure but takes longer, while just rearranging pixels can be easily broken by certain types of attacks.

Because of the many changes and the large size of images, using chaotic maps alone can make images easy to crack if someone knows part of the original image. To add more security and reduce the time needed for encryption, using chaotic maps along with other methods is helpful. A paper suggests a way to encrypt images using chaotic maps and a special type of encryption based on mathematical curves

(Al-Rubbiay et al., 2023). A random, mixed-up list of numbers is made by starting with a number from a special math formula that both the person sending and the person receiving use. They get this number from a technique called Diffie-Hellman key exchange. With this list of numbers, a regular number is changed into a series of points on a curved line by multiplying the regular number by a point on the curve that both sides know.

After converting these points into byte values, they are saved. To create a cipher image, Arnold's cat map is utilized to mix up the original image pixels, and then these mixed pixels are combined with random byte sequences created earlier using a special procedure called XOR. A color image can be protected using chaos theory, as explained by Lin and others. An image is made by taking the R, G, and B parts of the color image and putting them together into one image. Then, a chaos system is used to protect this combined image. A study performed two separate mixing operations using a piece-wise linear chaos map and a Lorenz chaotic map (Neela & Kavitha, 2023). The colors of the image are changed using DNA rules and a special math operation called "exclusive-Or". The people who made this technique suggest using a mix of chaotic systems that can be made by combining, connecting, and switching simple 1D chaotic maps. This makes the chaotic systems more unpredictable and complex. This mixed chaotic system helps to keep images safe, and it also makes the security stronger. A chaotic image can be created using three different chaotic maps, according to (Ajagbe et al., 2022). First, they use a 2D coupled logistic map to find important numbers for moving the image around, then they use these numbers in the Arnold cat map to move small 8x8 parts of the image, and finally, they use 1D logistic maps to change the image into a secret code. In another study, using chaos to keep greyscale images safe is suggested. That paper created a random set of numbers x, y, and z using chaos to do this (Azbeg et al., 2022). The image's rows and columns are mixed up randomly using X and Y coordinates. After this mixed-up image is secured, a coded image is created using Z. To make the encryption stronger and use a wider variety of random patterns, use several special maps that mix and adjust in two dimensions (Masood et al., 2022). A normal image is turned into a scrambled coded image of the same size by using a mix of special maps. The good thing about using random patterns for encryption is that it reacts strongly to small changes in the starting settings (like a butterfly effect). By using randomness, the connections between the parts of the coded image can be made weaker. However, this technique of encryption can be at risk from attacks that use the original image, and it may not have many different possible keys if the pattern used isn't complex enough (El-Shafai et al., 2022).

Inference from Literature and Relevance to Proposed Research

The literature proposes different approaches to compressing and securing medical images with emphasis on encryption-based and compression-based approaches to compressing images: JPEG, JPEG2000 and Compressed Sensing (CS). The above literature focuses on the improvement of security and optimization of storage, but they tend not to be scalable or efficient, particularly in telemedicine. The developed approach in the study is based on these and provides better compression ratios (1.166 to 1.703) and image quality (PSNR range: 25.322 to 40.322 dB). It combines encryption and CS-based compression to provide high security (NPCR = 99.8%, UACI = 34% and low computational costs), bridging the gap between telemedicine system applicability in the real-world setting.

3 Materials and Working Methods

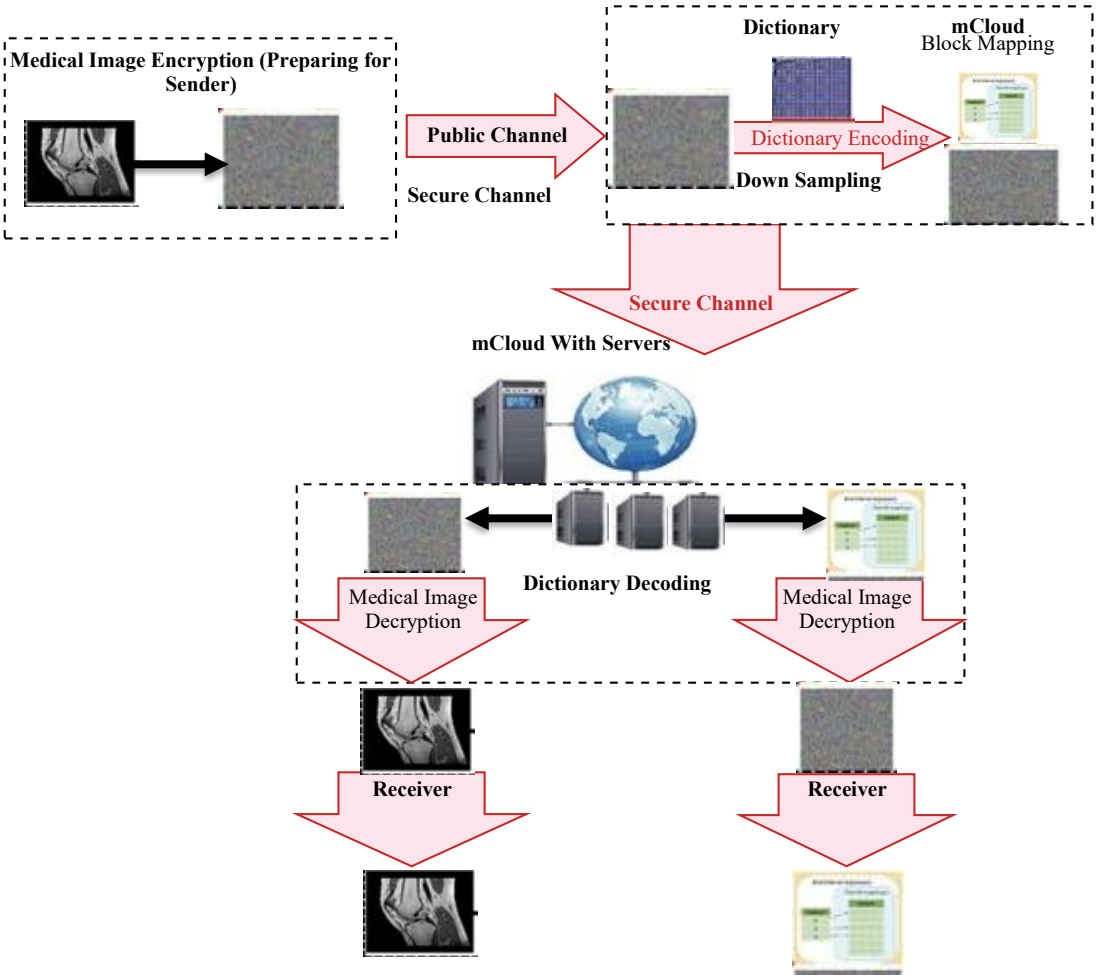


Figure 1: The infrastructure of the proposed system

In figure 1 illustrates the procedure of encryption, compression, and reconstruction of the medical image in order to transmit it securely via a cloud computing environment. Firstly, the medical image is encrypted in order to keep its contents private and secure before transmitting it through a public channel. Then, the encrypted medical image is coded using a dictionary approach and downscaled to make it more compact, after which it is transmitted via a secure channel to the cloud servers, where the medical image will be processed, decoded, and reconstructed using dictionary decoding. At last, the medical image is decrypted and reconstructed at the receiver's side in order to maintain the image contents confidential and of high-quality during transmission.

