Arabian Journal for Science and Engineering (2023) 48:1757–1770
https://doi.org/10.1007/s13369-022-06986-0

RESEARCH ARTICLE-COMPUTER ENGINEERING AND COMPUTER SCIENCE

Efficient Storage and Encryption of 32-Slice CT Scan Images Using Phase Grating

Anirban Patra[1,3] · Arijit Saha[2] · Kallol Bhattacharya[3]

Received: 6 December 2021 / Accepted: 15 May 2022 / Published online: 24 June 2022

Abstract

Medical images are treated as sensitive as it carries patients' confidential information and hence must be protected from unauthorized access. So, a strong encryption mechanism is a primary criterion to transmit these images over the internet to protect them from intruders. In many existing algorithms, noise affection in the extracted images is high, hence not suitable for medical data encryption. Here, we present a new method using phase grating to multiplex as well as encrypting 32 cross-sectional CT scan images (slices) in a single canvas for optimization of storage space and improvement of security. The entire process is divided into a few steps. Before transmission, the main canvas is encrypted with the help of a random phase matrix. The main canvas is further encrypted by the transposition method to enhance security. After decryption, inverse Fourier transform is applied at the proper location of the decrypted canvas to extract the images from the spectra. Quality is measured with peak-signal-to-noise ratio and correlation coefficient methods. Here, it is greater than 38 and the correlation coefficient is close to 1 for all images, thereby indicating of good quality of extracted images. The effect of three common cyber-attacks (viz. known-plaintext attack, chosen-plaintext attack, and chosen-ciphertext attack) is also presented here. The correlation coefficient during cyber-attacks is found to be close to zero, which implies the robustness of the algorithm against cyber-attacks. Finally, a comparison with existing techniques shows the effectiveness of the proposed method.

Keywords CT scan image · Phase grating · Random phase matrix · Inverse Fourier transform · Cyber attack

1 Introduction

In the medical field, the use of digital images is increasing day by day. Hence, large storage space is required to save these images for processing and future use. In addition, images must be protected from different cyber-attacks during transmission. So, to optimize storage space and protect medical images, it is necessary to compress and encrypt them. The challenge is therefore to transmit and store medical information without satisfactory security and fidelity [1].

A well-known diagnostic tool used to analyze several diseases is the computed tomography (CT) scan which uses X-ray measurement from multiple angles to generate cross-section images (slices) [2, 3]. In other medical imaging processes, the movement of organs due to respiration is a critical issue. CT scan images eliminate this drawback and provide a better output [4–6]. Recently, CT scan images are also widely used to diagnose the patient affected by a coronavirus [7]. Different approaches have been proposed for the multiplexing of images as well as holograms. In a recently proposed method, the images are multiplexed by phase grating with variable frequency and orientation angle. Due to modulation at a fixed orientation, multiple spectral bands are generated where only three visible spectral spots are taken into consideration (for each image). Variation of grating frequency and orientation angle create more than one spatial frequency spectrum plane which is added together to form a single package before transmission. During reconstruction, inverse Fourier transform (FT) in addition to low-pass filter (LPF) is applied at selected spots [8]. They also utilized this system to multiplex medical and remote sensing

✉ Anirban Patra
anitublu@gmail.com

[1] Department of ECE, JIS College of Engineering, Kalyani, India

[2] Department of ECE, B P Poddar Institute of Management and Technology, Kolkata, India

[3] Department of Applied Optics and Photonics, University of Calcutta, Kolkata, India

images by replacing phase grating with amplitude grating with reduced efficiency [9, 10]. Apart from amplitude and phase gratings, a few other grating systems are also used for the multiplexing of images due to their special properties. The reflective grating has minimized the number of required optical components in multiplexing [11]. Grating along with optical $2f$ system is applied to multiplex as well as compress low-resolution images. Here, each modulated image is added together to create a single element before reconstruction [12]. Color images are multiplexed by modulating with blazed gratings, where three planes of each image (red, green, and blue) are modulated separately by blazed grating and superposed into a phase-only hologram wherefrom the images are reconstructed. In this system, 256 color images can be multiplexed into 512 × 512 pixel holograms [13]. J E Harvey et.al. discussed the characteristics of different gratings and their applications in image multiplexing [14]. Apart from the grating, some well-known optical processes like wavelength-based systems [15], orthogonal phase encoding [16], angular phase encoding process, etc. [17, 18], are also used to multiplex and encrypt images and holograms. In a wavelength-based system, initially, images are modulated by the double phase encoding method before encryption. By maintaining a minimum separation of multiplexing wavelengths, storage capacity can be increased. An orthogonal phase encoding system is proposed to store and encrypt 3D images as well as holograms with a binary mask. Though the phase encoding system enhances storage capacity, it suffers from spatial phase fluctuations which increase cross-correlation noise. Sequential and non-sequential ray-tracing techniques in addition to couple wave methods of aperiodic gratings are applied to multiplex volume holograms in volume holographic imaging systems (VHIS). This can be easily implemented into commercial packages [19]. Using theta modulation, Lohman-type holograms are modulated individually, followed by the addition of modulated output to generate a single hologram [20]. The major drawbacks of these systems are noise affection, limitation to low-resolution images, and comparatively long reconstruction time. In the encryption process, the grating has also taken a major role in the last few years. Encryption with random phase matrix [8], laterally translated phase grating [20], optical double-image cryptography [21], diffraction imaging with interference superposition [22] are recently proposed by researchers. In laterally translated phase grating, a series of random phase masks is placed in the optical path which generates encrypted messages when they are laterally translated by phase grating. Cyphertexts are decrypted in an interference superposition system utilizing the properties of grating diffraction in an optical 4f system. Apart from the grating, other popular methods of image encryption are joint transform correlate [23], iterative algorithm process [24], use of chaotic system [25, 26], optical interference [27] etc. In an optical interference system, images are encrypted using optical interference and two-phase plates. This simple system doesn't require any iterative algorithm for decryption. To improve this system and to eliminate the contour problem, a three-phase plate technique is proposed by researchers. [28] Fractional Fourier transform is also widely used for image encryption for many years [29, 30]. Use of Krawtchouk polynomials [31], Meixner polynomials [32], Hahn polynomials [33] and Charlier polynomials [34] are being recently used by researchers nowadays for feature extraction from images.

In many existing works, the quality of output images is poor due to noise affection. Moreover, nowhere a proper discussion regarding the effect of cyber-attacks on medical images is reported. So, in this research paper, we proposed a novel technique of medical image compression as well as encryption using phase grating to efficiently store and encrypt the images. Here, 32 numbers of CT scan images are compressed and encrypted with the help of phase grating and random phase matrix. The entire operation is done in the frequency domain. In general, most of the attacking tools or software are designed on the basis of spatial domain encryption algorithms. Hence, frequency domain systems provide better security in cyber-attack spatial domain algorithms. It is well known that the efficiency of the amplitude grating at + 1 order is only 6.25% since the remaining light energy is lost due to the absorption by the grating. Hence the phase grating has been preferred due to its low power loss and better transmission contrast compared to amplitude grating [14]. Initially, CT scan images are modulated one by one using high-frequency grating along the x-axis. As a result of modulation, three spectral spots are generated for each image. Each spectral spot contains image information; hence we have selected only one spot for further processing. The selected 32 spectral spots are sequentially placed into the main canvas for multiplexing. Before transmission, the canvas which contains all spectra are multiplied by a random phase matrix for encryption. To enhance security, it is further encrypted by the transposition method. At the receiving end, after decryption processes, inverse Fourier transform is applied at selected zones for retrieval of images. To evaluate the quality of the extracted images, peak-signal-to-noise ratio (PSNR) and correlation coefficient methods are used here. The correlation coefficient is used also to measure the security of the cyber-attacked (known-plaintext attack, chosen-plaintext attack, and chosen-ciphertext attack) images. The mathematical analysis and a brief discussion of the methodology used are presented here. In the Results and Discussion section, a comparative study with some previous methods and the result of the three above-mentioned cyber-attacks have been discussed.

