Secure and Low-Complexity Medical Image Exchange Based on Compressive Sensing and LSB Audio Steganography

Wafaa Al-Chaab[1], Zaid Ameen Abduljabbar[2, 3, 4*], Enas Wahab Abood[1], Vincent Omollo Nyangaresi[5], Hussein M. Mohammed[6], Junchao Ma[7*]
[1]Department of Mathematics, College of Science, University of Basrah, Basrah 61004, Iraq
[2]Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah 61004, Iraq
[3]Technical Computer Engineering Department, Al-Kunooze University College, Basrah 61001, Iraq
[4]Huazhong University of Science and Technology, Shenzhen Institute, Shenzhen, 430074, China
[5]Jaramogi Oginga Odinga University of Science & Technology, Bondo 40601, Kenya
[6]Department of Computer Science, Shatt Al-Arab University College, Basra 61001, Iraq
[7]College of Big Data and Internet, Shenzhen Technology University, Shenzhen 518118, China
E-mail: wafaa.khudhair@uobasrah.edu.iq, zaid.ameen@uobasrah.edu.iq, enas.abood@uobasrah.edu.iq, vnyangaresi@jooust.ac.ke, husseinmazen@sa-uc.edu.iq, majunchao@sztu.edu.cn
*Corresponding author

Keywords: **i**mage compression, compressive sensing, securing medical images, moore-penrose pseudo-inverse

Received: January 20, 2023

Patients' data constitutes the vast majority of information exchanged over the Internet. The magnitude of maintaining its security and privacy directly correlates to the importance and privacy of the patients themselves. The manipulation of this data negatively impacts the patient's life and treatment, thus the researchers were inclined to find solutions for this confidentiality challenge by concealing the data to prevent unauthorized access. The process of data concealment is more complex when dealing with large amounts of data. Often, the proportions of the medical image are sizable, which creates challenges when compressing data while maintaining high accuracy. In this paper, a system for securing and compressing medical images based on the Compressive Sensing (CS) principle is presented. The medical image is divided into 8×4 sub-matrices that are multiplied by a 3×8 sensor matrix consisting of Gaussian random numbers. The proposed solution reduces the image's original size by about 30% and conceals it as a random distribution inside an audio (wav) file for more security, using the LSB technique for low complexity. For reconstruction, the sensed image is multiplied by the pseudo-inverse of Moore-Penrose. The statistical analysis proved the efficacy of the system in compression and recovery with reduced cost and time consumption, combined with reduced distortion of the cover file; it was also judged to be increasingly efficient compared to previous research.

Povzetek: V tem članku je predstavljen sistem za varovanje in stiskanje medicinskih slik na principu kompresijskega zaznavanja (CS).

1 Introduction

Medical imaging performs a crucial role in the medical field, particularly in the process of diagnosis, biomedical research, and telemedicine which is centered on imaging such as X-ray, ultrasound, Computed Tomography (CT) and Magnetic Resonance Imaging (MRI) [1]. Currently, telehealth applications such as remote surgery and remote consultation depend on the transmission of medical images between doctors, examination centers, and patients through an insecure communication medium [2]. This increases the chances of images being disclosed to third parties, which impacts patient confidentiality, and the potential for images to be modified, which impacts the integrity of the images. If a transmitted image is obtained and altered by anyone, it has the potential to cause life-threatening problems such as misdiagnosis [2][3]. Many methods have been proposed involving the transmission of secure data concealed in unsecured media like normal images, video or even text messages, most notably encryption and steganography [3]. Since the mid-1990s, many image security technologies have been introduced. Several encryption schemes such as RSA, Data Encryption Standard (DES), and International Data Encryption Algorithm (IDEA) have emerged which, although successful in securing traditional images, are not suitable for the objective of medical image encryption, due to their large data sizes, and proprietary storage format [4][5].

In 2006, Donoho et al., [6] proposed a new compression scheme known as compressive sensing. This scheme was based on the sparseness principle of signal, and utilized the measured values of the sensed signal to reconstruct the original signal, owing to the measured values being smaller than the Nyquist sampling rate. Any image can be defined as a two-dimensional signal, therefore, when compressive sensing is applied to an image as an encryption technique, it may also be resampled, compressed, and simultaneously encrypted [7]. Crucially, to reconstruct the image again, only a portion of the key information will need to be exchanged between the sender and the receiver [8].

In the encryption process, the message is transformed into an indecipherable format, known as a cipher message, which enables confidentiality, integrity, and authenticity [9]. The image encryption process transforms the classified image into a noisy image, which makes it suspicious and increases the possibility of detection. Based on this, another method has been proposed to further preserve the confidentiality of the image, which is the concealment of confidential information in standard, meaningful files, and many studies have proposed the implementation of this technique [10]. In the spatial domain, many techniques have been created for information concealment, but the most implemented technique is LSB. In an LSB algorithm, the least significant fragments of the confidential files are merged with sections of the cover file which may be an image or an audio file [9][11]. One of the most significant advantages of LSB is that it takes less time to implement, has a more efficient embedding ability, and uses spatial domain algorithms [12].

In the frequency domain, both the cover file and the secret file are transformed into the frequency domain such as Discrete Wavelet Transform (DWT) or Discrete Cosine Transform (DCT) and the confidential parameters are combined with the relevant coefficients in the cover, to achieve the required combination [13]. DWT and DCT require high computational complexity to complete the masking process. Fusing image encryption with an effective concealment process enables high levels of security when transmitting sensitive images over a public channel. A long encrypted message, however, may cause the cover file to be distorted, resulting in the need to encrypt and compress the image before embedding [14][15].