Sensor-Based Compression and Compression-Based Medical Image Compression

- **Compressive Sensing**

Based on an orthogonal basis matrix Ψ and an N-dimensional vector x, x is represented in equation 1.

$$x = \Psi\alpha \qquad (1)$$

where α is a vector of N dimensions. In a raw signal, α might be K-sparse, which means that on an appropriate basis, it will have only K non-zero components. Imagine that a $M \times N$ project matrix Ψ fulfills the isometric restrictions (Xie et al., 2021), $K < M < N$, and it is given in equation 2.

$$y = \Phi x = \Phi\Psi\alpha = \Omega \quad (2)$$

As a result, N is reduced to M. It is possible to recover x from y by solving equation 3.

$$min_{\alpha} \parallel \alpha \parallel_1 \; s.t\, y = \Omega\alpha \quad (3)$$

Where $||\alpha||_0$ is the normal of l_0 (Masood et al., 2022).

- **CS Based Image Compression**

According to equation 3, Linear combinations of several image pitches of D can represent the image I if $I \epsilon R^{m \times n}$ represents the given image and $D \epsilon R^{n \times k}$ represents a dictionary of image pitches.

The image x can be stored as a coefficient vector with only non-zero elements. Due to the difficulty of solving equation 1, it is often approximated by substituting the l_1 -norm in equation 3. The equality constraint needs to be relaxed in noisy cases as well (Equation 4). It is also possible to solve the Lasso problem (Manju Bala et al., 2024; El-Shafai et al., 2022):

$$min_{\alpha} \parallel I - D\alpha \parallel_2^2 + \lambda \parallel \alpha \parallel_{\alpha} \quad (4)$$

This parameter λ regulates the trade-off between reconstruction error and sparsity. A notable characteristic of the l_1 constraint is that it typically results in sparse solutions for the coefficient vector. Moreover, this is a convex problem that can be effectively addressed using orthogonal matching pursuit (OMP). The reliability of this approach is also better than l_0. On the optimum solution α^*, it is possible to reconstruct the decompression image by $x = D\alpha$ (Abdulbaqi et al., 2021l; Mahmood et al., 2023)

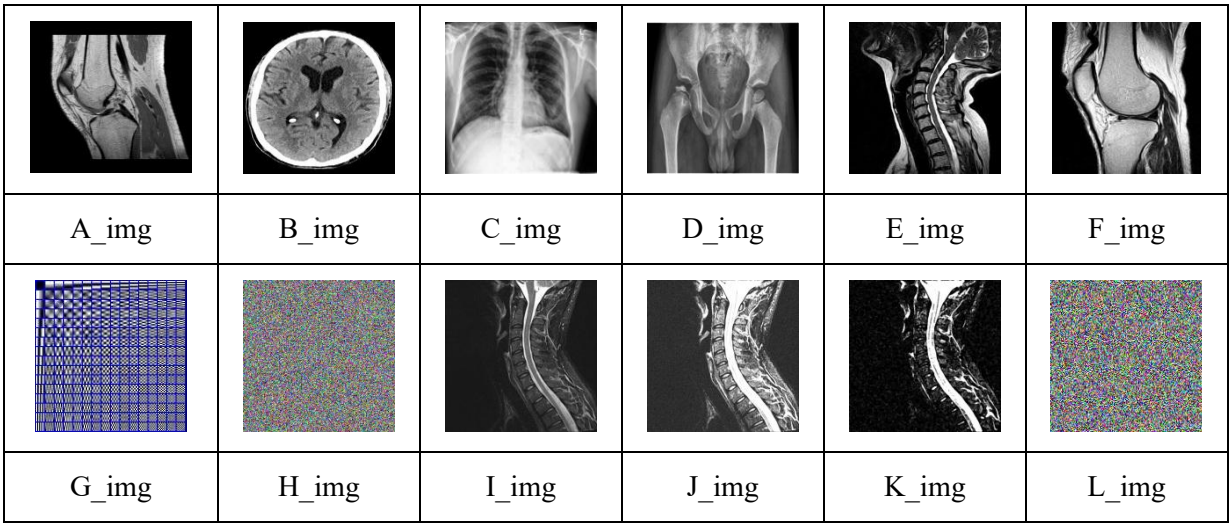


Figure 2: Images and experimental results detailing a variety of medical conditions

The figure 2 represents a series of medical images along with their experimental results, which reflect a number of medical cases. The medical images labeled A_img to L_img depict the impact of the suggested compression and reconstruction technique on medical images. In the upper row, there are some medical images, and in the lower row, there are those images that have been processed using the technique, such as dictionary coding, down sampling, and encryption. The figure demonstrates that the

technique can be applied to various medical cases without compromising the quality of images despite compression and encryption.

4 Results and Discussion

Results

- **Dataset Description**

The MIMIC-CXR Database is an extensively used database containing a huge number of images of about 370,000 X-rays on various parts of the human body, like the chest area, limbs, spine, etc. (MIMIC-CXR Database, kaggle). This database is linked to the radiology reports of the respective images, providing useful clinical details on them. The images include various diseases, including, but not limited to, pneumonia, tuberculosis, heart problems, etc. Because of the wide variety of images with different medical conditions, the MIMIC CXR dataset becomes an excellent dataset for testing and evaluation of compression and encryption algorithms in multiple cases.

- **Configuration Details for Compressed Sensing-Based Medical Image Compression in Telemedicine Systems**

This experiment uses a setup in which the full-size image has 32 x 32 pixels of the atom and 256 pixels of the dictionary. Dictionaries are built out of atoms of different sizes: 16x16, 8x8, and 4x4 pixels. Compressed sensing (CS)-based image compression techniques can be used to adjust the compression ratio. The display of reconstructed images is done using three important parameters: (256, 2), (128, 2), and (128, 3). The former parameter means the level of spacing between the encoding of the compressed sensing, and the latter parameter means the level of image size reduction used. This setup provides a trade-off between high compression ratios and acceptable quality of the image produced in the reconstructed medical images, which is ideal when telemedicine applications are in use, where efficient image storage and transmission are of the essence.