The following section deals with the methodology, where detailed process is explained using the numerical equation, flowchart, diagram, and pseudocode. In Sect. 3, the results have been shown and discussion on the quality of output images is given, including a comparative study with existing works. The effects of different cyber-attacks have been discussed in Sect. 4. Finally, the conclusion has been drawn in Sect. 5.

2 Methodology

2.1 Theory

Here the entire methodology is presented using mathematical equations, diagrams and flowchart. Flowchart is used to provide a basic idea of the process, and the process of practical implementation is illustrated with a bit of pseudocode. In this section, we have discussed the process part by part and provided detail information of them. Initially, the reason of high frequency selection for modulation is explained, followed by discussion of modulation process with numerical equations. In the next part, we have illustrated the extraction process and then quality detection of extracted images is discussed. At last, pseudo coding is provided for detail explanation.

2.2 Frequency Selection

In order to avoid aliasing problem high grating frequency is selected. Each CT scan image is modulated by a phase grating at 0° orientation angle (along the x-axis). Resultant spectra consist of multiple spots where the FT of the image exists. The selected frequency is 1000 lines per mm (which is sufficient to overcome the aliasing problem).

2.3 Modulation Process

Let us assume that the selected image $f_1(x, y)$ is modulated by phase gratings of the form $\exp\left[i\left(\frac{m}{2}\right)sin2\pi u_1 x\right]$ where u_1 is the grating frequency and m is the phase contrast. The modulated object may be expressed as [35]

$$s_1(x, y) = f_1(x, y)\exp\left[i\left(\frac{m}{2}\right)sin2\pi u_1 x\right] \quad (1)$$

By applying convolution theorem, the FT of this modulated object is given by

$$S_1(u, v) = [F_1(u, v) \circledast \left[\sum_{q=-\alpha}^{q=+\alpha} J_q\left(\frac{m}{2}\right)\delta(u - qu_1, v)\right] = \left[\sum_{q=-\alpha}^{q=+\alpha} J_q\left(\frac{m}{2}\right)F_1(u - qu_1, v)\right] \quad (2)$$

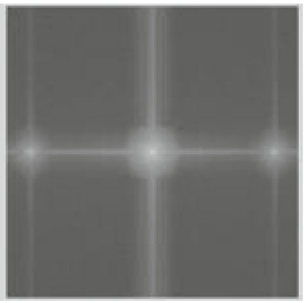


Fig. 1 Generated spatial frequency spectrum of modulated image 1

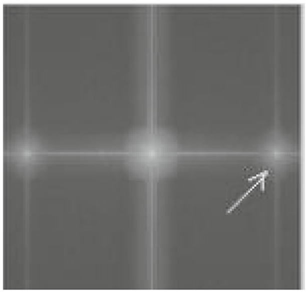


Fig. 2 Selected spot out of three spectral spots

where $J_q$isthe$q$thorderBesselFunction and 'q' is the diffraction order.

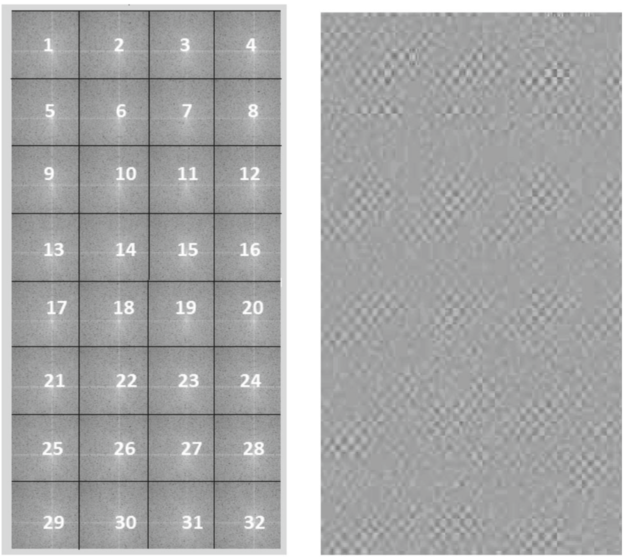
The diffraction pattern, as given by Eq. 2, is a series of diffraction spots each containing the object spectrum. Considering the zero-order and the first two orders of the spatial frequency spectrum, Eq. 2 may be represented by

$$S_1(u, v) = \left[J_0\left(\frac{m}{2}\right)F_1(u, v) + J_{-1}\left(\frac{m}{2}\right)F_1(u + u_1, v) + J_{+1}\left(\frac{m}{2}\right)F_1(u - u_1, v)\right] \quad (3)$$

Figure 1 represents spatial frequency spectrum of modulated image $f_1(x, y)$. The higher-order spots in the generated spatial frequency spectra are the replica of each other; hence, we have chosen only one spectral spot from each modulated image. The lower spectrum (marked by arrow Sign) of all image is selected here which is shown in Fig. 2.

2.4 Encryption of Filtered Spatial Frequency Spectrum

Selected spatial frequency spectrum which is shown in Fig. 2 is automatically placed in the main canvas (size 4100 × 2050) by maintaining a sequence (here 32 spectra are automatically arranged in 8 rows and 4 columns). After completion of this process, main canvas (where 32 spectra are placed) is multiplied by random phase matrix (R) for 1st phase of encryption.



(a) (b)

Fig. 3 **a** Canvas after sequential placement of selected spectra (marked with the spatial frequency spectrum of particular images); **b** first stage of encrypted canvas after multiplication with random phase matrix

Since one of our primary objectives is to optimize storage space, a large canvas is not considered. Figure 3a illustrates the canvas after sequential placing of spectra, whereas Fig. 3b shows the encrypted canvas after first stage of encryption.

Figure 3a represents the full canvas where 32 spectra are stored in 4-column and 8-row series. The number in the canvas indicates the selected spatial frequency spectrum of the particular image. After sequential placing of all selected spectra, it is multiplied by the random phase matrix which is shown in Fig. 3b. To enhance the security of the system, the encrypted images in the canvas are further encrypted by the transposition method which is shown in Fig. 4.

2.5 Retrieval of Images from Encrypted Canvas

In this process, transmitted main canvas consists of 32 spectra containing information of all images. Automatic placement of spectra is done by selecting number of rows, columns as well as sequential cell no in the program. This is performed in the transmitter side before encryption. Individual encryption of every spatial frequency spectrum reduces the security as it is easy to isolate the image position as well as total number. Hence, we have encrypted the whole canvas to enhance security. After receiving the encrypted canvas, 32 spectra have been retrieved by decryption process. As encryption is done is two phases, two-phase decryption is performed here. In the first phase of decryption, reverse transposition process is done followed by division of 1st phase decrypted canvas by random phase matrix.

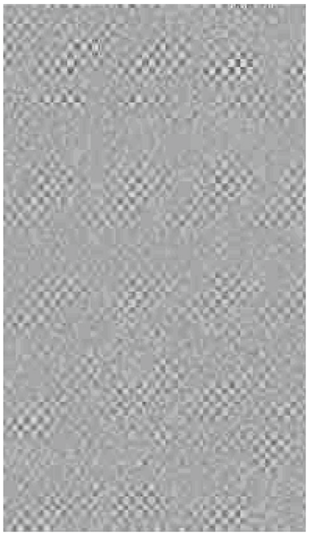


Fig. 4 Second stage of encrypted canvas after transposition

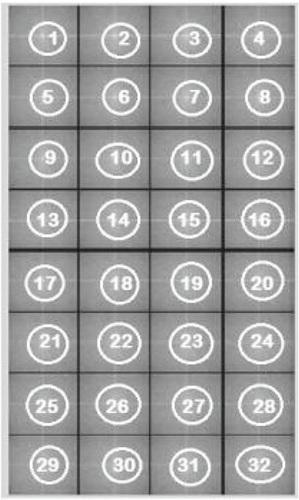


Fig. 5 Decrypted canvas marked with the spatial frequency spectrum of particular images

To get the information of all images from spectra, inverse Fourier transform (FT) is executed in the next process. This part may be done in two ways: The first one is automatic application of inverse FT in the sequential way at spectra of decrypted canvas, and the second one is application of inverse FT at maximum intensity areas in addition with low-pass filter (LPF). In the second process, initially a pixel intensity graph of each row or column must be calculated before inverse FT application. We have selected the first process to minimize the time requirement. Decrypted canvas is illustrated in Fig. 5.