In this paper, a hybrid system to ensure the confidentiality of medical images is presented. This process consists of two stages: firstly, the medical image was encrypted and compressed using the compressed sensing method, which is based on the principle of employing the pseudo-inverse to reduce the size of the samples and alter them by multiplying them with a suitable sensing matrix. The compression process was carried out at a high-to-medium ratio. The second stage used the audio steganography technique to obscure the compressed image by including it within a wav file, via the use of the LSB method.

This research aims to provide a method for compressing and securing medical images with high compression rates of 30%, resulting in excellent levels of effectiveness in terms of computation cost, greater masking capacity, and storage requirements. The compression method used is based on the CS and steganography, which are based on a scattering of data to be concealed, using LSB, which are both computationally fast and simple, making the system faster and more secure. In addition, the cost of communication is reduced due to data compression. Consequently, this method is suitable for use on constrained technology such as smart devices.

This research is organized in the following way. Section two analyses related works and section three details the methodology of the compressed sensing technique and LSB. The proposed method is introduced in section four, followed by section five which examines the implementation results, statistical analysis and comparison with previous works. The final section contains the conclusion.

2 Related works

Currently, many algorithms have been developed for image encryption [16], such as chaos-based algorithms, which contain properties such as unpredictability and sensitivity which make them a solid choice for distortion [17]. In 2015, Bao and Zhou [18] proposed an encryption scheme for images by inserting them into a visually meaningful cover imag. In 2016, Thenmozhi [19] proposed a system based on the SPIHT method of lossless compression to achieve image security, whereby the compressed image is encoded within a cover image through the use of the LSB method. The disadvantage of the SPIHT algorithm is that it requires a sizeable amount of memory for the size of the three lists, which is often large, and it demands repeated access to all lists, which consumes extensive time when encoding and compressing the image [20].

In 2017, Kanso and Ghebleh [21] presented a lossless, visually meaningful image encryption scheme, as an improvement for Bao and Zhou's algorithm, by adding distortions to the cover file to make it undetectable. In 2018, Hossam [5] introduced a method for an imaging cryptosystem that dynamically manipulates the image pixels by relying on simultaneous permutation and diffusion functions. This system used the Chebyshev-Chebyshev map to mix the information of the plain image and conceal image pixels through the employment of a modified logistic map and a chaos system to create different key streams for each confidential image. Unfortunately, this system can be less effective due to the complexity of the chaos system and Chebyshev polynomials [22]. In the same year, Nematzadeh e. al. [23], the authors presented a medical, image-encryption system based on genetic algorithms, combined with coupled map lattices. The coupled map is employed to generate pseudo-random numbers as the initial population for the genetic algorithm.

In 2022, Obaid et al. [4], a hyper Image Encryption framework, based on chaos, was proposed for securing sensitive images transmitted via the cloud. This framework applies encryption operations or image scrambling techniques according to the intensity and type of cyberattack taking place.

Combining with steganography, in 2007, Chang et al. [11] presented a lossless and reversible steganography system for securing images. It is a Discrete Cosine Transformation (DCT) system which is used to conceal the confidential sections in the consecutive zero coefficients of the DCT transform. In 2020, Noah et. al. [24] presented an enhanced blowfish algorithm for securing medical information such as text and images. The researchers used the F-function to generate resilient, round sub-keys that could better withstand attacks. The enhanced algorithm presented a better implementation time than the existing blowfish algorithm. In 2020, Chai et al. [25] proposed an efficient, visually meaningful image compression and encryption technique based on Compressive Sensing (CS) and (LSB) as steganography containing random embedding. A three-dimensional cat map was invested to generate the sensing matrix and hiding locations and the (DWT) was used to form the transformation matrix for sensing system. In 2020, G. Ye et. al. [8] proposed an image encryption algorithm based on CS and information masking, they used the discrete wavelet transform (DWT) to sparse the secret image as well for carrier image, then the image is compressed and encrypted by compressive sensing. The sensing matrix is generated by complex tent-sine system. A singular value decomposition operation was added such that the singular values of the carrier image are used to hold the singular values of the secret image. Both [25][8] require expensive processing time due to the use of DWT.

In 2021, Priyadharshini et al. [1] proposed a system employing cryptography and steganography for the safeguarding of medical images: the system first encrypts the image using a one-time pad algorithm, then uses an LSB technique for hiding the encrypted image in a cover file that is also an image. A one-time pad encryption algorithm is a symmetric key encryption approach which was proposed by Joseph Mauborgue. It is based on XOR-operation between a key and a secret message. The key is used only once per message. In the same year, Moya-Albor et. al. [3] proposed an encryption algorithm for medical images which was based on the Jigsaw transform, Langton's ant, and cyclic permutation, with the addition of a deterministic noise. Also, in the same year, Ogundokun [26] proposed the implementation of an enhanced Least Significant Bit (LSB) method for solving the crucial authentication issue. The system used a logical bit shift operation for hiding medical images with less noise in the cover image. All works [1][3][26] require high masking capacity, as they did not compress medical images, which are known to have large sizes. Also, such image sizes without compressing them may affect the distortion of the masking medium

The most common limitations of the aforementioned works are the complexity of computational cost, bandwidth and storage requirements. Furthermore, the requirements of high-resolution images are ineffective and unsuitable for practical applications where the carrier images appear distorted as if concealing something, and this problem is commonplace among other studies [11][21][27], especially when including high-resolution images such as medical images.

