ISSN: 0067-2904

Medical Image Compression and Encryption Using Adaptive Arithmetic Coding, Quantization Technique and RSA in DWT Domain

Nehad Hameed Hussein*, Maytham A. Ali
Computer Techniques Engineering Department, Baghdad College of Economic Sciences University

Received: 18/7/2021 Accepted: 6/9/2021 Published: 30/5/2022

Abstract

Currently, medical images represent basis of clinical diagnosis and source of telehealth and teleconsultation processes. Exchange of these images can be subject to several challenges, such as transmission bandwidth scarcity, time delivery, fraud, tampering, modifying, privacy, and more. This paper will introduce an algorithm consisting of a combination of compression and encryption techniques to meet such challenges in medical images field. First, compression is done by applying the Adaptive Arithmetic Coding (AAC) technique and controllable frequency quantization process in Discrete Wavelet Transform. After that, encryption process is applied using RSA and SHA-256 algorithms to encrypt the compressed file and to create digital signature. Performance analysis has shown that the algorithm can produce high compression ratio with good image quality, whereas range of PSNR near 45 dB and SIM is 0.88 as average values. For the security analysis, we have adopted data encryption and digital signature to guarantee the main data security services including integrity, authentication, and confidentiality, making the algorithm secure against passive or active attacks.

Keywords: Compression, Encryption, Medical Image, RSA, PSNR, Quantization, Arithmetic Coding, DWT.

ضغط الصورة الطبية ثم تشفيرها باستخدام الترميز الحسابي التكيفي وتقنية التكميم في المجال المويجي المنفصل

نهاد حميد حسين*, ميثم عبد الحسين علي

قسم هندسة تقنيات الحاسوب, كلية بغداد للعلوم الاقتصادية الجامعة, بغداد, العراق

الخلاصة:

في الوقت الحاضر ،اصبحت الصور الطبية تمثل الاساس في التشخيص السريري ومصدر مهم في خدمات الرعاية الصحية عن بعد والاستشارات عن بعد. يمكن أن يخضع تبادل تلك الصور للعديد من التحديات ، مثل النقص في الترددات العالية التي تحتاجها لضمان توفير سرعة نقل عالية لها، الاحتيال ، العبث ، التعديل ، فضح الخصوصية ، والمزيد من تلك المشاكل. ستقدم هذه الورقة خوارزمية تتكون من مزيج من تقنيات الضغط والتشفير لمواجهة مثل هذه التحديات في مجال الصور الطبية. أولاً ، يتم الضغط عن طريق تطبيق تقنية التشفير الحسابي التكيفي وعملية تكميم التردد التي يمكن التحكم فيها في تحويل الموجة المنفصلة. بعد ذلك ، يتم تطبيق عملية التشفير باستخدام خوارزميات RSA و SHA-256 لتشفير الملف

*Email: nehad.h.hussein@baghdadcollege.edu.iq

المضغوط وإنشاء التوقيع الرقمي. أظهر تحليل الأداء أن الخوارزمية يمكن أن تنتج نسبة ضغط عالية مع جودة صورة جيدة ، في حين أن نطاق PSNR بالقرب من 45 ديسيبل و SIM هو 0.88 كقيم متوسطة. لتحليل الأمان ، اعتمدنا تشفير البيانات والتوقيع الرقمي لضمان خدمات أمان البيانات الرئيسية بما في ذلك ضمان الخصوصية والمصادقة والسرية ، مما يجعل الخوارزمية آمنة ضد الهجمات الخاملة والنشطة.