The selected spots of decrypted canvas are marked as 1 to 32. Size (pixel resolution) of each marked spot is 480 × 480 here, whereas the pixel resolution of total canvas is 4100 × 2050.

2.6 Flowchart of the System

A general view of the important steps is shown in the flowchart.

Flowchart and diagram of the entire process in both transmitter and receiver sections are illustrated in the Figs. 6 and 7, respectively.

2.7 Quality Checking of Output Image

In this section, quality checking of the extracted images using PSNR and correlation coefficient is explained in detail.

To check the quality of output images, two methods are used: (i) conventional PSNR method and (ii) correlation coefficient method. For the last few years, PSNR and correlation coefficient methods are used as quality checking parameter in many image processing techniques [36–40]

(i)*PSNR method*: This is measured with the help of mean square error (MSE). In general, a PSNR value of the reconstructed image greater than 35 is considered as a good-quality image [41–44].

Mean square error (MSE) can be represented as

$$\mathrm{MSE} = \frac{1}{\mathrm{mn}} \sum_{\mathrm{y}=1}^{\mathrm{m}} \sum_{\mathrm{x}=1}^{\mathrm{n}} [\mathrm{f}(\mathrm{x},\ \mathrm{y}) - \mathrm{g}(\mathrm{x},\ \mathrm{y})]^2 \tag{4}$$

where $f(x,\ y)\ and\ g(x,\ y)$ are the original image and the retrieved image, respectively;

$$\mathrm{PSNR} = 20\log 10 \frac{255}{\sqrt{\mathrm{MSE}}} \tag{5}$$

(ii)*Correlation coefficient*: This measures the dependency of two adjacent pixels which are closely correlated in all directions. If the two values are closely related, the correlation coefficient is close to one; otherwise, its value is close to zero.

$$r = \frac{\sum_i (x_i - x_m)(y_i - y_m)}{\sqrt{\sum_i (x_i - x_m)^2}\sqrt{\sum_i (y_i - y_m)^2}} \tag{6}$$

where r indicates the correlation coefficient; x_i and y_i are the intensity values of the ith pixel of original and output images; and x_m and y_m represent the average intensity values of original and extracted images.

2.8 Pseudo Code of the Entire Process

Main function

```
a. Select grating frequency = 1000 for modulation
b. Define Grating function
c. Define a 1 × 30 array for the reading of 30 CT scan high-resolution images
d. Create a canvas for storing spectra and split it into 30 divisions
e. Create a loop for i = 1: 30
    i. Modulate image1 with Grating Equation
    ii. Fourier transform of the modulated output
    iii. Create spectra of image 1
    iv. Select a spectrum (LSB)
    v. Place it at jth location of canvas
    vi. Call next image (i = 2)
    vii. Repeat process i to v
    viii. Place it (j + 1) location of canvas
    ix. Continue up to i = 30
    x. End
f. Create random phase matrix
g. Multiply canvas with random phase matrix
h. Decrypt the encrypted canvas (dividing by random phase matrix)
i. Inverse Fourier transform at selected zones
j. Calculate PSNR and correlation coefficient
```

For Cyber Attack

```
a. Decrypt encrypted canvas (g) using different methods
b. Calculate PSNR and correlation coefficient
c. End
```

3 Results and Discussion

We have used 32 high-resolution CT scan images (shown in Fig. 8) of pixel size 677 × 598. Entire work is done using MATLAB simulation software, 16 GB RAM and Intel Core i5 Processor. No optical hardware is used in our research work. CT scan images are collected from the website of National Institute of Health which is freely available for research work.

32-Slice CT scan images are displayed in Fig. 8.

During the retrieval process, inverse Fourier transform is applied at selected areas of the canvas where the spots exist. Extracted images are displayed in Fig. 9.

PSNR values and correlation coefficients of output images are tabulated in Table 1. PSNR value is used to highlight the visual quality of the images, whereas correlation coefficients are calculated to measure similarity with the original images.

The size of all selected images is 677 × 598. To save storage space, we have transmitted only a part of the entire spectrum. The compression ratio is shown in Table 2.

Size of each image = 677 × 598 = 364.2 kB.

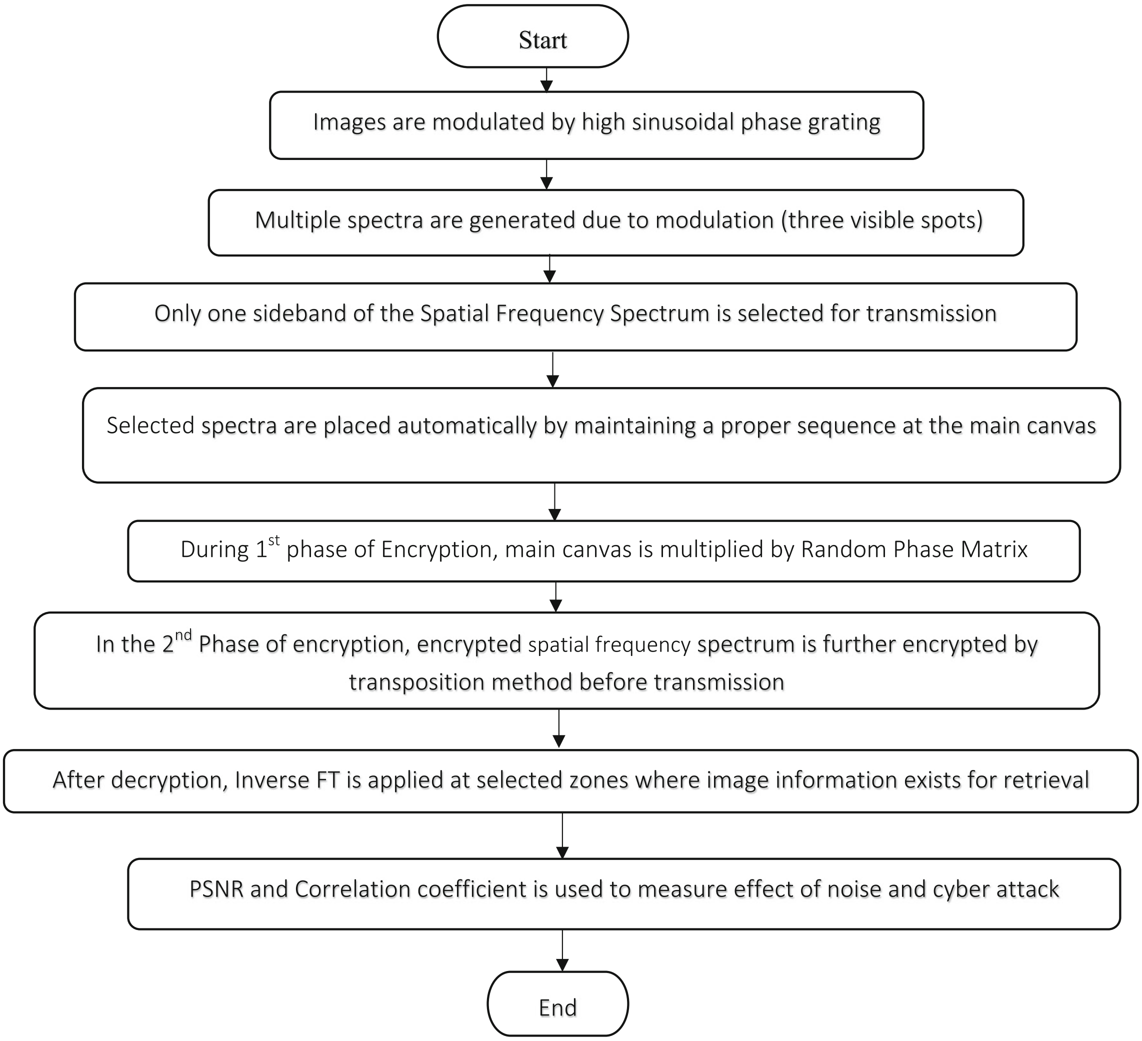

Start
Images are modulated by high sinusoidal phase grating
Multiple spectra are generated due to modulation (three visible spots)
Only one sideband of the Spatial Frequency Spectrum is selected for transmission
Selected spectra are placed automatically by maintaining a proper sequence at the main canvas
During 1st phase of Encryption, main canvas is multiplied by Random Phase Matrix
In the 2nd Phase of encryption, encrypted spatial frequency spectrum is further encrypted by transposition method before transmission
After decryption, Inverse FT is applied at selected zones where image information exists for retrieval
PSNR and Correlation coefficient is used to measure effect of noise and cyber attack
End