In this study, a hybrid encryption mechanism is presented that combines CS and steganography to secure medical images. The image is compressed and then hidden, which reduces the space required for storage, high masking capacity and decreases the distortion of the cover file. The compression method is computationally economical and less time-consuming due to its implementation of the high speed and uncomplicated multiplication operation for finding the pseudo-inverse and reconstruction [27].

Steganography, based on scattered LSB, is considered to be one of the fastest and simplest computational methods, which results in an efficient and secure system [9]. Table 1 includes a summary of the related works, their schemes, aims, and results.

Table1: Summery of the most related works.

Reference	Goals	Scheme	Results
[1] A. Priyadharshini et.al. 2021	Cryptography and steganography for the securing medical images	- One-time pad encryption algorithm XOR-operation - LSB technique	The results of the combined protection system are very good
[3] E. Moya-Albor *et al. 2021*	Encryption algorithm for Secure medical image	Encryption system based on Langton's ant and jigsaw transform	Flat histograms for encrypted pictures reflect the ability of the system for protection.
[4] A. J. Obaid et. al . 2022	Securing e-Health application of cloud computing	-Hyper Chaos Encryption -ANN learning process	The proposed framework has a good potential to resist known and unknown attacks in the image sharing process.
[8] G. Ye, et. al. 2020	A system for image compression and encryption	- CS - discrete wavelet transform (DWT) - Complex tent-sine - Singular value decomposition(SVD)	Strong anti-noise attack, cropping attack, and rotation attack ability
[25] X. Chai et. al. 2020	Visually meaningful	- Compressive Sensing	Robust to known-plaintext and chosen-

	image compression and encryption technique	(CS) - LSB - DWT	plaintext attacks.
[31] C. Zhang . et. al .2014	Object reconstruction of ghost imaging	- Pseudo-Inverse - DCT	PGI method provides an effective improvement
[24] N. O. Akande and C. O. Abikoye . 2019	Securing medical text and image information	-A modified blowfish algorithm -F-function	The enhanced algorithm is sensitive to changes in its key and it resistive to differential attacks with less time than the existing blowfish algorithm.
[12] K. Dasgupta et. al. 2014	A echnique for hiding data in digital images	- Chaos theory -LSB	Provides added security to the base steganography technique
[17] L. M. H. Yepdia and A. Tiedeu, 2020	Securing the Transmission of Medical Images	- Chaotic maps - Logistic-May (LM) and Henon maps and Logistic-Sine(LS) - Cramer’s rule	Good encryption and fast performance
[10] X. L. H. Wang et. al. 2019	Secure image encryption	Logistic-Tent system - 3-D Cat map	Good concealing and satisfactory recovery quality

All the schemes and approaches produced in Table1 approved a good efficiency in securing data but it is noteworthy to mention its cons such as [25][8][3][4][31] are requiring expensive processing time and complexity due to the use of DWT, DCT or some are incapable to secure crucial information about the patient like their health state. In [24][10][1] the global key-space is too long for high-resolution images.

The chaotic system that invested in [17][12][4] is suffering from sensitivity to the initial values and parameters and slower, Complex, difficult to implement with high resolutions and high computational cost

In view of all the above defects, we proposed a simple but effective system for protecting and securing medical data as well as compressing it, as it achieves both security and reduces storage space, and it is characterized by fast implementation due to its reliance on the pseudo-inverse mechanism and LSB.

3 Methodology

A. Compressive sensing

Compressive sensing attracted increased attention due to its ability to perform image operations, such as sampling, compression, and encryption, simultaneously [8]. Compressive sensing is based on three critical keys: sparsity, uncorrelated observation, and reconstruction of signals [8][28]. CS can be formulated with a linear system of equations, where the number of equations is not required to be equal to the number of variables [29], which is mathematically represented as:

$$Y = TX \qquad (1)$$

where the signal $X_{n\times 1} \in R^n$, which was multiplied by measurement matrix $T_{m\times n}$ to produce the sensed signal y with m-length $\in R^m$ [27][30].

Because the number of equations is not equal to the variables, there are infinite probable solutions. The possible true solution for vector X may be obtained with new techniques such as non-deterministic CS, optimization techniques, the metaheuristic evolutionary technique or linear programming (LP) [29].

Remark 1: the proposed work was designed to secure medical images through encryption and compression using the CS technique. The CS technique stated that the image is multiplied with an appropriate sensing array. To ensure that the signal is retrieved with the least possible data loss, a technique derived from linear algebra was used, known as the pseudo-inverse, which is computationally inexpensive [31][32], uncomplicated and provides excellent retrieval results.

B. Moore-Penrose pseudoinverse

The Moore-Penrose pseudo-inverse is one of the most well-known methods employed, in linear algebra, to find matrix inverse T^+ of a matrix - T in cases of non-squared matrix [33] which was proposed firstly by E. H. Moore in 1920 [34][35].

The pseudo-inverse can be calculated with the singular value decomposition SVD for all matrices of any type of number (real, integer or complex) [36].