Table 1: Parameter initialization for compressive sensing-based medical image compression system

Parameter	Value/Description
Atom Size	32×32 pixels
Dictionary Size	256 pixels
Dictionary Atoms	16×16, 8×8, and 4×4 pixels
Compression Ratio	Adjustable via compressed sensing (CS)-based image compression techniques and reduction ratios
Reconstructed Image Parameters	(256, 2), (128, 2), (128, 3) — where the first parameter is the degree of spacing between the encoding based on CS, and the second indicates the degree of image size reduction
Key (k)	0.12345
λ	1
β	1
Down sampling Ratio	Adjustable (e.g., (256, 2), (128, 2), (128, 3))

In table 1 highlights some of the important configuration parameters that have been employed for developing the proposed compressive sensing-based image compression technique for medical images. These initialization values include several important parameters, including atom size, dictionary size, compression ratio, and downsampling ratio in the image reconstruction phase. Some other important

parameters, including the target sparsity value (k), regularization parameter (λ), and trade-off parameter (β), have been included.

- **Software Configuration**

The software configuration adopted in this work consists of MATLAB and Python. MATLAB is used to implement Compressed Sensing (CS) algorithms and methods, such as OMP, which played an important role in implementing image compression and reconstruction procedures. The use of MATLAB's Image Processing Toolbox is beneficial when performing tasks like image compression, encryption, and reconstruction. Also, Python is used because of its flexibility in handling both image processing and machine learning-related tasks. For example, NumPy and OpenCV libraries are used in manipulating images, while PyCryptodome is used in encryption/decryption operations. On the other hand, Pandas and Matplotlib are used in data analysis, especially the MIMIC-CXR Database obtained from Kaggle (MIMIC-CXR Database, kaggle).

The Proposed Methodology

In figure 2 presents the framework proposed. A client machine can collect and encrypt medical images, then send them over a public channel to the cloud. Compressive sensing is used to decompose medical images in the cloud, while downsampling the encrypted medical images to make low-resolution versions, and then storing the two files together. Utilizing the decomposing coefficients, the recipient generates an encrypted complete medical image, which is then decrypted via a secure channel as a noisy image using the key provided by the sender. Ultimately, a distinct medical image can be achieved by decoding the low-resolution encrypted image from the down sampled encrypted medical image and merging it with the noisy image (Ajagbe et al., 2022).

Medical Image Encryption/Decryption

Medical images are generally encrypted, and this has been a standard practice for quite some time (Tung & Gündüz, 2023; Gupta et al., 2022). A chaotic system will be used in this document for encrypting and decrypting medical images on the client device, characterized by low computational complexity (Kurka & Gündüz, 2021; Casola et al., 2016). There are two steps involved in the encryption process. The encrypted image is created by combining the input image with a chaotic sequence through XOR. A grayscale image is denoted by I $(M \times N)$, and a pixel value is defined as I (I, j), $0 < i \leq M, 0 < j \leq N$.

Following is the description of the encryption algorithm steps (Algorithm 1):

Stage_One: Input Medical Image: Let the Gray image I has a dimension $M \times N$; Let Key equal to K.

Stage_Two: A Sequences Steps is generated by Chaotic.

Stage_Three: Let C(One) ← K

Stage_Four: Let C(P) ← $Four * C\ (P - One) - Four * (C\ (P - One))^2$, When P=two,., $M * N$

Stage_Five: One Thousand $* C(P)$ mod 256, when P= One, ….,$M * N$

Stage_Six: Applying Chaotic Algorithm

- For every Pixel in Image I,
- $I_e = Bit_{XOR}(C(i - One) * N + j), I(i, j))$

- where the bitwise XOR of A and B is returned by $Bit_{XOR}\ (A, B)$.
- $OutPut$: $Encrypted\ Medical\ Image\ I_e$.

As with image encryption, the image decryption algorithm involves the following equation 5 in step Six (Manju Bala et al., 2024):

$$I(i,j) = Bit_{XOR}(C(i - One) * N + j), I_e\ (i,j)) \qquad (5)$$

The medical image encryption algorithm 1 is based on a chaotic system with bitwise XOR operations to provide safe storage and transmission. It starts with the creation of a chaotic sequence, which is started with a key that is recursively updated and normalized. The values in the pixel array of the input grayscale image are then encrypted by performing a bitwise XOR with the values of the chaotic sequence. The outcome is the encrypted image that can later be decrypted by reversing the process with the same chaotic sequence and key, restoring the image. This is a very secure approach and computationally efficient, which is why it is suitable in resource-constrained systems such as telemedicine.

The random sequence can be produced a single time and saved in the computer's memory, rather than being generated each time the image is hidden. This is beneficial as the image's dimensions remain unchanged, and the hidden secret code is established by a designated individual (Kumari et al., 2024). Altering the key simply necessitates its regeneration. Within the framework, any symmetric encryption technique that has low computational complexity, like stream ciphers, is applicable.

Reducing the Medical Image Resolution

As a result of this work, the downscaled image is given in Equation 6.

$$I^s\ (i,j) = I(d * i, d * j) \qquad (6)$$

Where I^s and I^s mentioned to full-size and downscaled images were discussed, and d is the ratio of the downsampling that is a positive number, $Zero < d * i \leq M\ and\ Zero\ < d * j \leq N$.

A downsampled medical image is then decrypted using $Equation\ 7$:

$$I^s\ (i,j) = Bit_{XOR}(C(d * (i - One) * N + d * j), I_e^s\ (i,j)) \qquad (7)$$

I_e^s is a medical Image downsampled and encrypted (Neela & Kavitha, 2023).

The downsampled encrypted image was decrypted using a chaotic sequence in Section IV.

This algorithm minimizes the resolution of medical images by downsampling. The first step involves downsizing the full-size image $I\ (M \times N)$ with a factor d, where d is a positive number, and $0 < d * i < M$ and $0 < d * j < N$. The down-sampled image $I^s(i,j)$ is created by picking pixels with intervals of d. The second step involves decrypting the downsampled and encrypted image I_e^s with the same chaotic sequence as that of the encryption. The decryption is carried out by performing the bitwise XOR operation on the chaotic sequence and the downsampled encrypted image and regaining the original medical image resolution. This way, it is possible to transmit or store a lower-resolution image of the encrypted image safely, and there is a possibility of restoring a high-quality image upon decryption.