Fig. 6 Fundamental steps of our proposed method indicated in the flowchart

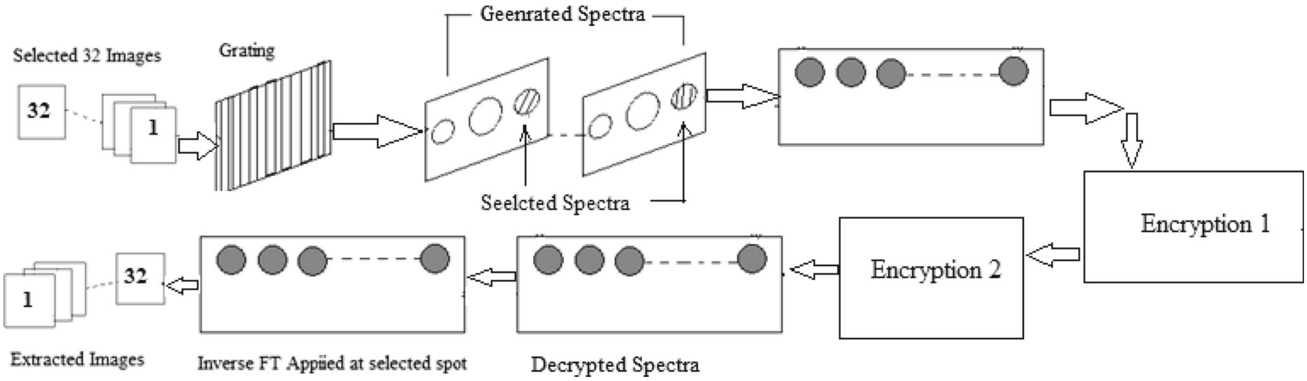


Fig. 7 Schematic diagram of the entire process of the proposed method

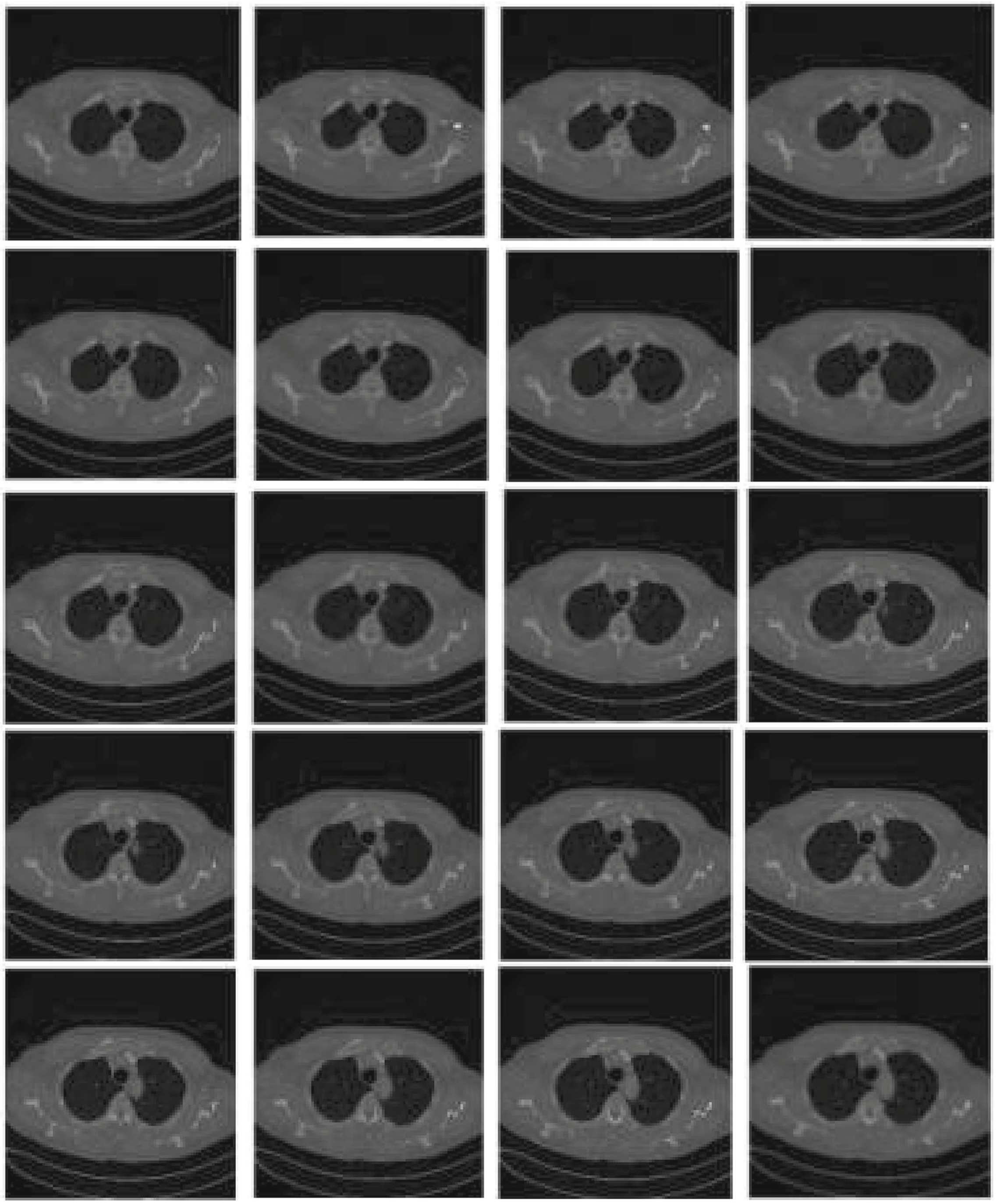


Fig. 8 32-Slice CT scan images used as input

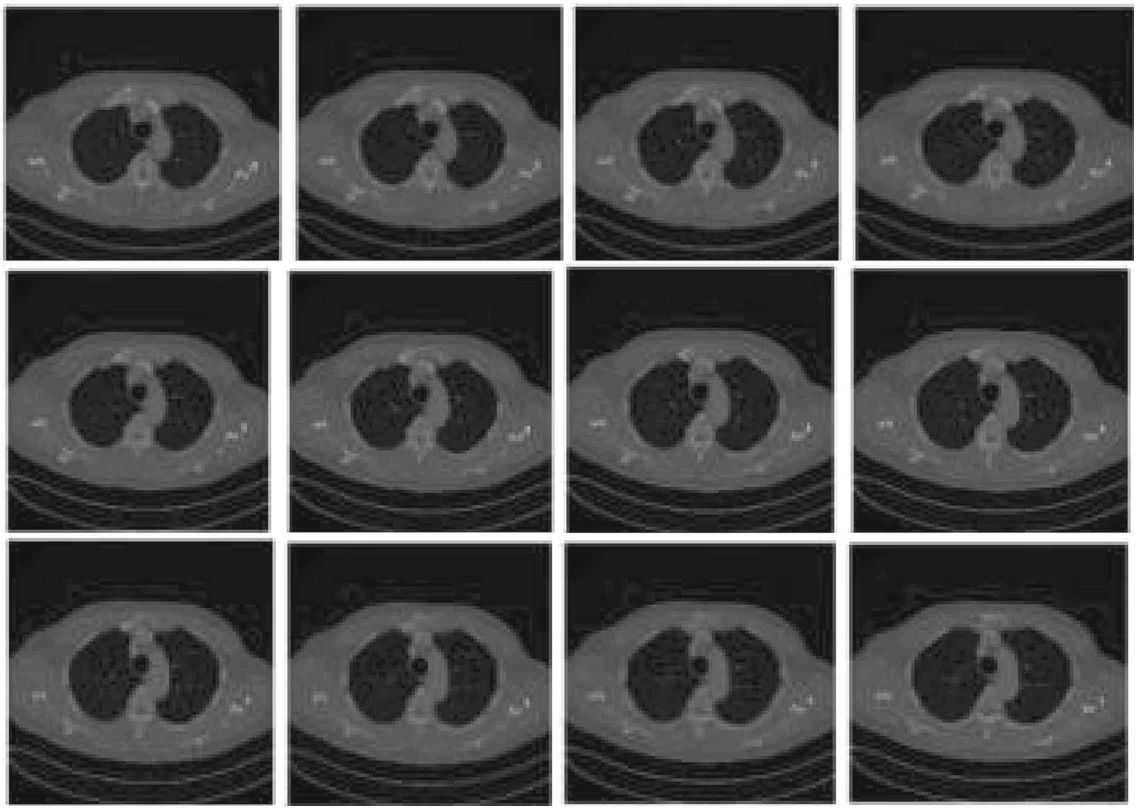


Fig. 8 continued

Size of 32 images = 11.3 MB.

Size of transmitted spatial frequency spectrum = 8.41 MB.

In medical image processing, images carry a lot of information. Hence during compression of images loss of information should be as minimum as possible. Therefore, many existing algorithms are not suitable for medical image compression. In our proposed algorithm, compression ratio is not so high. Moreover, PSNR value is greater than 38 in all cases and correlation coefficient is also close to 1. Each one indicates the good quality standard of output images, and hence this system is acceptable for medical image compression.

3.1 Comparison with Previous Methods

Table 3 highlights the comparison between our proposed method and that of few existing techniques already reported. However, effects of different cyber-attacks on medical images have not been reported in any scholarly articles.

Table 3 shows the limitations of some existing methods. The main drawbacks of the existing systems are low PSNR (< 32), correlation coefficient not close to one, limited for few images, etc. Our algorithm overcomes these limitations which are clearly shown in the table.

4 Result and Analysis of Possible Attacks

To evaluate the security of the proposed method, correlation coefficients in cyber-attacks have been calculated. In this method, exact decryption is impossible without knowledge of the proper algorithm as well as the key selection and zonal position of images. Some spatial domain attacks are not effective in this method as it is performed in the frequency domain. We have analyzed our result for three cyber-attacks: (a) known-plaintext attack, (b) chosen-plaintext attack and (c) chosen-ciphertext attack, respectively. In each possible attack, correlation coefficients are calculated and the result is illustrated in Table 4.

4.1 Known-Plaintext Attack

In a known-plaintext attack, the intruder has information about at least one message of both the plaintext as well as the ciphertext. The primary objective of the attacker is to guess about the secret key or algorithm which helps to decrypt any further messages. We have tried with different keys and algorithms, and the output result is displayed in Fig. 10a–l, respectively.