1 INTRODUCTION

The tremendous growth of ICT releases a wide range of applications in E-health like teleconsultation, tele-diagnosis, tele-radiology, etc. At the present time medical images may be stored locally for archive purposes or be shared for teleconsultation and tele-diagnosis purposes. Nevertheless, local storage structures cannot ensure the scalable storage abilities especially with massive number of medical images produced every day. For that problem, cloud storage can be adopted to offer scalable storage area with online data access. But keep in mind, huge cloud storage spaces should be purchased from providers. Away from that, data storage in remote cloud systems leads to many security issues. Healthcare organizations may anxiety data is vulnerable when sharing or storing it remotely. However, various security services such as confidentiality, privacy, integrity, authentication, and control access are required to be satisfied in cloud-based infrastructures [1] [2]. On the other side, the large size of medical images requires to be minimized before transmission or storage it. Data compression algorithms can use here to generate the output data with a smaller size [3]. Data compression techniques broadly are divided into two categories, lossless and lossy compression. first is a data compression technique that doesn’t eliminate any information from input data, while lossy techniques eliminate some of information from input data [4]. A higher compression ratio can be generated through using lossy compression methods without seeing destruction in source image data [5]. Using lossy compression techniques may create mistrust by many doctors or consultants where image information loss may cause loss of ROI or diagnostic areas. Even though lossy compression provides attractive quality but it may add medically undesirable objects into image. On the other hand, using lossless techniques will satisfy high quality but does not ensure a high compression ratio [6]. However, these problems lead to urgent need for an effective solution to meet possibility of data transmission with acceptable access time and sufficient security services. The solution to these problems can be achieved through combining data compression and encryption techniques. Through these techniques we will reduce size of data before transmission it and enhance its security in transmission and remote storage. In this regard, in this paper we will begin from the following question: How can we develop an algorithm to verify medical image security to ensure a high compression ratio while preserving good images quality? To achieve that we propose an integration of compression and encryption schemes. For compression scheme, Adaptive Arithmetic Coding (AAC) technique incorporated with adaptive quantization process in the discrete wavelet domain (DWT) will be used. First, the medical image will be compressed through applying DWT then quantization and AAC are applied. The quantization factors can be changed until reach the acceptable compression ratio and image quality. This allows the algorithm to be more flexible and adaptive. For encryption purpose, we used RSA and SHA-256 algorithms for encrypting data and creating a digital signature. After the compression process, security process will begin through creating a digital signature of compressed file and then secure it using sender’s secret key. After that, the compressed file with digital signature will be secure again using receiver’s public key. Here digital signature will verify the authenticity of both the data contents and its origin. As a result, the encryption of compete file will ensure the data will be secure in the transmission from both passive and active attacks. The paper details can be summarized as: Section 2 contains related works. Section 3 will detail contain literature used here. In section 4, proposed algorithm is presented. Also, section

5 will include experimental evaluation and security analyses. Finally, conclusions will be presented in sect. 6.

Literature Review

Transmission and sharing of medical images is a daily routine so, it is vital to find an efficient way to share them securely. This encourages researchers to make a huge effort for this purpose. The aim was to satisfy transmission bandwidth utilization with security approval. So, the authors were working to combine compression and encryption techniques in a single scheme. Three views for combining these techniques have been claimed: first compression tracked by encryption, second view starts with encryption, then compression, and finally, cooperative compression-encryption is suggested.

Encryption-Compression (E-C) Methods

These approaches start by encrypting images then compressing them. As general speaking, these schemes will take an extended processing time because data will be encrypted with redundant data that later may be eliminated in the compressing stage. This will provide an additional burden on processing time. However, in [7], they suggested compression of secured images using resolution progressive compression (RPC). DES algorithm tracked by Huffman coding and arithmetic coding. As a result, scheme was introduced an acceptable compression ratio, but data authentication and ownership are not guaranteed. In [8], they used 3D-AES and RSA cryptographic techniques for data encryption, with Shanon Fano is used as a lossless compression method. This scheme was provided a high level of data security and confidentiality. In [9], they suggested a joint scheme of symmetric encryption using random permutation algorithm and Haar and Daubechies wavelet lossy compression techniques. It ensured high security and compression ratio, but may cause something damage in the original image. In [10], they proposed the combination RSA and SPIHT methods as encryption and compression techniques. They concluded the usage of RSA would ensure high security with less processing time as compared with AES and 3D-AES algorithms. In [11], they used DWT, Singular Value Decomposition (SVD), and Huffman coding for medical image compression and encryption purpose. In [12], the researcher proposed partial image encryption and compression that takes on chaotic 3D combined with an adaptive thresholding method that is considered a lossy scheme. Here, least significant parts are lossy compressed by using a simple thresholding rule and arithmetic coding. The compression and security investigation demonstrates high-security levels for images in real time uses. However, according to [13] and [14], this scheme is not being better, and this back to two reasons: the processing time consumed in the redundant data encryption and second due to an attacker can access the original data due to more hints. In [15], data are encrypted through combination of RSA, Steganography and Huffman coding with DWT. They have ensured the algorithm efficiency through different metrics such as compression ratio, PSNR, SSIM, and compression saving. However, the algorithm lacks to authentication verification.

Compression-Encryption (C-E) Methods

These methods can minimize data size before encrypting it to ensure a lesser amount of processing time. In [16], they used DWT for image compression, and then DES encrypts the compressed images. They were intended to allow delivery of medical images in an efficiently and securely manner. Unfortunately, because DES, it is relatively slow to satisfy real-time constraint. In [17], they based on DWT as an image encryption method through encrypting the DWT coefficients then scrambling them by adjusting chaos sequence. In [18], the authors created a medical image encryption scheme using 2-D DWT and chaos transform. The image is DWTed then, low and high frequencies are scrambled by chaos transform. In [19], they suggested an algorithm for image compression-encryption using multilevel wavelet transform; then thresholding is practiced as a final step in the compression scheme. Security is achieved through decomposing the compressed image through 2-D DWT and scrambling them. Joined lossy and lossless algorithms with DCT, quantization, and Huffman coding to get a high compression ratio, then followed by asymmetric security algorithm (SHA1) for data encrypting purposes is suggested in [20]. In [21], they suggested use of adaptive compression to get an adequate compression rate. The suggested method can reduce data size through analyzing frequencies frequently and holding them in a tabular form. They used Milline transform approach for data security. In [22], a medical image compression-encryption system through compressive sensing, RSA, and SHA-256 is suggested. In [23], they suggested an algorithm for patient data security through using a combination of Hyper Chaotic-LZW and DWT-SVD for data compression and security. However, according to [5], [24] and [23], C-E methods will decrease data duplication which is vulnerable to cryptanalytic exploiting. So that the compression process can accelerate the encryption process; on the other side, the decryption method will provide corresponding plaintexts. Moreover, firstly compression can decrease efficiency of some attacks; brute force may take extended time [25].