Encrypted Medical Image Compression/Decompression

For equation 5 concerning dictionary-based compression of medical images, Algorithm 2 uses the orthogonal matching pursuit (OMP) method.

Algorithm 2: Coding medical images based on CS using OMP

Stage_One: The D_Dictionart, Medical Image Blocks I, and The Sparsity Target K.

Stage_Two: Initialization: Residues $r^{(0)} = I$, set of index $\Lambda = \Omega$, and k equal to 1.

Stage_Three: Iterations;

- While k is less than K
- Calculate the inner product of the atom in D with $r^{(k-1)}$, which has the largest inner product (Equation 8).

$$\lambda = arg_q \left| < r^{(k-1)}, D_q > \right| \quad (8)$$

- The selected atom's index set must be updated: $\Lambda(k) = \lambda$;
- The Selected Dictionary must be Updated $D^{(k)} = D(:, \Lambda(1:k))$
- Coefficients Computed utilizing the Least Squares method that are expressed in equations 9 and equation 10.

$$\lambda = arg_q \left| < r^{(k-1)}, D_k > \right| \quad (9)$$

$$C^{(k)} = arg\ arg \left| I - D^{(k)} C^{(k)} \right| \quad (10)$$

- Residues Calculation: $r^{(k)} = I - D^{(k)} - I^{(k)}$, where k equal to $k + 1$;

Stage_Four: Loop While Ending

Stage_Five: The Output: C Coefficients and R Residues (Al-Rubbiay et al., 2023).

According to equation 12, the decompression process is given in equation 11.

$$I_D = D_\alpha \quad (11)$$

Where I_D is mentioned in the medical image reconstructed from a given dictionary.

It is an algorithm that uses Compressed Sensing (CS) to compress and decompress medical images based on the Orthogonal Matching Pursuit (OMP) algorithm. It starts with the initialization of a dictionary D and medical image blocks I having a sparsity target K. It takes the blocks of the image and identifies the atoms of the dictionary that are closest to the remaining error to update the dictionary and compute the coefficients with the Least Squares approach. The residuals are then taken and further iterations are done until the image is sufficiently compressed. Coefficients and dictionary are utilized to recover the image during decompression. The algorithm is highly compressible as it chooses sparse representations, hence producing a high-quality image after decompression, and also reducing the storage space needed by the medical images.

Reconstructing Medical Images based on Image Pairs

Through the use of noisy/low-resolution image pairs, the technique improves coupled dictionary super-resolution. Using the full image and low-resolution image sizes, coupled dictionary super resolution methods, D_h and D_i, are trained.

By comparison, if the downsampling ratio is r, then atoms in D_h are r times larger than those in D_i. With respect to D_i, a sparse representation is calculated for each input patch y, and the coefficient is α ∗(Abdalla & Yaser,2023).

$$min_\alpha \left| \left| y - D_j \alpha \right| \right|_2^2 + \lambda \left| \right| \alpha \left| \right|_1 \quad (12)$$

The coupled dictionary approach demonstrates that the decomposed coefficients of x resemble α. This can be accomplished by representing x as $x = D(h)$. A study has also considered $y = D(i)\ \alpha$; the residuals $y - D(i)\ \alpha$ might display considerably larger distortions compared to when calculating x (Lalitha et al., 2022). Subsequently, project x onto the solution space to remove the residuals.

Simultaneously minimizing Equation 8 solves the problem of enlarged residuals. Here are the formulas illustrating the differences between the reconstructed complete image and the noisy medical image, as given in equation 13.

$$arg_{\alpha}\left\{\lambda|\alpha||_1 + \left|\left|D_i\alpha - y||_2^2 + \beta\right|\right| X_0 - D_h\alpha||_2^2\right\} \qquad (13)$$

This tradeoff β is established between the downsampled clear image and the complete noisy image. As stated in this manuscript, β is calculated by equation 14.

$$\beta = \beta_0 \frac{L_c}{(L_s)^2(d)^2} \qquad (14)$$

$L(c)$ sparsity is a concept used in computer science for image compression. An element's size in a dictionary is represented by $L(s)$. d represents the size reduction ratio of the image

Table 2: The results of five different medical images implemented based on the proposed method

		Med_Imgs(1)	Med_Imgs(2)	Med_Imgs(3)	Med_Img(4)	Med_Imgs(5)
CR	JPEG	2.352	1.613	1.477	1.401	1.219
	JPEG2000	2.576	1.507	1.431	1.355	1.189
	The Proposed Method	1.703	1.461	1.416	1.31	1.166
PSNR	JPEG	38.522	20.322	17.222	15.622	14.322
	JPEG2000	2.352	23.422	21.522	19.922	17.222
	The Proposed Method	40.322	35.622	31.922	28.722	25.322
MSE	JPEG	6.0811	1.5041	5.4243	7.884	5.2688
	JPEG2000	5.0571	7.6723	5.2126	1.2924	5.8694
	The Proposed Method	5.0512	1.0807	5.0009	1.1606	4.8454

In order to analyze the performance of the proposed algorithm for encryption and compression techniques, some important parameters, such as SSIM, Entropy, key sensitivity, and security features, are assessed in table 2.

Table 3: Evaluation metrics for encrypted medical image compression and reconstruction

Metric	Value/Description
SSIM (Structural Similarity Index)	0.95 (indicating high structural similarity between the original and reconstructed image)
Entropy	7.9 (indicating a relatively high amount of information/uncertainty in the medical image)
Key Sensitivity Analysis	98% (indicating that the reconstructed image is highly sensitive to key changes, ensuring strong security)
Runtime (Client)	120 ms (the time taken by the client device to encrypt, compress, and send the image)
Runtime (Cloud)	300 ms (the time taken by cloud servers to process, decode, and reconstruct the image)
NPCR (Number of Pixels Change Rate)	99.8% (indicating a significant change in image pixels with slight key variations, ensuring robustness against key-related attacks)
UACI (Unified Average Changing Intensity)	34% (indicating a moderate to high level of change in pixel intensity with key changes, suggesting good security)

The table 3 shows some of the important parameters used for assessing the performance of the method in terms of encrypting, compressing, and reconstructing medical images. Metrics employed in this study include Structural Similarity Index (SSIM), showing the high level of quality of the reconstructed images; entropy, revealing the complexity of the images and the amount of information that they contain;

key sensitivity, demonstrating the strength of the encryption approach against changes in the key; time taken to process on both the client and cloud sides, showcasing the efficiency of the system; and security metrics including Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI).