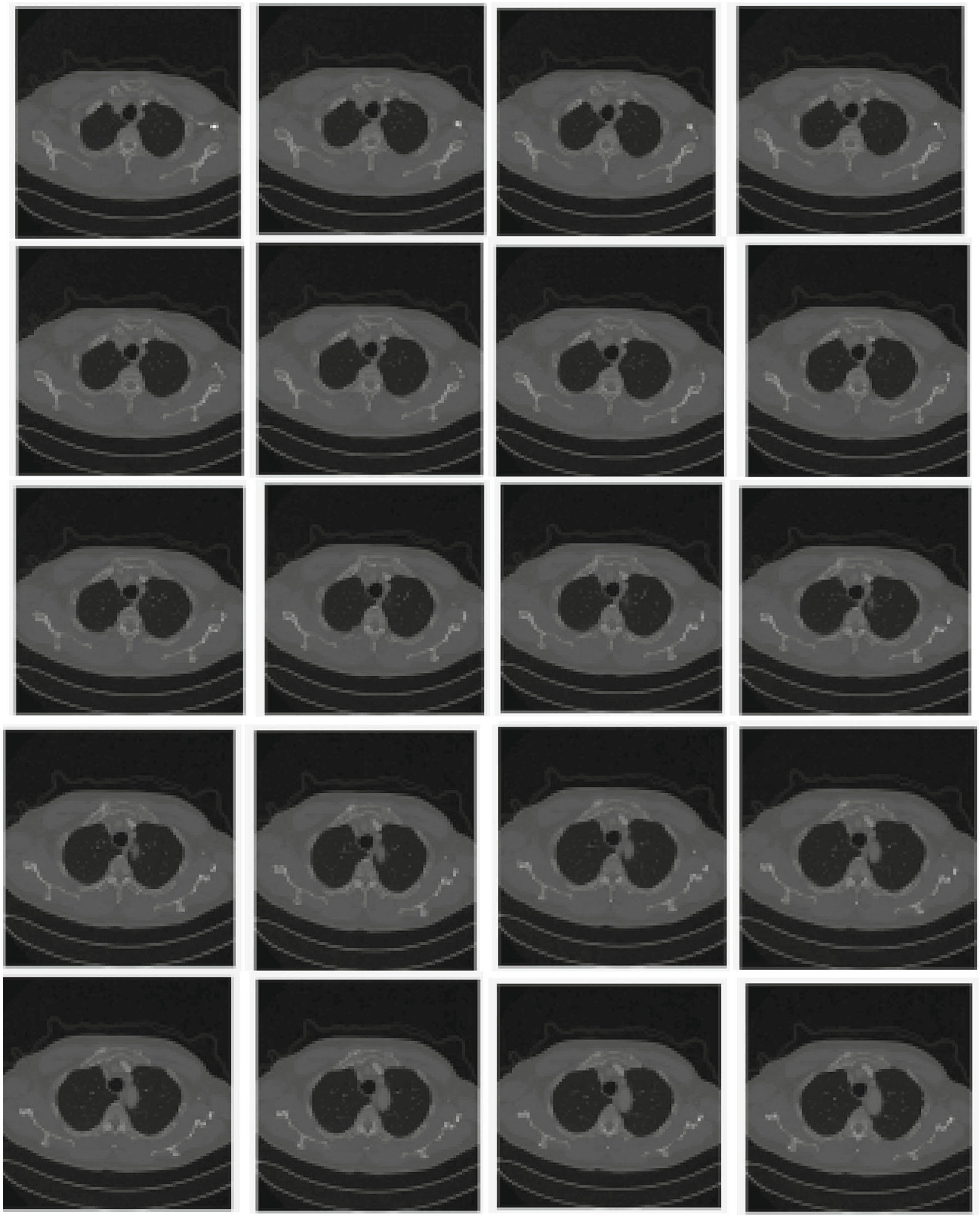


Fig. 9 Extracted CT scan images

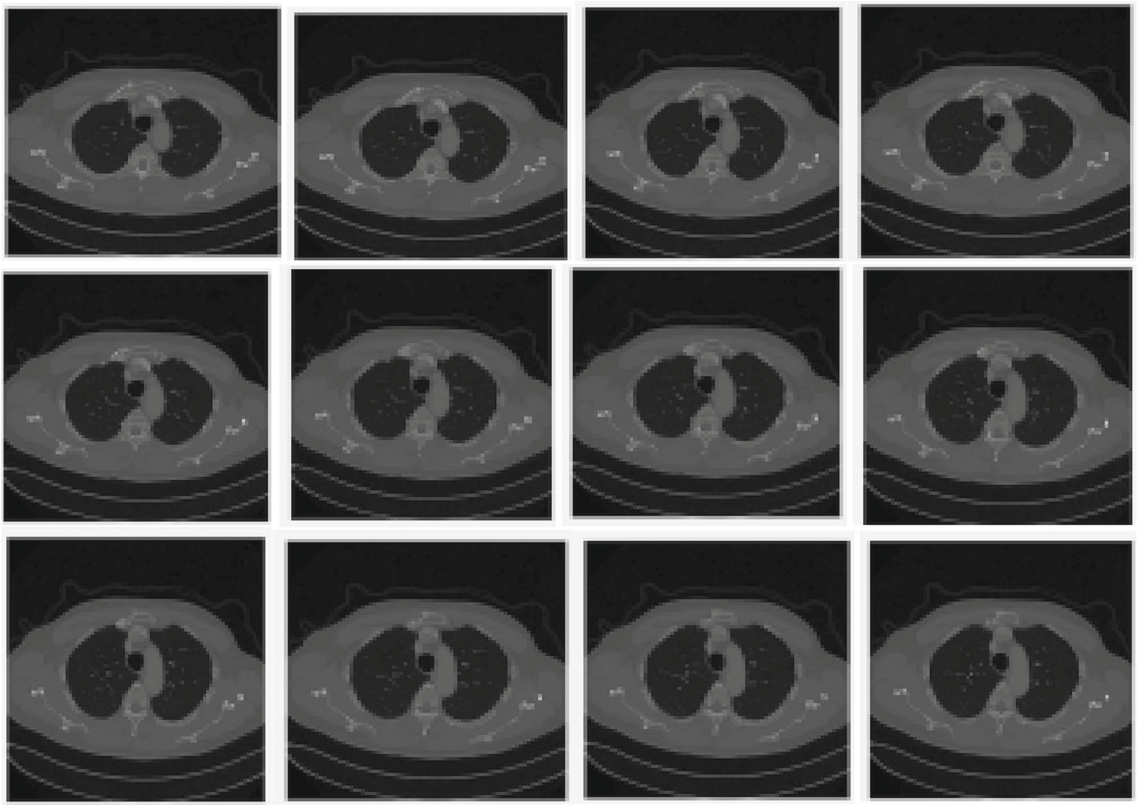


Fig. 9 continued

Table 1 Quality check result

Image no.	PSNR	Corr. Coef	Image no.	PSNR	Corr. Coef.
1	39.2	0.997	17	39.1	0.997
2	38.8	0.996	18	38.8	0.996
3	39.2	0.997	19	38.8	0.996
4	39.1	0.997	20	38.9	0.996
5	38.9	0.996	21	39.3	0.998
6	39	0.997	22	39.1	0.997
7	38.8	0.996	23	38.9	0.996
8	38.8	0.996	24	39.2	0.997
9	38.9	0.996	25	38.9	0.997
10	39.2	0.997	26	39.3	0.998
11	38.9	0.996	27	38.9	0.997
12	38.9	0.997	28	39	0.996
13	38.9	0.997	29	38.9	0.996
14	39.1	0.997	30	39.2	0.997
15	39.2	0.997	31	38.9	0.996
16	38.9	0.996	32	38.8	0.996

Table 2 Calculation of storage space

The original size of each image (pixel resolution)	Total no. of images	Total size of original images (pixel resolution)	Total spatial frequency spectrum size (pixel resolution)	Ratio of storage space saved (original spatial frequency spectrum size/transmitted spatial frequency spectrum size)
677 × 598	32	677 × 598 × 32 = 1,29,55,072	4100 × 2050 = 84,05,000	1.34: 1

Table 3 Comparison table

References	Limitations	Our proposed scheme
[8, 9]	PSNR < 32 A limited no. of images (only 10 images) are used	PSNR > 38 32 images are used
[36]	Correlation coefficient = 0.946	Correlation coefficient > 0.99
[37]	Correlation coefficient (0.72 – 0.96)	Correlation coefficient > 0.99
[38]	Correlation coefficient (0.98)	Correlation coefficient > 0.99
[39]	Correlation coefficient (0.95 – 0.99) Only Lena image is used	Correlation coefficient > 0.99 32 number of images are used
[40]	PSNR < 29	PSNR > 38

Table 4 Correlation coefficients

Case No	Known-plaintext attack	Chosen-plaintext attack	Chosen-ciphertext attack	Case no	Known-plaintext attack	Chosen-plaintext attack	Chosen-ciphertext attack
1	0.061	0.026	0.008	7	0.196	0.011	0.159
2	0.078	0.014	0.003	8	0.141	0.023	0.008
3	0.032	0.017	0.241	9	0.028	0.238	0.233
4	0.381	0.049	0.267	10	0.255	0.388	0.068
5	0.344	0.073	0.235	11	0.084	0.062	0.337
6	0.309	0.042	0.272	12	0.272	0.027	0.094