Hybrid Compression-Encryption

These methods are based on joining a compression and encryption, or vice versa. This joint is not operated in sequence order. This model is predictable to merge tremendous properties of lossy and lossless methods and to equalize the weakness of symmetric and asymmetric cryptosystems, mainly the complexity and execution time are the main drawbacks of this approach [26-30]. However, from the previous studies, we develop an algorithm with following contributions.

1. The algorithm based on asymmetric key instead of symmetric encryption that has major disadvantage in distribution of secret key and takes longer processing time.
2. The algorithm enhances data integrity and authenticity using digital signature.
3. The compression algorithm is followed by an encryption process that allows to operating the algorithm as lossy or lossless without affecting decryption process.
4. The compression algorithm is adaptive through using AAC and adjustable quantization.
5. The control of DC values in DWT without compressing and quantizing ensures good image quality.

Research Methodology

Discrete Wavelet Transform (DWT)

DWT is mainly suitable for non-stationary signals analysis, image processing as an example. DWT decomposes image signal into four bands at different frequencies named low-frequency band (LL1), horizontal detail band (HL1), vertical detail band (LH1), and diagonal detail band (HH1). Moreover, LL1 can be DWTed again to provide another four sub-bands called LL2, HL2, LH2, and HH2. The LL band contains main features of image so that any modification here may be observable. The other three bands contain high frequencies that describe marginal information like edges and textures. Figure 1 illustrates a 2-DWT of MRI image [31]. Here, we will decompose medical image using 2-DWT. Because of the human visual system (HVS) is further sensitive to low frequencies (LL bands), high level bands of the 1-D DWT will be ignored where it has less sensitivity affect [32].

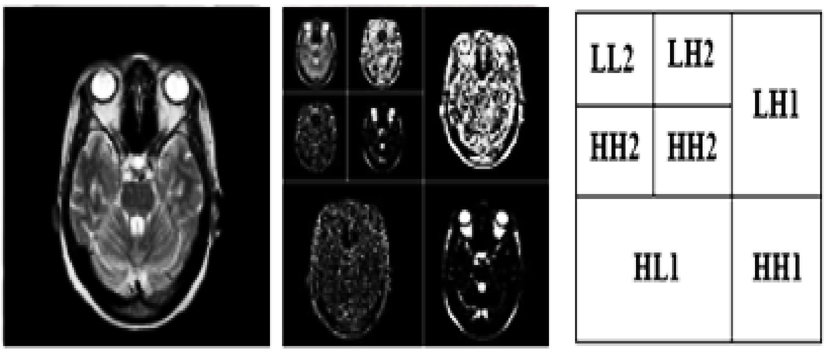


Figure 1-2-level DWT decomposition.

Adaptive Arithmetic Coding

As others entropy encoding schemes, arithmetic coding is created for lossless data compression. It is centered on assigning the least number of bits to most frequently used symbols, whereas most bits are assigned to most infrequently symbols [33]. There are two methods for data compression in arithmetic coding, static and adaptive method. In static method, symbols probability is computed through a large number of experimental data and high compression ratio is achieved. Meanwhile, symbols probability distributions may differ in each sequence, so compression efficiency is not greatest in static scheme. Moreover, the symbols probabilities table requires adding to the compressed file, which may cause a minor reduction in the compression efficiency [34]. To solve these weaknesses, an adaptive arithmetic coding technique is used that updates symbols' probability continuously while processing data. Thus, the probability distributions aren't transmitted to the AAC decoder.

Adaptive Quantization

Human Vision System (HVS) is proper at distinguishing slight variances in brightness over a quite large area, but it doesn't so respectable at differentiating particular strength of variance in high-frequency brightness areas [35]. This will allow decreasing amount of information by reducing high frequencies. This can be done just through applying quantization process by dividing each coefficient in frequency domain by a constant, then rounding to the nearest integer [21]. Quantization is applied to control compression quality through excluding some information of data that has been compressed. The excluded information is information that is considered to be at least important to HVS [36]. The formula of frequency quantization defined in Eq. (1). The inverse quantization can be calculated using equation (2) to restoring the coefficients to their original form. The formula of inverse quantization

$$\mathrm{Quantization} = \frac{\mathrm{DWT\ (i,j)}}{\mathrm{Quantization\ factor}} \qquad (1)$$

$$\mathrm{Inverse\ Quantization} = \mathrm{DWT\ (i,j)} * \mathrm{\ Quantization\ factor} \qquad (2)$$

Here quantization process is done on DWT sub-bands coefficients to minimize number of bits required to represent them. The output is a sequence of integer numbers that have to be set bit-by-bit. The quantization factors according to different bands are selecting to control quality of compressed image. For high compression ratio, large quantization factor is needed but this will produce lossy compression and cause to degrade image quality. If a lesser quantization value is selected, compression will be lossless. To maintain image quality, coefficients of LL2 sub-band need a smaller quantization value than coefficients of LH, HL, and HH bands.