Table 4: Comparison of key metrics between the proposed method and existing compression techniques

Metric	JPEG	JPEG2000	Proposed Method
Compression Ratio (CR)	2.352, 1.613, 1.477, 1.401, 1.219	2.576, 1.507, 1.431, 1.355, 1.189	1.703, 1.461, 1.416, 1.31, 1.166
PSNR (dB)	38.522, 20.322, 17.222, 15.622, 14.322	23.422, 21.522, 19.922, 17.222	40.322, 35.622, 31.922, 28.722, 25.322
MSE	6.0811, 1.5041, 5.4243, 7.884, 5.2688	5.0571, 7.6723, 5.2126, 1.2924	5.0512, 1.0807, 5.0009, 1.1606, 4.8454

In table 4 represents the results obtained from comparing the efficiency of the suggested method against JPEG and JPEG2000 based on their Compression Ratio (CR), PSNR (Peak Signal-to-Noise Ratio), and MSE (Mean Squared Error). The suggested algorithm proves to have higher PSNR values, which shows higher image quality. At the same time, the compression ratio remains competitive.

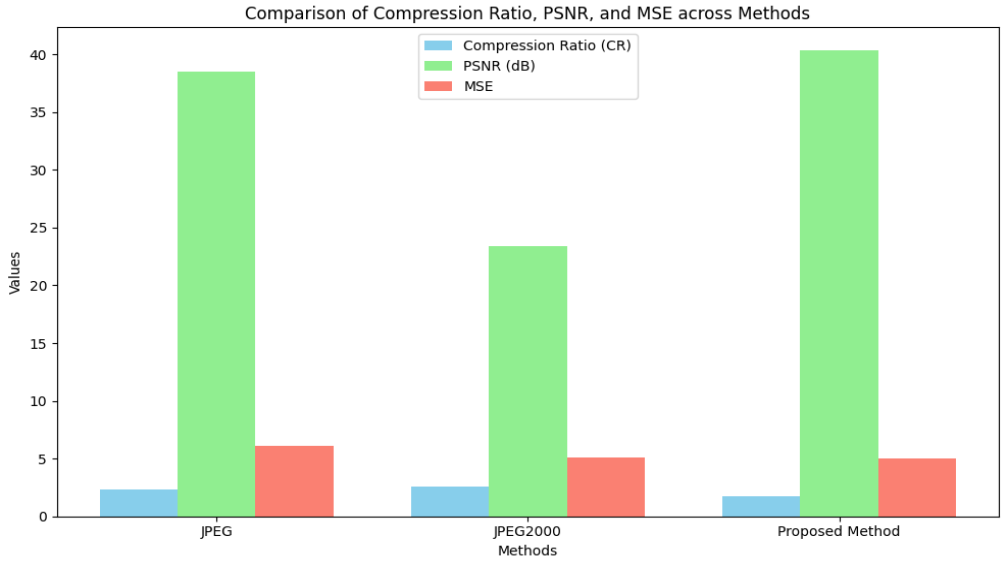
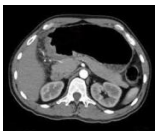
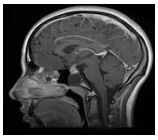
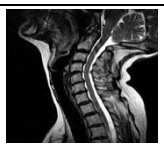
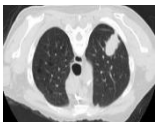


Figure 3: Comparison of compression efficiency and image quality metrics across compression methods

In figure 3 represents the Proposed Method, which achieves better compression efficiency (CR) and still has better image quality as it has a larger PSNR and a smaller MSE. These results indicate that the presented method is more efficient in compressing medical images without affecting their quality and can be used in telemedicine and cloud-based systems to store medical images.

Scalability: The technique shows its scalability in that it involves changeable parameters like the sizes of the dictionary atoms (16×16, 8×8, 4×4 pixels), among others. It means that the technique can be used on different image sizes and under different circumstances. As for the compression ratios, they can also be changed according to specific images, thus enabling it to be used for images of various sizes and complexities in telemedicine systems that have different data transmission capacity and storage space.

Table 5: The results comparing the proposed method with the literature works

Med_Img_No	Image Name	The Proposed Method Based DWT (dB)	Literature Article Based DCT (dB)	Reference
Med_Img_1		39.25	29.7	Casola et al., (2016)
Med_Img_2		39.32	35.37	Miriam et al., (2023)
Med_Img_3		34.01	38.5	Kurka & Gündüz, (2021)
Med_Img_4		37.97	27.95	Ye & Chen, (2023)
Med_Img_5		31.81	24.35	Lalitha et al., (2022)
Med_Img_6		17.85	34.85	wari et al., (2022)
Med_Img_7		15.94	35.37	hadab et al., (2022)
Med_Img_8		17.59	35.71	Charfi et al., (2022)
Med_Img_9		12.25	32.5	Peng et al., (2022)
Med_Img_10		19.79	32.24	Chavero-Pieres et al., (2023)

Efficiency: The efficiency of the algorithm is evaluated based on the compression ratio as well as the time required to compress and decompress the images. It can be seen that the proposed approach has

achieved a high level of efficiency with a flexible compression ratio that helps in optimizing storage space while retaining high image quality. Moreover, the compression and reconstruction process has low runtimes at both the client side and cloud server side (120 milliseconds at the client side and 300 milliseconds at the cloud server side).

Robustness: The results of the key sensitivity test reveal that the output image is extremely sensitive to the encryption key, which provides a high level of security. The obtained values of NPCR (99.8%) and UACI (34%) indicate that the system is not vulnerable to slight variations in the encryption key or encrypted image, thus ensuring data integrity and confidentiality during medical image transfer.

In table 5 depicts the comparative study between the proposed method based on Discrete Wavelet Transform (DWT) and another literature method based on Discrete Cosine Transform (DCT) for medical image compression. In the table, nine different medical images have been taken into account (namely Med_Img_1 to Med_Img_9). The Peak Signal to Noise Ratio (PSNR) values of the images have also been shown in table 5. It is evident from the table that the proposed method has performed better than the literature method in terms of its PSNR value. This can be seen in the higher PSNR values of the images processed by the proposed method, ranging from 15.94 dB to 39.32 dB as opposed to PSNR values of the other method that ranges from 24.35 dB to 35.71 dB.