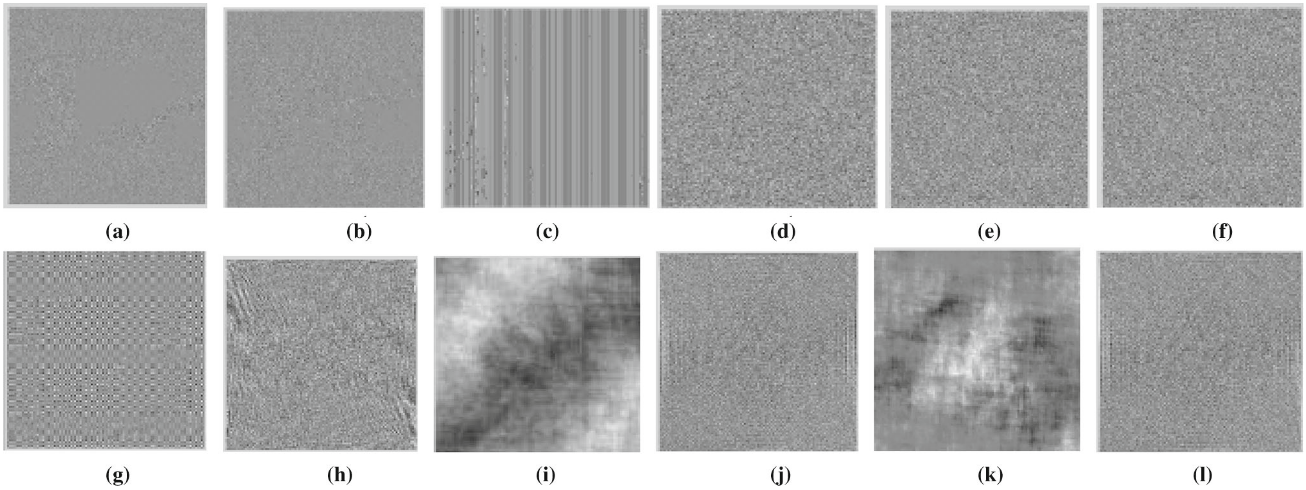


Fig. 10 **a–l** Recovered known-plaintext-attacked images

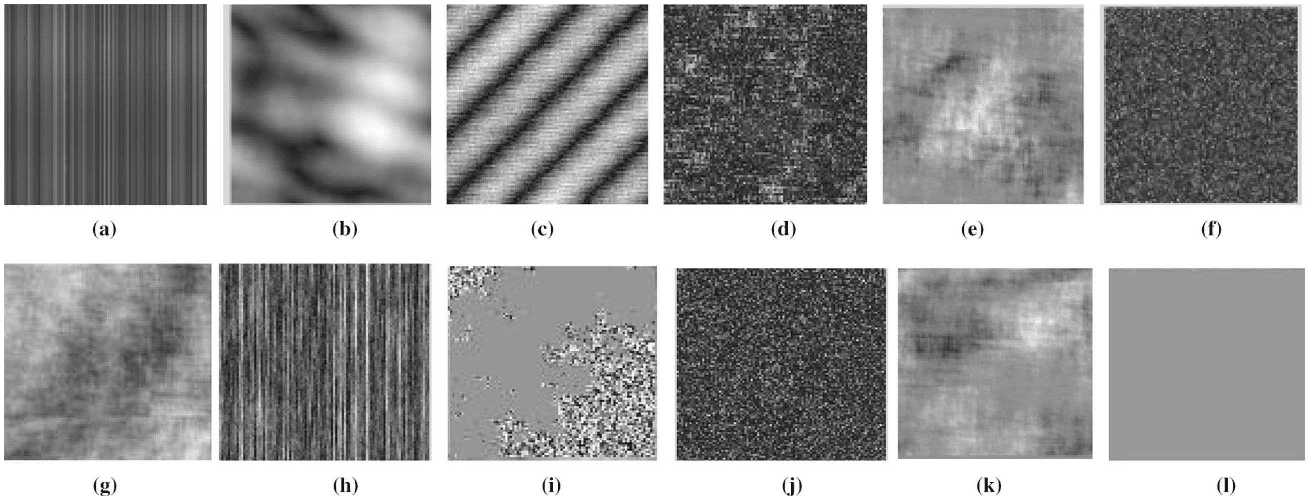


Fig. 11 **a**–**l** Recovered chosen-plaintext attacked images

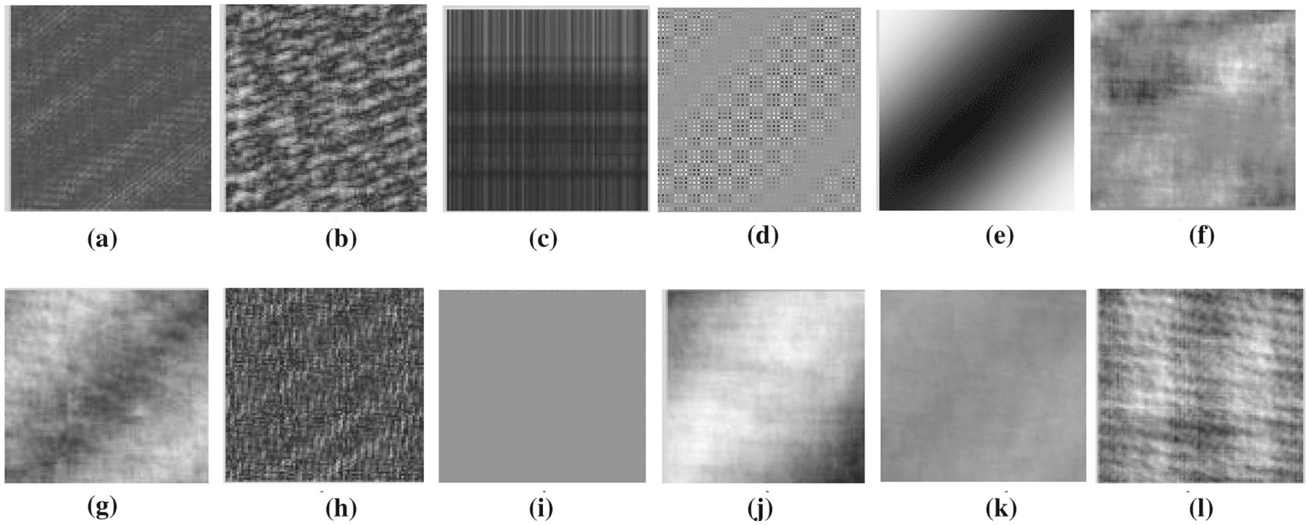


Fig. 12 **a**–**l** Recovered Chosen-ciphertext attacked images

4.2 Chosen-Plaintext Attack

In a chosen-plaintext attack, an attacker can select arbitrary plaintext images which are to be encrypted and generates corresponding ciphertexts. By this method, the attacker tends to know the secret key as well as the algorithm of the system. Without any knowledge of the secret key, the attacker tries to get information about the secret key to generate an algorithm that allows him to decrypt any encrypted messages. By this method, the attacker is able to analyze the system characteristic using any type of input data. Alternately we can say that in a chosen-plaintext attack, an attacker chooses any plaintext data to be encrypted and then tries to analyze the secret encryption key or algorithm after receiving the corresponding ciphertext. Here the main objective of the attacker is to know the key or algorithm by which the attacker can decrypt any message. Our experimental result is shown in Fig. 11 a–l, and it indicates the ruggedness of the proposed method. Like a known-plaintext attack, here also, the correlation coefficient is used to measure the security.

4.3 Chosen-Ciphertext Attack

In chosen-ciphertext attack, an attacker tries to analyze the secret key or algorithm using any chosen ciphertext together with corresponding plaintexts. Primary objective of the attacker is to get more information about the secret key or algorithm of the system. The intruder has capability to create the victim (person knows the key) decipher any ciphertext and send him back the result. By analyzing the chosen ciphertext and also the corresponding received plaintext, the intruder tries to guess the secret key that has been employed by the victim. During the chosen-ciphertext attack, an attacker analyzes any chosen ciphertexts with their corresponding plaintexts. The main aim is to get knowledge regarding the secret key or algorithm. Our experimental result is shown in Fig. 12a–l, respectively.

The effect of three commonly known cyber-attacks has been discussed. Output in each case is displayed, and correlation coefficient values are placed in Table 4. From Table 4, it is clear that in maximum cases, correlation coefficients values are close to zero which implies that our proposed system is highly secured.

Table 4 displays the effect of three commonly known cyber-attacks. We have examined its robustness with the help of correlation coefficient value. In all cases, the value is far away from one which proves that there is no similarity with the original images. Hence this system is prone to cyber-attack.

5 Conclusion

In cryptography, encryption of medical images is considered one of the most predominant areas of application. This encryption is required to enhance confidentiality as well as to protect the images from intruders. In this communication, we have presented an encryption technique along with the multiplexing process of medical images with the help of phase grating and random phase matrix to optimize storage space and enhance security level. To maintain a better quality of output images, the compression ratio is kept low here. PSNR is nearly 39, and the correlation coefficient is 0.997 for each image which implies that the quality of the output images is really good. During different cyber-attack, correlation coefficients are also close to zero, which indicates the high security of our proposed scheme. This method shows the applicability of phase grating for information storage.

Here, we have worked with 32 CT scan images (grayscale). In the case of color images, spatial frequency spectra for three different color channels will be required to multiplex the same number of images, and hence more storage space is required to save them. So, compression of color images for storage space optimization using this algorithm is a challenging task.

Author contributions All authors have equal contribution to preparing the manuscript.

Funding No funding from any source.

Declarations

Conflict of interest We further declare that we have no conflicts of interest regarding this manuscript.