Cryptographic Hash Function

A hash algorithm results in a fixed-size value called hash digest for any variable-length data as input. Any alteration that occurred for any segment (even one bit) in data will result in a different digest value; this will use to verify data integrity [5]. It must be a one-way function:

for any data *D*, basically, it is difficult to extract a message *M* such that *H (M) =D*. As well, it should be collision-free such that for any different data blocks *A* and *B*, there are different hash values *H (A) ≠ H(B)* [37]. Here, SHA-3 is utilized that can result in 256-bits digest.

RSA Encryption Algorithm

RSA is an asymmetric cryptographic scheme that requires two keys: private and public keys [5]. Data security is based on keys used, where strong keys make decryption process more difficult. It is not necessary for public key to be secret; on the other hand, private key should be secure so encrypted data can't be decrypted [17]. Here, we will use RSA algorithm for medical image encryption and digital signature creation to validate confidentiality, integrity, and origin authentication [38], [2]. RSA cryptosystem can be shortened in the following steps, where, c-cipher text, m–message [5].

1. Choose two prime numbers x and y, where x ≠ y.
2. Compute n = x × y.
3. Compute φ (n) = (x -1) × (y -1).
4. Choose integer e such that gcd (e, φ (n)) =1 such that 1 < e <φ (n).
5. Compute private key, d = e^{-1} mod φ(n)).
6. Public key = {e, n}.
7. Private key = {d, n}.
8. Encryption: c = m^e mod n.
9. Decryption: m = c^d mod n.

Performance Evaluation Metrics

Data compression ratio

Data compression ratio is used to measure data size reduction made by a data compression method [12]. As shown in equation (3), compression ratio is the ratio between uncompressed and compressed data size.

$$C.R = \frac{\text{Uncompressed Data Size}}{Compressed\ Data\ Size} \tag{3}$$

Data-rate saving

Data rate saving means the reduction in data-rate in relative to uncompressed data rate [9]. Eq. (4) shows how data rate saving can be calculated.

$$D.R.S = (1 - \frac{\text{Compressed Data Size}}{Unompressed\ Data\ Size})\ \% \tag{4}$$

Peak signal-to-noise ratio (PSNR)

PSNR is the relation between maximum possible power of signal and noise power that affects its quality [12]. The higher value of PSNR means better compression that results in higher matching between compressed and uncompressed image [4]. PSNR is computed using mean squared error (MSE) as shown in Eq. (6). Given $m \times n$ image *I* and its reconstructed one *K*, MSE is:

$$MSE \ = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I\ (i,j) - K\ (i,j)]\ ^2 \tag{5}$$

$$PSNR = 10.log_{10}\ \left(\frac{MAX^2}{MSE}\right) \tag{6}$$

where *MAX* is the maximum pixel value in the image.

Structural Similarity (SSIM)

SSIM computes similarity between two images through attempt to measure change in luminance, contrast, and structure of digital image. Its results more consistent with human perception than PSNR [30]. As long as SSIM value is nearest to 1, reconstructed image is exactly similar to original image [8]. The SSIM metric can be computed between the original image x and reconstructed image y by Eq. (7):

$$\mathrm{SSIM}(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \quad (7)$$

where µx is mean of x, µy is mean of y, σ^2x is variance of x, σ^2y is variance of y, and σ_{xy} is covariance of x and y.

4. MEDICAL IMAGES COMPRESSION-ENCRYPTION ALGORITHM

The proposed algorithm takes advantage of the AAC algorithm and the quantization technique which makes it more flexible and efficient to compress medical image that typically have large redundant data. Moreover, DWT itself provides additional compression to data. This makes ability to preserve image quality with high compression ratio the main feature of the suggested system. Also, because of possibility of transfer of medical images and their share between doctors, we took into consideration security of images over the Internet or in cloud storage; we made an algorithm based on method of RSA and SHA-256 algorithms. Figure 2 illustrates suggested compression-encryption algorithm.