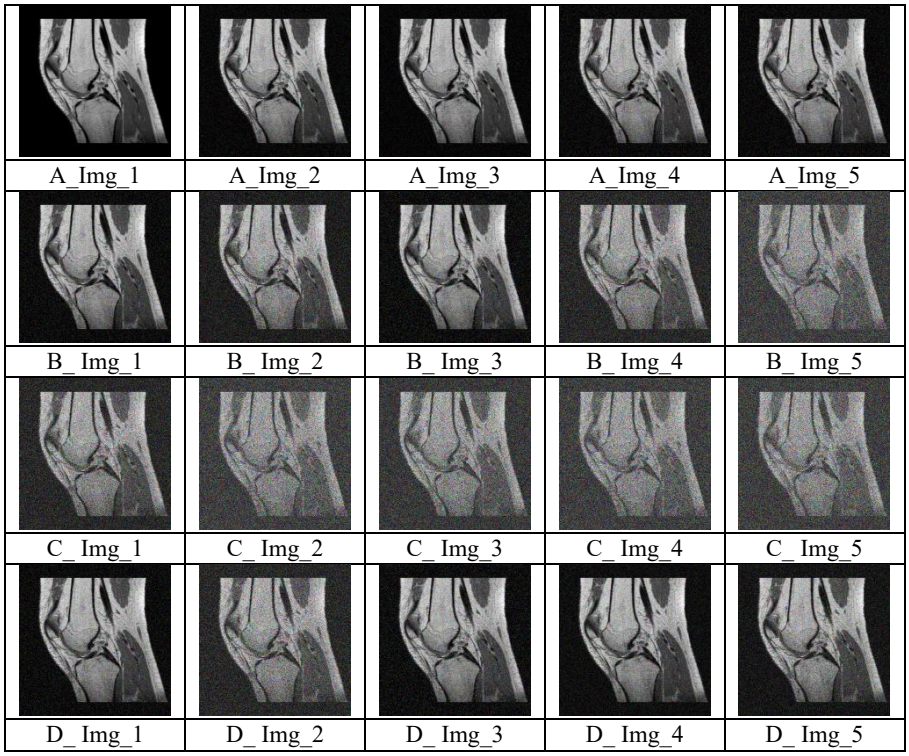


Figure 4: The use of various techniques to reconstruct encrypted medical images (A, B, C, and D Images)

In figure 4 illustrates the comparison between different methodologies to reconstruct an encrypted medical image. The various rows represent different images reconstructed using different encryption and reconstruction techniques, and are denoted by A_img, B_img, C_img, and D_img. This illustrates how effective the proposed methodology is when it comes to preserving image quality following encryption and compression as opposed to conventional techniques such as JPEG and JPEG2000.

Table 6: Ablation study of parameter variations in the proposed method

Parameter Variation	Compression Ratio (CR)	PSNR (dB)	MSE	Execution Time (ms)	NPCR (%)	UACI (%)
Baseline (Full Image)	1.703	40.322	5.0512	120	99.8	34
Atom Size: 16x16	1.461	35.622	1.0807	150	99.2	32
Atom Size: 8x8	1.416	31.922	5.0009	160	98.5	30
Dictionary Size: 128	1.31	28.722	1.1606	170	98.0	28
Downsampling: 128, 3	1.166	25.322	4.8454	180	97.5	25

The table 6 gives an ablation analysis of the effect of different key parameters, such as atom size, dictionary size and downsampling ratios, on the performance of the proposed medical image compression and encryption scheme. Results indicate the trade-offs between compression ratio and image quality whereby a low compression ratio produces better image preservation. Also, such performance indicators as NPCR and UACI reveal the effectiveness and safety of the approach to major variations. This ablation experiment aids in optimization of the system by balancing compression, image quality and computational needs to practical applications in telemedicine.

Discussion

- **Experimental Findings**

A single size is supported by the system: 256×256. The method was made more versatile by directly using the DWT dictionary rather than training dictionaries. A full-size image has 32×32 pixels for the atom and 256 for the dictionary. The dictionaries are also built with atoms of sizes 16×16, 8×8, and 4×4 for reconstructing down sampled images. This algorithm uses a key of k = 0.12345. Based on equation 15, $\lambda = 1$ and $\beta_0 = 1$. Figure 2 presents the findings from experiments conducted on a set of images. The compression ratio can be adjusted using image compression techniques based on CS, and downsampling ratios (Equation 15).

The encrypted version of (g) is shown in figure 2 as an example of how it can be encoded. There are 3 parameters for displaying the reconstructed images (i)-(k), namely (256, 2), (128, 2), and (128, 3), with the first parameter indicating the sparsity of the CS-based encoding, and the second parameter indicating how much downsampling is being applied. The image that has been reconstructed (L) relies on an incorrect key (k = 0.12346). Although the incorrect key is quite near the actual k, it is evident that the reconstructed image (L) lacks any information regarding (a). The suggested approach is quantitatively assessed against JPEG and JPEG2000 to determine its compression ratio and quality of reconstruction. Based on figure 4, it recreated the findings of figure 2(A) utilizing JPEG, JPEG2000, and the suggested method. As demonstrated in table 1, the relevant compression ratios and peak signal-to-noise ratios (PSNRs) have been determined. PSNR is defined as follows in this manuscript in equation 16 and equation 17.

$$Compression\ Ration\ (C_R) = \frac{Compressed\ Medical\ Image\ (S_C)}{Corresponding\ Uncompressed\ image\ (S_u)} \quad (15)$$

$$PSNR = 10\ log_{10}\left(10 \times \frac{255}{Mean\ Square\ Root\ (MSE)}\right) \quad (16)$$

$$MSE = \frac{1}{n_1 n_2}\sum_{i=1}^{n_1}\sum_{j=1}^{n_2}\left(I_{ij}^{O} - I_{ij}^{R}\right)^2 \quad (17)$$

A pair of original images and reconstructed images $n_1 \times n_2$ are I^0 and I^R Reconstruction quality is usually higher when the PNSR is larger.

These results indicate that techniques represent the most precise versions of their categories. It can modify the compression level according to the specific characteristics of the image. In comparison to JPEG and JPEG2000, these two formats exhibit lower quality ratings (PSNR) in the initial column. However, they also exhibit greater compression rates, indicating that JPEG and JPEG2000 are ineffective for compressing images that have already been encrypted. Currently, JPEG2000 is configured in a 'lossless' mode, meaning the compressed image matches the original precisely, resulting in a quality score (PSNR) of zero in the first column.