References

1. Ammah, P.N.T.; Owusu, E.: Robust medical image compression based on wavelet transform and vector quantization. Inform. Med. Unlocked **15**, 100183 (2019)
2. Karatas, O.H.; Toy, E.: Three-dimensional imaging techniques: a literature review. Eur. J. Dent. **8**(1), 132–140 (2014)
3. Pan, X.; Siewerdsen, J.; La Riviere, P.; Kalender, W.: Development of x-ray computed tomography: the role of Medical Physics and AAPM from the 1970s to present. Med. Phys. **35**(8), 3728–3739 (2008)
4. Rubin, G.: Computed tomography: revolutionizing the practice of medicine for 40 years. Radiology **273**(2S), S45–S74 (2014)
5. Van, R.A.; Bipat, S.; Zwinderman, A.H.; Ubbink, D.T.; Stoker, J.; Boermeester, M.A.: Acute appendicitis: meta-analysis of diagnostic performance of CT and graded compression; US related to prevalence of disease. Radiology **249**, 97–106 (2008)
6. Hricak, H.; Brenner, D.J.; Pearce, M.S.; Suleiman, O.H., et al.: Managing radiation use in medical imaging: a multifaceted challenge. Radiology **258**, 889–905 (2011)
7. Ai, T.; Yang, Z.; Hou, H.; Zhan, C.; Chen, C.; Lv, W.; Xia, L.: Correlation of chest CT and RT-PCR testing in coronavirus disease 2019 (COVID-19) in China: a report of 1014 cases. Radiology **296**, E32–E40 (2020)
8. Patra, A.; Saha, A.; Bhattacharya, K.: Multiplexing and encryption of images using phase grating and random phase mask. Opt. Eng. **59**(3), 033105 (2020)
9. Patra, A.; Saha, A.; Bhattacharya, K.: Compression and multiplexing of medical images using optical image processing. In: Verma, J.K.; Paul, S.; Johri, P. (Eds.) Computational Intelligence and Its Applications in Healthcare, pp. 63–71. Academic Press, Cambridge (2020)
10. Patra, A.; Saha, A.; Bhattacharya, K.: High-resolution image multiplexing using amplitude grating for remote sensing applications. Opt. Eng. **60**(7), 073104-1–11 (2021)
11. Valencia, J.V.: Analysis of the efficiency of a virtual-optical multiplexing method, by using theta modulation. TecnoLógicas **20**(39), 175–186 (2017)
12. Cabezas, L.; Tebaldi, M.; Barrera, J.F.; Bolognini, N.; Torroba, R.: Optical smart packaging to reduce transmitted information. Opt. Express **20**(1), 158–163 (2012)
13. Shanshan, C.; Shubo, C.; Tian, X.; Shaohua, T.: Storage and reconstruction of multiple color images with a phase only hologram. J. Phys. Commun. **2**, 055021 (2020)
14. Harvey, J.E.; Pfisterer, R.N.: Understanding diffraction grating behaviour: including conical diffraction and Rayleigh anomalies from transmission gratings. Opt. Eng. **58**(8), 087105 (2019)
15. Situ, G.; Zhang, J.: Multiple image encryption by wavelength multiplexing. Opt. Lett. **30**(11), 1306–1308 (2005)
16. Kim, Y.; Sim, M.; Moon, I.: Secure storage and retrieval schemes for multiple encrypted digital holograms with orthogonal phase encoding multiplexing. Opt. Express **27**(16), 22147–22160 (2019)
17. Denz, C.; Pauliat, G.; Roosen, G.; Tschudi, T.: Volume hologram multiplexing using a deterministic phase encoding method. Opt. Commun. **85**(2–3), 171–176 (1991)
18. Lembcke, J.; Denz, C.; Tschudi, T.: General formalism for angular and phase-encoding multiplexing in holographic image storage. Opt. Mater. **4**(2–3), 428–432 (1995)
19. Luo, Y.: Simulations and experiments of aperiodic and multiplexed gratings in volume holographic imaging systems. Opt. Express **18**(18), 19273–19285 (2010)
20. Wong, K.W.; Cheng, L.M.: A new theta modulation multiplexing scheme for computer-generated holograms. Opt. Laser Technol. **24**(2), 89–92 (1992)

21. Wen, C.; Xudong, C.; Colin, J.R.S.: Optical double-image cryptography based on diffractive imaging with a laterally-translated phase grating. Appl. Opt. **50**(29), 5750–5757 (2011)
22. Zhong, Y.; Chen, L.; Gan, W.; Liu, Y.; Mao, H.: Optical system for recovering optical interference encryption using grating diffraction. J. Opt. **49**, 216–223 (2020)
23. Nomura, T.; Javidi, B.: Optical encryption using a joint transform correlator architecture. Opt. Eng. **39**, 2031–2035 (2000)
24. Sui, L.; Du, C.; Xu, M.; Tian, A.; Asundi, A.: Information encryption based on the customized data container under the framework of computational ghost imaging. Opt. Express **27**, 16493–16506 (2019)
25. Zhou, N.; Pan, S.; Cheng, S.; Zhou, Z.: Image compression-encryption scheme based on hyper-chaotic system and 2D compressive sensing. Opt. Laser Technol. **82**, 121–133 (2016)
26. Li, L.; Xie, Y.; Liu, B.; Ye, Y.; Liu, Y.; Song, T.; Zhang, Y.: Exploiting optical chaos for colour image encryption and secure resource sharing in cloud. IEEE Photon. J. **11**, 1503112 (2019)
27. Zhang, Y.; Wang, B.: Optical image encryption based on interference. Opt. Lett. **33**, 2443–2445 (2008)
28. Wang, X.; Zhao, D.: Optical image hiding with silhouette removal based on the optical interference principle. Appl. Opt. **51**, 686–691 (2012)
29. Liansheng, S.; Xiao, Z.; Huang, C.; Ailing, T.; Asundi, A.K.: Silhouette-free interference-based multiple-image encryption using cascaded fractional Fourier transforms. Opt. Lasers Eng. **113**, 29–37 (2019)
30. Liansheng, S.; Yin, C.; Zhanmin, W.; Ailing, T.; Asundi, A.K.: Single-pixel correlated imaging with high-quality reconstruction using iterative phase retrieval algorithm. Opt. Lasers Eng. **111**, 108–113 (2018)
31. Al-Utaibi, K.A., et al.: Reliable recurrence algorithm for high-order Krawtchouk polynomials. Entropy **23**(9), 1162 (2021)
32. Abdulhussain, S.H., et al.: Fast and efficient recursive algorithm of Meixner polynomials. J. Real-Time Image Process. **18**(6), 2225–2237 (2021)
33. Mahmmod, B.M., et al.: Fast computation of Hahn polynomials for high order moments. IEEE Access **10**, 48719–48732 (2021)
34. Abdul-Hadi, A.M., et al.: On the computational aspects of Charlier polynomials. Cogent Eng. **7**(1), 1763553 (2020)
35. Goodman, J.W.: Introduction to Fourier optics, 3rd edn., p. 11, 82. Viva Books Private Limited, New Delhi (1982)
36. Rashvand, M.; Akbarnia, A.: The feasibility of using image processing and artificial neural network for detecting the adulteration of sesame oil. AIMS Agric Food **4**(2), 237–324 (2019)
37. Okarma, K.; Lech, P.; Lukin, V.V.: Combined full-reference image quality metrics for objective assessment of multiple distorted images. Electronics **10**, 2256 (2021)
38. Eyssa, A.A.; Abdelsamie, F.E.; Abdelnaiem, A.E.: An efficient image steganography approach over wireless communication system. Wirel Pers Commun **110**, 321–337 (2020)
39. Zayed, M.: Ramadan, using entropy and 2-D correlation coefficient as measuring indices for impulsive noise reduction techniques. Int. J. Appl. Eng. Res. **12**(21), 11101–11106 (2017)
40. Goyal, C.; Ubhi, J.S.; Raj, B.: A low leakage TG-CNTFET–based inexact full adder for low power image processing applications. Int. J. Circuit Theory Appl. **47**, 1446–1458 (2019)
41. Rajkumar, S.; Malathi, G.: A comparative analysis on image quality assessment for real time satellite images. Indian J. Sci. Technol. **9**(34), 1–11 (2016)
42. Zhao, H., Shi, Y.Q., Ansari, N.: Hiding data in multimedia streaming over networks. In: 8th Annual Communication Networks and Services Research Conference, pp. 50–55 (2010)
43. Khan, A., Sun, L., Jammeh, E., Ifeachor, E.: Content classification-based and QoE-driven video send bitrate adaptation scheme. In: Proceedings of the 5th International Conference on Mobile Multimedia Communications, MobiMedia (2009)
44. Horé, A, Ziou, D.: Image quality metrics: PSNR vs. SSIM. In: 20th International Conference on Pattern Recognition*,* pp. 2366–2369 (2010)