Having $T \in R^{mxn}$, a pseudoinverse of Matrix T is T^+ which fulfills four criteria (the Moore–Penrose terms):

1- $T^+T = T$

2- $T^+TT^+T = T^+$

3- $(TT^{+})^{T} = TT^{+}$
4- $(T^{+}T)^{T} = T^{+}T$

Where T^{+} is the inverse of T, TT^{+} and $T^{+}T$, called the Hermitian conditions, while the two last conditions are the uniqueness property of the inverse T^{+} [36].
For reconstruction to the signal X in a linear system:

$$X = T^{+}Y \qquad (2)$$

Where T^{+} is computed with Moore-Penrose in two possible relations:

$$T^{+} = T^{T}(T^{T}T)^{-1} \qquad (3)$$

TT^{+}=I, the Moore-Penrose pseudoinverse, is characterized by its lower requirements and the simplicity of implementation and its complexity is suitable *O(mn)* [32]. It provides the most suitable approach for systems that have multiple solutions; therefore it was used in the proposed system.
Remark 2: Moore-Penrose was used to calculate the pseudo-inverse of the sensing matrix as a retrieval key, after compression and encryption.

C. LSB steganography

A color image consists of pixels, each pixel has three values: red, green and blue in the range of 0-255 (8-bits). The principle of the LSB method is to replace the least significant part of the cover image pixel with one of the secret message bits. LSB will have less effect on the result (1 out of 256 degrees) [1]. Figure 1 shows the mechanism of LSB steganography.

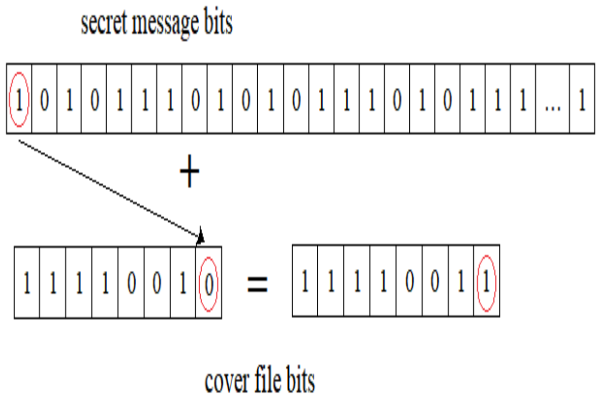


Figure 1. LSB Steganography scheme.

Remark 3: The LSB mechanism was used as low-cost mechanism to hide the sections of the compressed image inside the cover file, which is an audio file (wav).

4 Proposed method

This study presents a system for securing medical images by employing encryption and steganography to achieve integrity and confidentiality. The system operates in two stages: the medical image is ciphered and compressed using a compressive sensing algorithm, and then the cipher image samples are distributed within the cover audio file in a scattered substitution technique. At the receiving end, the recipient extracts the encrypted image from the cover and applies a reconstruction algorithm to retrieve the original image.

4.1 Stage 1: Securing the image via two algorithms

A. Image Compression and encryption

The initial step is to compress the image, by dividing it into frames of pixels, which will be multiplied with a key (sensing matrix) to get compressed image which will be ciphered as an algorithm:

CS Algorithm 1
- Input: X is a medical image.
- Input: K is the sensing matrix $K_{h\times n}$.
- Divide X into sub-matrices with size sub_$X_{n\times m}$, where both h, m less than n.
- Multiply the key K by each sub_X to get $KX_{h\times m}$.
- Collect the sub_X metrics to form one compressed image X_comp.
- Output: X_comp which is the compressed image.

Example:
sub_X=[138 67 40 42; 129 70 41 41;
117 75 43 37; 106 82 48 34;
103 88 54 33; 106 94 60 35;
114 97 66 38; 120 101 70 40] $_{8\times 4}$
K=[1 2 3 4 5 6 7 8;3 4 2 5 6 8 2 7;9 8 7 6 5 4 3 2] $_{3\times 8}$
KX=K*sub_X=[4080 3251 2095 1332
4228 3222 2036 1368
5250 3489 2125 1668]$_{3\times 4}$

Remark: The resulting matrix is almost 0.3 in size of the original.

B. LSB (Less Significant Bit) steganography

Each bit of the compressed image is replaced by the least significant bit of the audio cover file samples, as stated in algorithm 2. The cover file consists of audio samples, each with the range [1, -1] in the 2^{16} coding.

Stego Algorithm 2:
- Input: XK is the compressed image.
- Input: A is the audio cover file.
- Convert pixels of XK into binary encoding.
- Generate random positions in A for hiding.
- Take each value of 2 bits of the XK pixel and randomly substitute it in 2 LSBs of the sample of A.
- Output: A is the resulting steganography audio file.

4.2 Stage 2: Extraction and reconstruction

To extract the sensed image, the cover file is re-converted to binary encoding and each pair of LSB adjacent bits is acquired and combined to form the compressed image pixels again, as in algorithm 3. For reconstruction (which represents a step for decryption too), the sensed image is re-divided into partial images in the HMX dimension and then multiplied by the pseudo-inverse, as calculated by equations (Eq.2) and (Eq.3) to reacquire the original image, stated in algorithm 4.