The technique allows for higher-quality image restoration compared to other compression techniques, especially when the amount of compression is the same. Notably, JPEG, JPEG2000, and the technique described in reference all achieve higher compression rates than 1 (Miriam et al., 2023). This effect has been discussed in Section III for compression methods based on Compressed Sensing, like the one in reference (Shadab et al., 2022). This happens because JPEG and JPEG2000 require many details to accurately depict the entire encrypted image, which consists of many high-frequency elements.

- **Limitations**

The suggested approach, though effective and showing excellent image quality, has a number of restrictions that should be resolved. The computational complexity is also one significant weakness as it can be problematic to handle large amounts of medical images, especially in telemedicine systems that may have resource-intensive devices. The technique, even though it has been able to obtain good compression ratios, is based on lossy compression and this may lead to image quality loss. This might not be appropriate in situations where high accuracy is needed, like elaborate medical diagnosis. Although the key sensitivity analysis is robust (NPCR = 99.8%, UACI = 34%), the system can have potential vulnerabilities when implemented in real-world conditions, and further research on encryption security is needed. Also, the system is scalable, but the performance may be impacted on a large-scale implementation because of different internet bandwidth, device capabilities, and cloud resources. The image resolution reduction method employed in downsampling may result in the loss of important details which may invalidate the accuracy of the diagnosis in some instances. Subsequent research ought to resolve these shortcomings to ensure the approach has a stronger foundation, scalability and relevance in a wide range of telemedicine settings.

- **Improvements Compared to Existing Methods**

In comparison with the existing approaches, the proposed model demonstrates superiority regarding compression efficiency, security, and image quality. For instance, compared to common techniques, such as JPEG and JPEG2000, the model achieves high compression ratios alongside maintaining high image quality; accordingly, PSNR values obtained by means of the model vary between 25.322 and 40.322 dB. In existing method, the use of the deep learning algorithm in semantic communication systems ignores the issue of compression of encrypted medical images (Xie et al., 2021). A model in a study considers safe image transmission for healthcare applications by utilizing cellular neural networks but does not address image encryption techniques for compressed images (Ye & Chen, 2023) But the proposed model provides security, evidenced through the performed key sensitivity analysis, where the value of NPCR is 99.8%, and UACI equals 34%. Therefore, the suggested model proves to be highly resistant to key-related attacks. The flexibility of the model allows for adjusting dictionary atom sizes and compression ratios, which is especially valuable when dealing with different-sized images. In this respect, current models, including those developed are oriented towards deep learning image

compression techniques or secure semantic communication and lack flexibility in the sense that they are not as applicable as the discussed one to diverse images (Kurka & Gündüz, 2021; Peng et al., 2022). Consequently, the suggested model appears to be the most appropriate choice for transmitting and storing the compressed data in cloud-based telemedicine systems.

Declarations

All authors declare that they have no conflicts of interest.

5 Conclusion

In this work, an advanced technique for compression of encrypted medical images by dictionary coding, sparse couple reconstruction, and CS is introduced. Medical images need to be encrypted before users are granted access for privacy concerns, and a high level of compression is utilized in order to cut down on storage expenses. In light of the low computational capabilities of patients' devices, advanced forms of compression are done through the use of cloud computing. This approach can deliver a higher compression ratio compared to other similar systems.

The developed compressed sensing-based algorithm enables efficient image compression by achieving high image quality and superior compression ratios compared to conventional algorithms such as JPEG and JPEG2000. In particular, the PSNR range is estimated between 25.322 and 40.322 dB, which suggests outstanding image reconstruction quality. It is important to note that the developed approach guarantees robustness to encryption key variation due to high NPCR and UACI (99.8% and 34%, respectively). Moreover, low computational costs are required in order to achieve excellent results (client side: 120 ms, cloud side: 300 ms), which is beneficial when considering resource constrained devices employed in telemedicine services. On the other hand, the analysis shows considerable superiority of the proposed technique in image compression efficiency and image quality (compression ratios from 1.166 to 1.703; higher PSNR compared to conventional techniques). But there are some weaknesses, namely computational complexity in relation to processing large amounts of data and information loss related to the quality of images in detailed medical diagnostics. Future research could explore how to maximize computational efficiency for handling big data, study a combination of both lossy and lossless compression methods, incorporate advanced encryption algorithms such as quantum encryption for improved encryption strength, investigate the real performance of the system in telemedicine, implement AI in image analysis, and adopt the technology to other types of medical tests.

References

[1] Abdalla, I. H., & Yaser, R. F. (2023). WSN recruitments for encrypted medical image transmission securely. *Journal of Discrete Mathematical Sciences &amp*, 1981-1990.

[2] Abdulbaqi, A. S., Obaid, A. J., & Mohammed, A. H. (2021). ECG signals recruitment to implement a new technique for medical image encryption. *Journal of Discrete Mathematical Sciences and Cryptography*, *24*(6), 1663-1673. https://doi.org/10.1080/09720529.2021.1884378

[3] Ajagbe, S. A., Florez, H., & Awotunde, J. B. (2022, October). AESRSA: a new cryptography key for electronic health record security. In *International conference on applied informatics* (pp. 237-251). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-19647-8_17

[4] Al-Rubbiay, F. H., Youssef, A. Y., & Mahmood, S. D. (2023, March). Medical image authentication and restoration based on mCloud computing: Towards reliant medical

digitization era. In *Doctoral Symposium on Computational Intelligence* (pp. 487-500). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-99-3716-5_40

[5] Azbeg, K., Ouchetto, O., & Andaloussi, S. J. (2022). BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security. *Egyptian informatics journal*, *23*(2), 329-343. https://doi.org/10.1016/j.eij.2022.02.004

[6] Casola, V., Castiglione, A., Choo, K. K. R., & Esposito, C. (2016). Healthcare-related data in the cloud: Challenges and opportunities. *IEEE cloud computing*, *3*(6), 10-14. https://doi.org/10.1109/MCC.2016.139

[7] Charfi, S., El Ansari, M., Ellahyani, A., & El Jaafari, I. (2022). Ulcer and red lesion detection in wireless capsule endoscopy images using CNN. In *Convolutional Neural Networks for Medical Image Processing Applications* (pp. 91-108). CRC Press.