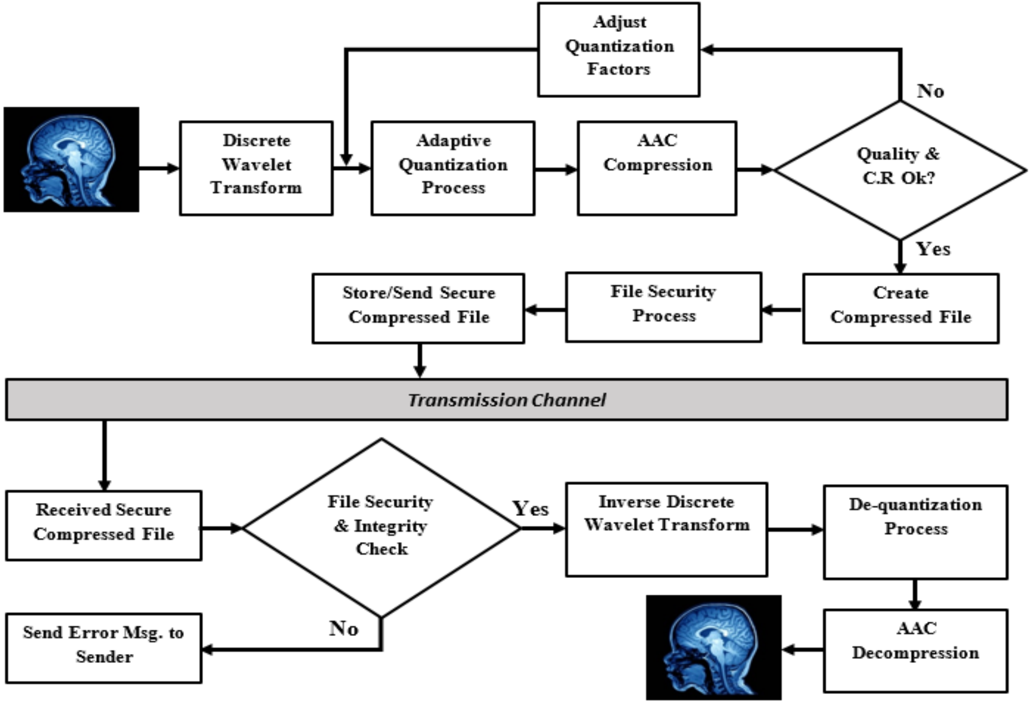

Adjust Quantization Factors
No
Discrete Wavelet Transform
Adaptive Quantization Process
AAC Compression
Quality & C.R Ok?
Yes
Store/Send Secure Compressed File
File Security Process
Create Compressed File
Transmission Channel
Received Secure Compressed File
File Security & Integrity Check
Yes
Inverse Discrete Wavelet Transform
De-quantization Process
Send Error Msg. to Sender
No
AAC Decompression

Figure 2-Compression-Encryption Algorithm.

4.1 *Compression Process*

The compression process benefits from frequency transformation, quantization process, and then the AAC technique to provide high compression ratio. It consists of the following steps:

INPUT: M × N uncompressed medical image, Quantization Factors (Qf1, Qf2),

OUTPUT: Medical Compressed Image File

Step 1: Load the Medical image to the algorithm as input image and determine the quantization factors.

Step 2: Convert the image color space from RGB to YCbCr

Step 3: Apply two levels DWT. This step produces 7-levels (LL2, HL1, LH1, HL1, HH1, HL2, LH2, HH2)

Step 4: Eliminate high-frequency components of first level (LH1, HL1, HH1)

Step 5: Quantizing the high-frequency levels of 2-DWT (LH2, HL2, HH2) by dividing coefficients by Qf2.

Step 6: Apply AAC on each quantized Sub-band (HL2, LH2, and HH2)

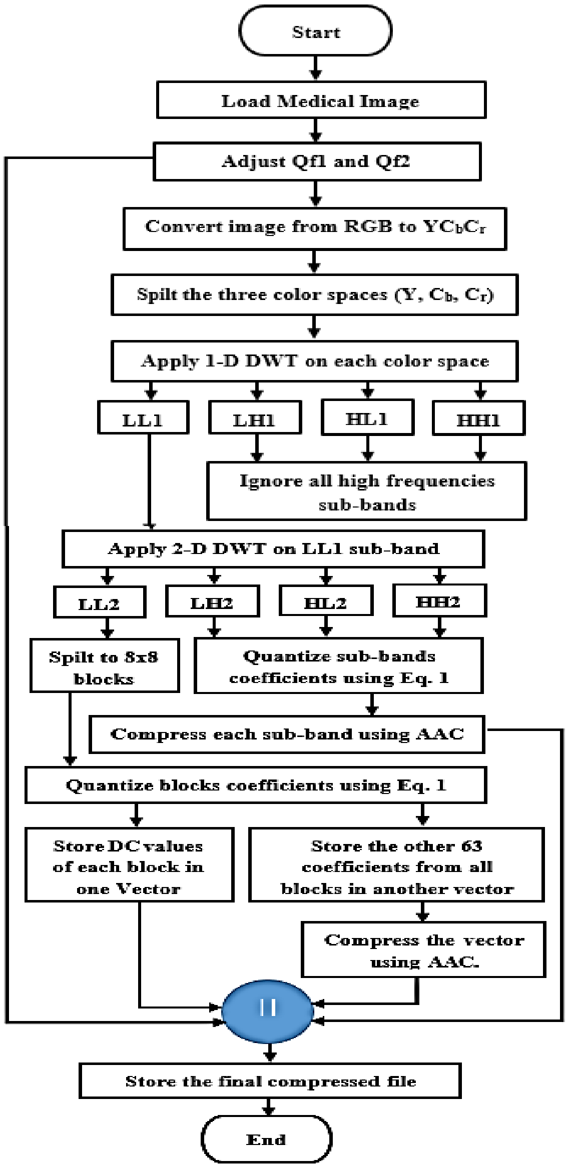
Step 7: Spilt LL2 sub-band into 8×8 blocks,