A: Extraction Algorithm 3

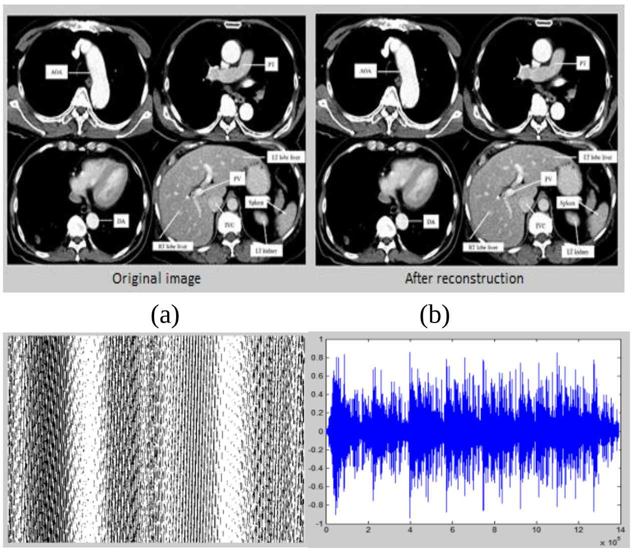
- Input: the steganography audio file A.
- Convert A to binary encoding
- Each pair of LSB adjacent bits are taken and combined to form the compressed image pixels again XK.
- Output: compressed image XK.

B: Reconstruction Algorithm 4

- Input: The XK file.
- XK is re-divided into partial images in the HMX dimension sub-XK.
- Each sub-XK is multiplied by the pseudo-inverse, calculated by equations (2) and (3) to re-form the original sub-image.
- Gathering sub-images to form the original image X.
- Output: original image X.

5 Experimental results and discussion

To test the efficiency of the proposed method, several medical images, of the type MCI and CT were tested with different resolutions, ranging from (300×168 to 2028×2914), taken from [37] and [38]. the images were compressed with a compression ratio of 30%, as shown in Figure2.



(a) (b)

(c) (d)

Figure 2. An image of CT with resolution 1192×1984 (a) and (b) before and after compression, (c) the compressed image and (d) the audio cover file.

Figure 2 displays the CT image, before and after being reconstructed at a 30% rate, while the masking proposed scheme was tested using various audio signals, such as speech, songs and music with different sample frequencies ranging from 11-48 kHz. The software was conducted on an Intel® Core i7-4520M CPU 2.90 GHz 4.00 GB RAM using a MATLAB R2020a. The reconstructed image was virtually indistinguishable from the original one. This indicates the system's ability for retrieval, which has relied on the Moore-Penrose pseudo-inverse.

Furthermore, statistical analysis tests were implemented to estimate the reconstruction quality of the method when using a compression rate of 30%. Although the system can compress at more than 30%, the PSNR values are close to the range of 29-32 dB. Unfortunately, the retrieved image is visually blurred, and, therefore, this study adopted a compression rate of 30%. The results of which are detailed below.

5.1 Elapsed time and compression rate

The proposed system achieves encouraging results in time cost for reconstruction and compression implementation. Many different-sized images for CT and MIR were compressed with 30% compression rates. The number of compression file samples decreased steadily, as shown in Table 2.

Table2. Time consumption and compression rate.

File	**File resolution**		**Time (s)**	**Compression rate**
	Before	After		
CT1	2028×2914	1286×1400	5.901	30%
CT2	1192×1984	821×823	4.526	28%
CT3	186×300	102×141	0.08	28%
MIR1	261×360	150×178	0.1	28%
MIR2	420×540	210×308	0.3	28.5%
MIR3	1106×1300	600×684	2.01	28.5%

The Table 2 shows the relatively low execution time, given the use of LSB and CS, its suitability for smart devices and online systems and the suitability of the compression ratio.

5.2 Pearson correlation analysis

It is one of the significant criteria for evaluating the correlation and similarity between images in encryption and recovery systems, and it is known by the following equation:

$$R = \frac{\sum_1^n \left(x_i - \underline{x}\right)\left(y_i - \underline{y}\right)}{\sqrt{\sum_1^n \left(x_i - \underline{x}\right)^2 \sum_1^n \left(y_i - \underline{y}\right)^2}} \qquad (4)$$

Where x_i represents the sample value of the original matrix, $\underline{x}$ is the mean of the samples, y is the matrix to measure the correlation with, and here represents the image after its restoration and construction, while r is a real number in the range 1-0 to determine the degree of congruence, 1 is identical and 0 is different [17].

5.3 PSNR and MSE analysis

This is a metric for evaluating the recovery ability and the extent of image noise after recovery, based on a calculation of peak signal-to-noise ratio (PSNR) and the normalized mean square error (MSE) [39]. It is calculated by:

$$MSE = \frac{\sum_{i=0}^{m-1}(X_i - Y_i)^2}{m} \qquad (5)$$

$$PSNR = 10 * log_{10}\left(\frac{Max_X^2}{MSE}\right) \qquad (6)$$

Where X is the original image and Y is the image after restoration.

5.4 Structural similarity index (SSIM)

SSIM is a perceptual scale for measuring matrix, quality distortion resulting from processing operations, such as encryption or compression. It was used in this paper to evaluate the ability of the system to rebuild the signal after compression, as given by:

$$SSIM = \frac{(2\underline{x}\underline{y} + c_1)(2\sigma xy + c2)}{(\sigma x2 + \sigma y2 + c2)(\underline{x}\ 2 + \underline{y}2 + c1)} \qquad (7)$$

Here c_1= $(Z_1L)^2$, and c_2= $(Z_2L)^2$ are constant; L is 255 which is the highest range of the image sample values; Z_1 and Z_2 are 0.01 and 0.03 respectively. The score is ranged between [-1,1], thus 1 for identical matrices and decreasing to −1 as they change [40].