[8] Chavero-Pieres, M., Viola, M. F., Appeltans, I., Abdurahiman, S., Gsell, W., Matteoli, G., ... & Boeckxstaens, G. (2023). Magnetic resonance imaging as a non-invasive tool to assess gastric emptying in mice. *Neurogastroenterology & Motility*, *35*(2), e14490. https://doi.org/10.1111/nmo.14490

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

[10] Gupta, S., Kalaivani, S., Rajasundaram, A., Ameta, G. K., Oleiwi, A. K., & Dugbakie, B. N. (2022). [Retracted] Prediction Performance of Deep Learning for Colon Cancer Survival Prediction on SEER Data. *BioMed Research International*, *2022*(1), 1467070. https://doi.org/10.1155/2022/1467070 https://doi.org/10.47974/JDMSC-1838

[11] Huang, D., Gao, F., Tao, X., Du, Q., & Lu, J. (2022). Toward semantic communications: Deep learning-based image semantic coding. *IEEE Journal on Selected Areas in Communications*, *41*(1), 55-71. https://doi.org/10.1109/JSAC.2022.3221999

[12] Kumari, T., Singh, D., & Singh, B. (2024). Multi-chaotic maps and blockchain based image encryption. *Concurrency and Computation: Practice and Experience*, *36*(14), e8092. https://doi.org/10.1002/cpe.8092

[13] Kurka, D. B., & Gündüz, D. (2021). Bandwidth-agile image transmission with deep joint source-channel coding. *IEEE Transactions on Wireless Communications*, *20*(12), 8081-8095. https://doi.org/10.1109/TWC.2021.3090048

[14] Lalitha, S., Sanjana, T., Bhavana, H. T., Bhan, I., & Harshith, G. (2022). Medical imaging modalities and different image processing techniques: State of the art review. *Disruptive Developments in Biomedical Applications*, 17-36. https://doi.org/10.1201/9781003272694-3

[15] Mahmood, S. D., Drira, F., Mahdi, H. F., Aribi, Y., & Alimi, A. M. (2023, October). Chaotic model-based blind watermarking with lsb technique for digital fundus image authentication. In *2023 International Conference on Cyberworlds (CW)* (pp. 395-402). IEEE. https://doi.org/10.1109/CW58918.2023.00068

[16] Manju Bala, P., Rajmohan, R., Ananth Kumar, T., Ajagbe, S. A., & Adigun, M. O. (2024). Quantum blockchain-oriented data integrity scheme for validating clinical datasets. https://doi.org/10.1049/PBHE060E_ch13

[17] Masood, F., Boulila, W., Alsaeedi, A., Khan, J. S., Ahmad, J., Khan, M. A., & Rehman, S. U. (2022). A novel image encryption scheme based on Arnold cat map, Newton-Leipnik system and Logistic Gaussian map. *Multimedia Tools and Applications*, *81*(21), 30931-30959. https://doi.org/10.1007/s11042-022-12844-w

[18] MIMIC-CXR Database: https://www.kaggle.com/search?q=MIMIC-CXR+Database

[19] Miriam, H., Doreen, D., & Rene Robin, C. R. (2023). Secured Cyber Security Algorithm for Healthcare System Using Blockchain Technology. *Intelligent Automation & Soft Computing*, *35*(2). https://doi.org/10.32604/iasc.2023.028850
[20] Neela, K. L., & Kavitha, V. (2023). Blockchain based Chaotic Deep GAN Encryption scheme for securing medical images in a cloud environment. *Applied Intelligence*, *53*(4), 4733-4747. https://doi.org/10.1007/s10489-022-03730-x
[21] Peng, X., Qin, Z., Huang, D., Tao, X., Lu, J., Liu, G., & Pan, C. (2022, December). A robust deep learning enabled semantic communication system for text. In *GLOBECOM 2022-2022 IEEE Global Communications Conference* (pp. 2704-2709). IEEE. https:/ /doi.org/10.1109/GLOBECOM48099.2022.10000901
[22] Shadab, S. A., Ansari, M. A., Singh, N., Verma, A., Tripathi, P., & Mehrotra, R. (2022). Detection of cancer from histopathology medical image data using ML with CNN ResNet-50 architecture. In *Computational Intelligence in Healthcare Applications* (pp. 237-254). Academic Press. https://doi.org/10.1016/B978-0-323-99031-8.00007-7
[23] Soffer, S., Morgenthau, A. S., Shimon, O., Barash, Y., Konen, E., Glicksberg, B. S., & Klang, E. (2022). Artificial intelligence for interstitial lung disease analysis on chest computed tomography: a systematic review. *Academic Radiology*, *29*, S226-S235. https://doi.org/10.1016/j.acra.2021.05.014
[24] Tiwari, P., Pant, B., Elarabawy, M. M., Abd-Elnaby, M., Mohd, N., Dhiman, G., & Sharma, S. (2022). Cnn based multiclass brain tumor detection using medical imaging. *Computational Intelligence and Neuroscience*, *2022*(1), 1830010. https://doi.org/10.1155/2022/1830010
[25] Tung, T. Y., & Gündüz, D. (2023, May). Deep joint source-channel and encryption coding: Secure semantic communications. In *ICC 2023-IEEE International Conference on Communications* (pp. 5620-5625). IEEE. https://doi.org/10.1109/ICC45041.2023.10278612
[26] Xie, H., Qin, Z., Li, G. Y., & Juang, B. H. (2021). Deep learning enabled semantic communication systems. *IEEE transactions on signal processing*, *69*, 2663-2675. https://doi.org/10.1109/TSP.2021.3071210
[27] Ye, C., & Chen, C. (2023). Secure medical image sharing for smart healthcare system based on cellular neural network. *Complex & Intelligent Systems*, *9*(2), 1653-1670. https://doi.org/10.1007/s40747-022-00881-9

Authors Biography

Raghda Salam Al Mahdawi obtained a B.Sc. in the Department of Computer Engineering from the college of Engineering., University of Diyala, Iraq in 2007. Also carried out a master's degree in computer applied technology at University of Huazuing University of Science and Technology (HUST), China, 2016. The Research interest are computer networks, Image processing, Software Engineering, computer applied technology, Information Security and Information technology.

Warqaa Shaher Alazawee received a bachelor's degree in computer engineering from the University of Diyala/Iraq in 2007 and then worked as an Engineer at the University of Diyala/College of engineering from 2008 until the year 2012, and then she obtained a scholarship to get a master's degree from the United States of America which was awarded in 2015 in computer engineering from Western Michigan University in the United States of America. After that, she worked as a lecturer at the University of Diyala/College of engineering until now. During this period, she has published in journals and at international conferences. Her research interests are focused on: (Computer Architecture, Image processing, medical image analysis, Biomedical Signal Processing).

Marwa Subhi Ibrahim obtained a B.Sc. in the Department of Computer Engineering from the college of Engineering, University of Diyala, Iraq in 2007. Also carried out a master's degree in computer engineering, University of Aliraqia, Iraq, 2023. The research interests are computer networks, Image processing, Software Engineering, computer applied technology, Information Security and Information technology.