Step 8: Repeat for each 8×8 block

- Quantize the coefficients of each block (Divide each block by a Factor 1)
- All DC-values of each 8×8 block are stored in a new array called: DC-Values. This array will add in the header of compressed file.
- Other 63 coefficients from each 8×8 block are stored in one-dimensional vector.

Step 9: Concatenate all 8×8 blocks in one n×8×8 vector where n is the number of blocks.
Step 10: Compress the final vector values using AAC.
Step 11: Store the complete data in one file that will include quantization factors, LH2, HL2, HH2 compressed blocks, quantized DC-values of LL2 blocks, and the compressed [(n×8×8) – n] vector of 63 coefficients of LL2.

The DWT is used to eliminating high frequencies from medical image that cause to increase redundant data. On the other hand, LL2 sub-band generated in the 2-D DWT will be preserved here because it has main information of medical image that will ensure high quality after decompression process. Moreover, the DC value from each 8×8 block will be quantized only and stored in a separate vector without any further compression.


Start
Load Medical Image
Adjust Qf1 and Qf2
Convert image from RGB to YCbCr
Spilt the three color spaces (Y, Cb, Cr)
Apply 1-D DWT on each color space
LL1
LH1
HL1
HH1
Ignore all high frequencies sub-bands
Apply 2-D DWT on LL1 sub-band
LL2
LH2
HL2
HH2
Spilt to 8x8 blocks
Quantize sub-bands coefficients using Eq. 1
Compress each sub-band using AAC
Quantize blocks coefficients using Eq. 1
Store DC values of each block in one Vector
Store the other 63 coefficients from all blocks in another vector
Compress the vector using AAC.
||
Store the final compressed file
End

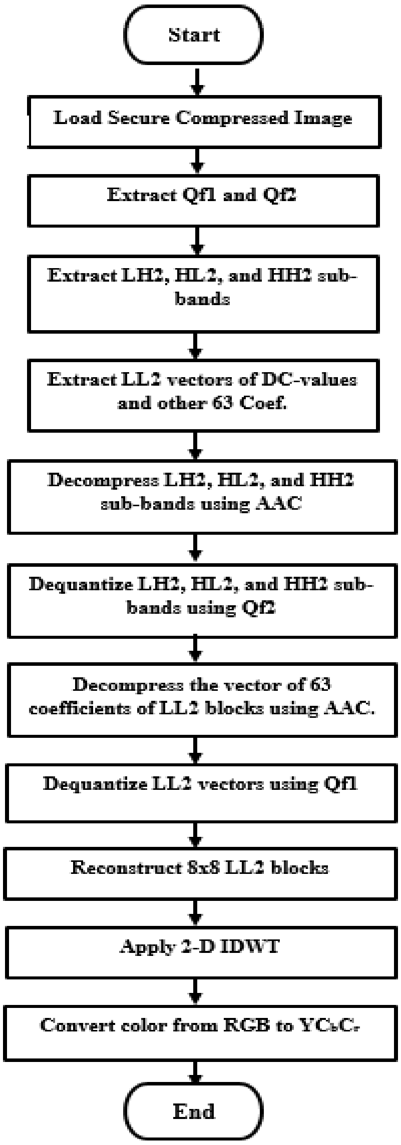

Start
Load Secure Compressed Image
Extract Qf1 and Qf2
Extract LH2, HL2, and HH2 sub-bands
Extract LL2 vectors of DC-values and other 63 Coef.
Decompress LH2, HL2, and HH2 sub-bands using AAC
Dequantize LH2, HL2, and HH2 sub-bands using Qf2
Decompress the vector of 63 coefficients of LL2 blocks using AAC.
Dequantize LL2 vectors using Qf1
Reconstruct 8x8 LL2 blocks
Apply 2-D IDWT
Convert color from RGB to YCbCr
End

Figure 3-Medical image compression process.

Figure 4-Medical image decompression process.

4.2 Decompression Algorithm

The suggested algorithm can be a lossy or lossless method. This depends on the coefficients. In the proposed algorithm the quantization coefficients (Qf1, Qf2) are stored in the final file.