Table 3 demonstrates that the compression ratio was 30% and was employed for images of different resolutions (i.e., the compressed image was 0.3 of the original size). The proposed work implementation for the SSIM, PSNR, and correlation metrics reflected relatively good results. The PSNR scored 25-45 dB, and the SSIM was in the range of 0.77-0.9, indicating a good recovery; the correlation value was almost 0.9 which indicates satisfactory results [41]. Through the use of the criteria, the proposed system proved its effectiveness in terms of time consumed and reducing the volume in implementation as stated in Table 1, and the recovery accuracy was within the expected parameters.

Table3. Objective measures of reconstructed speech quality with DFT as on sparse basis.

File	**File resolution**		**PSNR**	**SSIM**	**R**	**Compression rate**
	Before	**After**				
CT1	2028×2914	1286×1400	45.7	0.9054	0.98	30%
CT2	1192×1984	821×823	38.06	0.86	0.99	28%
CT3	186×300	102×141	27.44	0.78	0.9709	28%
MIR1	261×360	150×178	27.89	0.77	0.93	28%
MIR2	420×540	210×308	24.8	0.7902	0.911	28.5%
MIR3	1106×1300	600×684	25.33	0.83	0.985	28.5%

5.5 Comparisons with other proposed work

Compared to previous works, the research registered high effectiveness in securing medical images using the CS technique and hiding with the LSB method. In addition to image encryption, the CS method reduces the size of the image while preserving the accuracy of its details and information upon retrieval. These two methods have a low cost in both calculations and time. The proposed system overcomes the problems that existed in previous works, as well as its confrontation with various attacks also its speed of implementation, and fewer requirements made it suitable for network devices.

Table4. shows the results of comparison with the papers [8] and [25] by implementing the proposed system on 256 × 256 images, and the result in terms of time and PSNR was as follows:

Table4: comparison of the proposed system and Guodong Ye et. al.[8] by Time and PSNR values at a compression rate 28%.

Image file	**File size (sample/ frame)**	**Ref.[8]**		**Proposed**	
		Time	**PSNR**	**Time**	**PSNR**
bridge	256×256	2.05	26	0.1	27

lake	256×256	2.1	23	0.03	25.08
Building	256×256	2.2	21.42	0.03	24.9
Lena	256×256	2.04	22.45	0.05	26.01
Babon	512 ×512	11.1	24.94	0.12	31
Lena	1024×1024	10.94	30.1	1.05	33

Table5: comparison of the proposed system and C. Xiuli [25] by Time and PSNR values at a compression rate 28%.

Image file	**File size (sample /frame)**	**Ref.[25]**		**Proposed**	
		Time	**PSNR**	**Time**	**PSNR**
bridge	256×256	1.103	25.1	0.1	27
lake	256×256	1.12	26.09	0.03	25.08
Building	256×256	1.095	25.97	0.03	24.9
Lena	256×256	1.74	26.5	0.05	26.01
Babon	512 ×512	10.9	34	0.12	31
Lena	1024×1024	8.03	35	1.05	33

The system was compared using identical images that were used in the two comparison papers [8][25], and the PSNR values and the time between the original image, and the image after decompression, were calculated. It is clear from Table 4 and 5 that the PSNR values differ according to the image, although the size and time are fixed. The reason may be that the cover file of the compressed image may affect the quality of the reconstructed images [25]. The results also indicate that the proposed solution is successful in terms of implementation time and higher levels of efficiency. The consuming time is very low, when compared to other research, due to a reliance on CS and LSB techniques, which makes this research suitable for electronic devices with lower processing cost, while both [8] and [25] are based on CS with DWT, which is computationally complex.

6 Conclusion

This paper presents a system for securing and compressing medical images based on the CS principle. The image is segmented as 8 x 4 sub-matrices. The sub-matrices are then multiplied by a 3 x 8 sensing matrix, consisting of Gaussian random numbers. The compression method is represented by a linear system Y=AX and can be resolved to retrieve X, by calculating A-1 using the Moore-Penrose pseudo-inverse, which is easy-to-implement and a low-cost method with reduced time consumption, while providing improved compression, an acceptable safety rate and simple complexity. The compressed file is hidden in a random distribution, within an audio file, for more security. The statistical analysis measures and implementation results demonstrate the reliability of the proposed work, suitability of the compression ratio, and buildability of a good quality signal, as indicated by SSIM and correlation coefficients, which are very close to one. The PSNR was within an acceptable range. The results of this research were comparable with previous systems, demonstrating the efficiency of the proposed solution.

Acknowledgement

This work is supported by Natural Science Foundation of Top Talent of SZTU (grant No. 20211061010016).

References

[1] A. Priyadharshini, R. Umamaheswari, N. Jayapandian, and S. Priyananci, "*Securing medical images using encryption and LSB steganography*," *Proc. 2021 1st Int. Conf. Adv. Electr. Comput. Commun. Sustain. Technol. ICAECT 2021*, 2021, doi: 10.1109/ICAECT49130.2021.9392396.

[2] Jose Conde, Suvranu De, Richard W Hall, Edward Johansen, Dwight Meglan, Grace C Y Peng, "*Telehealth Innovations in Health Education and Training*," *Telemed. e-Health*, pp. 103–106, 2010. doi.org/10.1089/tmj.2009.0152.

[3] E. Moya-Albor *et al.*, "*Secure medical image encryption approach based on Langton's ant and jigsaw transform*," vol. 9, no. December, p. 59, 2021, doi: 10.1117/12.2606294.

[4] A. J. Obaid, P. Malik, R. Sharma, S. Khatak, A. Dumka, and R. Singh, "*Securing e-Health application of cloud computing using hyperchaotic image encryption framework*," vol. 100, no. May, pp. 1–7, 2022. doi.org/10.1016/j.compeleceng.2022.107860.

[5] H. Diab, "*An Efficient Chaotic Image Cryptosystem Based on Simultaneous Permutation and Diffusion Operations*," *IEEE Access*, vol. 6, pp. 42227–42244, 2018, doi: 10.1109/ACCESS.2018.2858839.

[6] D.L.Donoho, "*Compressed sensing*," *IEEE T. Inform. Theory 52*, pp. 1289-1306., 2006. doi.org/10.1109/tit.2006.871582.

[7] W. S. and M. B. Prter Gerstoft, Christoph F. Mecklenbrauker, "*introduction to compressive sensing in acoustics*." The journal of the Acoustical Society of America, pp. 3731–3736, 2018. doi.org/10.1121/1.5043089.

[8] G. Ye, C. Pan, Y. Dong, Y. Shi, and X. Huang, "*Image encryption and hiding algorithm based on compressive sensing and random numbers*

insertion," *Signal Processing*, vol. 172, p. 107563, 2020, doi: 10.1016/j.sigpro.2020.107563.

[9] H. P. Harshita Kapadia, Harawane Sneha Haribau, "*Audio Steganography and Security by using Cryptography*," *Int. J. Comput. Sci. Network*, vol. 4, no. 2, pp. 285–288, 2015.

[10] X. L. H. Wang, D. Xiao, M. Li, Y. Xiang, "*A visually secure image encryption scheme based on parallel compressive sensing*," *Signal Process*, vol. 155, pp. 218–232, 2019. https://www.doi.org/10.1016/J.sigpro.2018.10.001

[11] C. C. Chang, C. C. Lin, C. Sen Tseng, and W. L. Tai, "*Reversible hiding in DCT-based compressed images*," *Inf. Sci. (Ny).*, vol. 177, no. 13, pp. 2768–2786, 2007, doi: 10.1016/j.ins.2007.02.019.

[12] K. Dasgupta, J. K. Mandal, and P. Dutta, "*A Novel Secure Image Steganography Method Based on Chaos Theory in Spatial Domain,"* no. February, 2014, doi: 10.5121/ijsptm.2014.3102.

[13] Yasir A. H., Nada E. T., Mohammed Q. A., " *An Enhanced Approach of Image Steganographic Using Discrete Shearlet Transform and Secret Sharing*." *Baghdad Science Journal*, vol.19, no. 1, : pp:197-207, 2022. http://dx.doi.org/10.21123/bsj.2022.19.1.0197

[14] Sahera A., Najat H. Q., Hamid A.," *Robust Method For Embedding An Image Inside Cover Image Based On Least Significant Bit Steganography*," *Informatica. Vol 46, No 9, 2022,* doi.org/10.31449/inf. v46i9.4362

[15] C. T. Jian, C. C. Wen, N. H. Binti Ab Rahman, and I. R. B. A. Hamid, "*Audio Steganography with Embedded Text,*" *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 226, no. 1, 2017, doi: 10.1088/1757-899X/226/1/012084.

[16] A. Nkandeu, Y. P. K., Mboupda Pone, J. R., & Tiedeu, "*Image encryption algorithm based on synchronized parallel diffusion and new combinations of 1D discrete maps.*," *Sens. Imaging.*, 2020, doi: https:// doi. org/ 10. 1007/ s11220- 020-00318-y.

[17] L. M. H. Yepdia and A. Tiedeu, *Secure Transmission of Medical Image for Telemedicine*, vol. 22, no. 1. 2021. doi.org/10.1007/s11220-021-00340-8.

[18] L. Bao and Y. Zhou, "*Image encryption: Generating visually meaningful encrypted images*," *Inf. Sci. (Ny).*, vol. 324, pp. 197–207, 2015, doi: 10.1016/j.ins.2015.06.049.

[19] D. T. M. M.J.Thenmozhi, "*A New Secure Image Steganography Using LSB And SPIHT Based Compression Method,*" *Int. J. Eng. Res. Sci.*, vol. 2, no. 3, p. pp.80-85., 2016.

[20] A. S. Ritu Chourasiya, "*A Study of Image Compression Based Transmission Algorithm Using SPIHT for Low Bit Rate Application*," *Bull. Electr. Eng. Informatics*, vol. 2, no. 2, pp. 117–122, 2013. doi.org/10.12928/eei.v2i2.214.

[21] M. G. A. Kanso, "*An algorithm for encryption of secret images into meaningful images*," *Opt. Lasers Eng.*, vol. 90, pp. 196–208, 2017, doi: https://doi.org/10.1016/j.optlaseng.2016.10.009.

[22] L. A. Kohda T, Tsuneda A, "*Correlational properties of chebyshev chaotic sequences*," *J TiJ Time Ser Anal*, vol. 21, no. 2, pp. 181–191, 2000. doi.org/10.1111/1467-9892.00180.