INPUT: M×N compressed file. ***OUTPUT***: Medical Uncompressed Image
Step 1: Load the compressed file to the algorithm.
Step 2: Extract the main components of the compressed file that are: Qf1, Qf2, LH2, HL2, HH2 compressed blocks, Vector of quantized DC-values of LL2 blocks, and the compressed [(n×8×8) – n] vector of 63 LL2.
Step 3: Decompress the LH2, HL2, HH2 sub-bands using AAC.
Step 4: Dequantize the coefficients of LH2, HL2, HH2 blocks.
Step 5: Decompress the one-dimensional vector of 63 coefficients of LL2 blocks using AAC.
Step 6: Dequantize the values in the vector of DC-values of LL2 blocks
Step 7: Dequantize the values in the decompressed vector of the 63 coefficients of all LL2 blocks.
Step 8: Reconstruct 8×8 LL2 blocks.
Step 9: Apply 2-D IDWT.
Step 10: Convert the image color space from YCbCr to RGB.

4.3 Security Verification Process

As shown in Figure 5, we use public key algorithm to ensure data security and integrity through

1. Compute the hash value of the compressed file.
2. Encrypt the computed hash value using the sender private key.
3. Concatenate the computed hash value with the compressed file.
4. Encrypt the complete file using RSA with the receiver public key.

This process will satisfy digital signature that will ensure data authentication and integrity. To do that, the image's hash value is encrypted using sender's RSA private key. However, only the receivers who have the sender's RSA public key can decrypt the digital signature and verify the integrity of the send image. However, more than image integrity verification, encryption of digest value with sender's private key can ensure data was sent by authentic sender. For data confidentiality, combination of digital signature and image data should be encrypted, but receiver's public key will be used.