[23] V. N. Nematzadeh, H., Enayatifar, R., Motameni, H., Guimar, F. G., & Coelho, "*Medical image encryption using a hybrid model of modified genetic algorithm and coupled map lattices.*," *Opt. Lasers Eng.*, vol. 110, pp. 24–32, 2018. doi.org/10.1016/j.optlaseng.2018.05.009.

[24] Noah Oluwatobi Akande, Christiana Oluwakemi Abikoye, Marion Olubunmi Adebiyi, Anthonia Aderonke Kayode, Adekanmi Adeyinka Adegun, Roseline Oluwaseun Ogundokun, "*Electronic Medical Information Encryption Using Modified Blowfish Algorithm"*, no. January 2020. Springer International Publishing ICCSA 2019, pp: 166:179, 2019, doi.org/10.1007/978-3-030-24308-1_14

[25] X. Chai, H. Wu, Z. Gan, Y. Zhang, Y. Chen, and K. W. Nixon, "*An efficient visually meaningful image compression and encryption scheme based on compressive sensing and dynamic LSB embedding,*" *Opt. Lasers Eng.*, vol. 124, Jan. 2020, doi: 10.1016/j.optlaseng.2019.105837.

[26] R. O. Ogundokun and O. C. Abikoye, "*A Safe and Secured Medical Textual Information Using an Improved LSB Image Steganography*," *Int. J. Digit. Multimed. Broadcast.*, vol. 2021, p. 8827055, 2021, doi: 10.1155/2021/8827055.

[27] S. Yu, R. Wang, W. Wan, L. Du, and X. Yu, "*Compressed sensing in audio signals and it's reconstruction algorithm*," *ICALIP 2012 - 2012 Int. Conf. Audio, Lang. Image Process. Proc.*, no. 1, pp. 947–952, 2012, doi: 10.1109/ICALIP.2012.6376750.

[28] M. Rani, S. B. Dhok, and R. B. Deshmukh, "*A Systematic Review of Compressive Sensing: Concepts, Implementations and Applications*," *IEEE Access*, vol. 6, no. c, pp. 4875–4894, 2018, doi: 10.1109/ACCESS.2018.2793851.

[29] Mahdi Khosravy, Neeraj Gupta, Nilesh Patel, Tomonobu Senjyu, "*Frontier Applications of Nature Inspired Computation*," *Springer,* 2020. doi.org/10.1007/978-981-15-2133-1.

[30] D. Fonseca Resende, M. Khosravy, H. L. M. Monteiro, N. Gupta, N. Patel, and C. A. Duque, *Neural signal compressive sensing*. Elsevier Inc., pp:201: 221 2020. doi.org/10.1016/b978-0-12-821247-9.00016-0.

[31] C. Zhang, S. Guo, J. Cao, J. Guan, and F. Gao, "*Object reconstitution using pseudo-inverse for ghost imaging,*" *Opt. Express*, vol. 22, no. 24, p. 30063, 2014, doi: 10.1364/oe.22.030063.

[32] E. W. Abood, Z. A. Hussien, H. A. KAwi, ..., M. A. Al Sibahee, and S. A. A. Kalafy, "*Provably secure and efficient audio compression based on compressive sensing,*" *Int. J. Electr. Comput. Eng.*, vol. 13, no. 1, pp. 335–346, 2023.

doi.org/10.11591/ijece.v13i1.

[33] C. D. Campbell, S. L.; Meyer, Jr., “*Generalized Inverses of Linear Transformations*,” *Dover. ISBN 978-0-486-66693-8*, 1991.

[34] E. H. Moore, “*On the reciprocal of the general algebraic matrix*,” *Bull. Am. Math. Soc.*, vol. 26, no. 9, pp. 394–95, 1920, doi:10.1090/S0002-9904-1920-03322-7.

[35] A. M. Kanan and Z. A. Zayd, “*Using the Moore-Penrose Generalized Inverse in Cryptography*,” vol. 148, no. August, pp. 1–14, 2020.

[36] Ivan Dokmanic, Mihailo Kolundzija, Martin Vetterli, “*Beyond Moore-Penrose : Sparse Pseudoinverse”, 2013 IEEE International Conference on Acoustics, Speech and Signal Processing.*, pp. 6526–6530, 2013. doi.org/10.1109/icassp.2013.6638923.

[37] “https://www.nih.gov/news-events/news-releases/nih-clinical-center-releases-dataset-32000-ct-images.”

[38] “https://www.aylward.org/notes/open-access-medical-image-repositories.”

[39] M. Zamani, B. A. M. Azizah, M. A. Shahidan, and C. S. Shojae, “*Mazdak technique for PSNR estimation in audio steganography*,” *Appl. Mech. Mater.*, vol. 229–231, no. November, pp. 2798–2803, 2012, doi: 10.4028/www.scientific.net/AMM.229-231.2798.

[40] E. W. Abood, Z. A. Abduljabbar, and M. A. Al Sibahee, “*Securing audio transmission based on encoding and steganography,*” vol. 22, no. 3, pp. 1777–1786, 2021, doi: 10.11591/ijeecs.v22.i3.pp1777-1786.

[41] C. B. Papafitsoros, K., & Schönlieb, “*A Combined First and Second Order Variational Approach for Image Reconstruction.*,” *J. Math. Imaging Vis.*, vol. 48, no. 2, pp. 308–338, 2013, doi: 10.1007/s10851-013-0445-4.