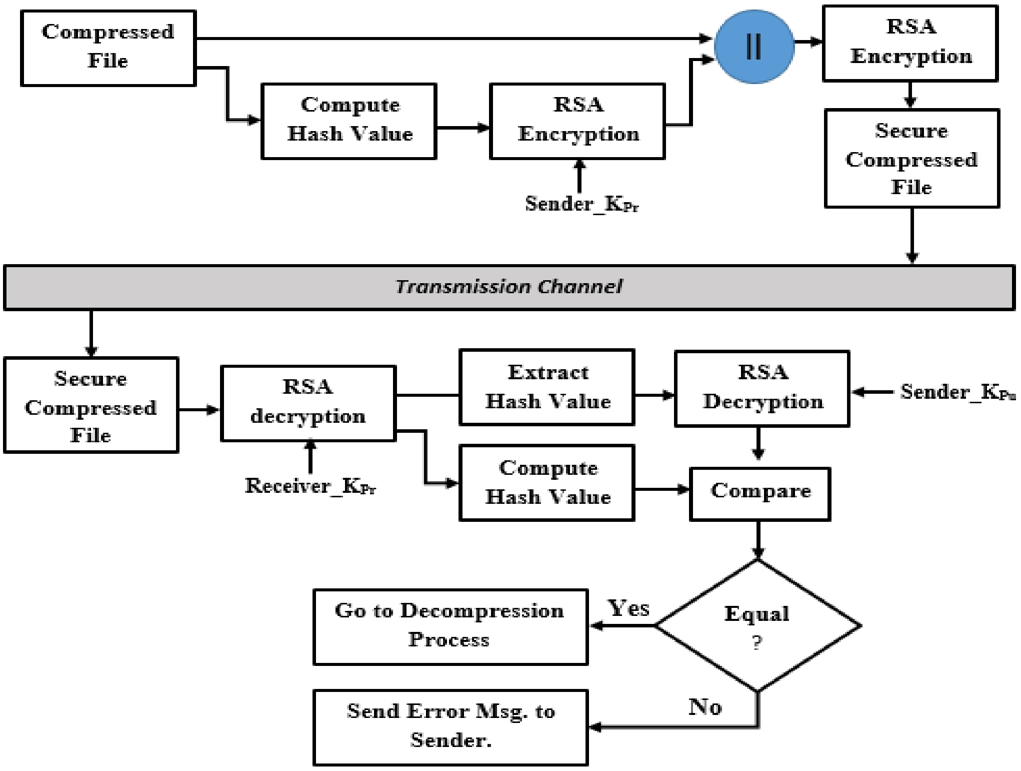


Figure 5-Medical Images Encryption Process

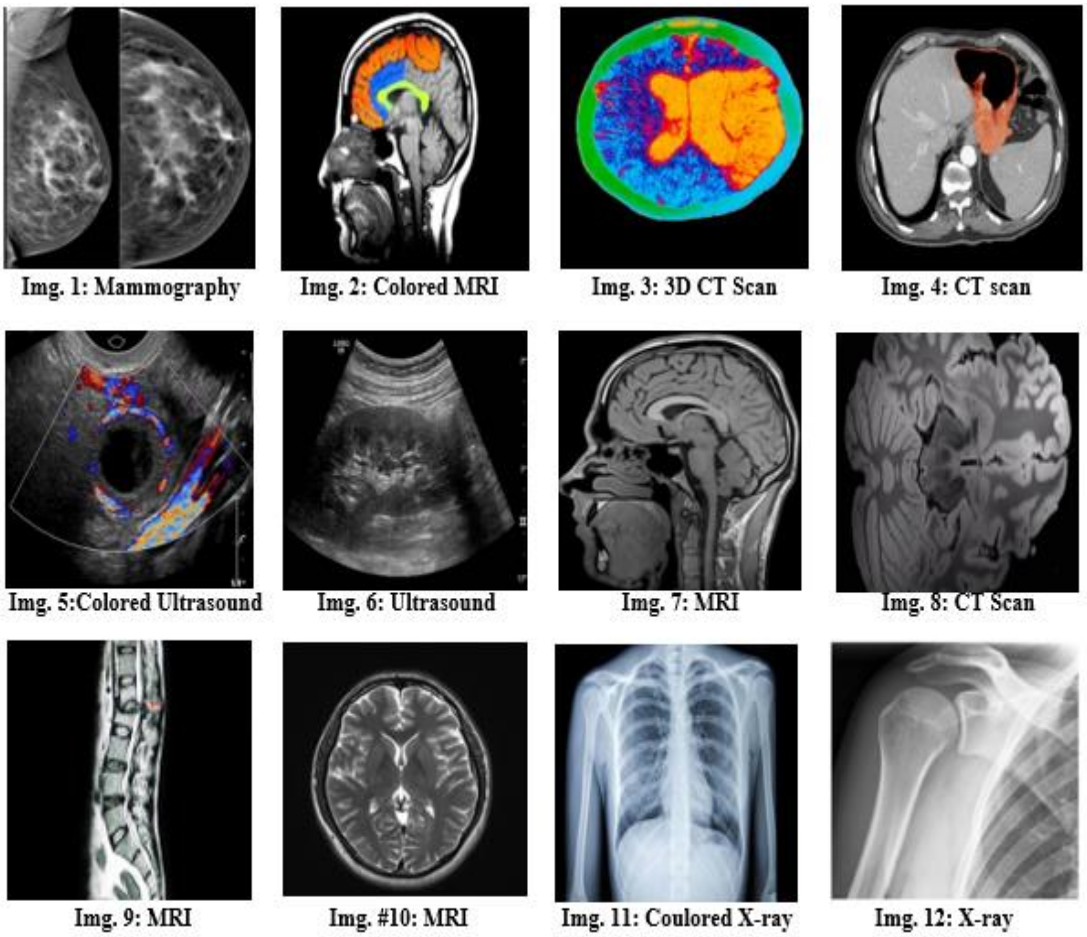
5. RESULTS AND ANALYSIS

The strength and efficiency of the proposed scheme are achieved through two types of analysis that are compression and security analysis. Compression analysis validates the compression process efficiency through applying the algorithm on many medical images and check mentioned metrics. For security analysis, security method is analyzed through validating the realization of many security services.

5.1 Compression Algorithm Analysis

However, we tested the algorithm on 12 medical images with different sizes from 700 KB to 19 MB. The images are acquired with different modalities like mammography, MRI, CT, Ultrasound, etc. The algorithm will be tested with different values of quantization values. However, Figure 6 shows the images used here.

First, we applied the algorithm with equalized quantization factors (Qf1=Qf2 =0.015) to ensure high image quality with acceptance compression ratio. From Table 1, we can conclude that storage saving may be 40% as average, which is acceptance value in medical image compression. Also, from the Table, we can see that the SSIM values close to 1 which means images have good quality. On another side, PSNR values are near to 50 that ensure decompressed images have good quality and tight quality of original image, as shown in Figure 7.



Img. 1: Mammography
Img. 2: Colored MRI
Img. 3: 3D CT Scan
Img. 4: CT scan
Img. 5:Colored Ultrasound
Img. 6: Ultrasound
Img. 7: MRI
Img. 8: CT Scan
Img. 9: MRI
Img. #10: MRI
Img. 11: Coulored X-ray
Img. 12: X-ray

Figure 6-Tests Medical Images

In Table 2, we applied the algorithm but with larger values for quantization factors that are 0.025. This would ensure a higher compression ratio and storage-saving that will be greater than 70% but, on the other side it will degrade image quality slightly as it can be observed in Figure 8. Also, the SSIM metric will move away from 1, and PSNR will be decreased.

In Table 3, we applied the algorithm but with larger values for quantization factors that are 0.5. This would cause to degrade image quality and corrupt the main features of medical images, as shown in Figure 9. On the other side, these values will ensure a higher compression ratio with storage saving near to 90% as average. However, as long as the quantization values will be higher, the compression ratio will increase but image quality will degrade more.

Table 1-Metrics factors with QF1=Qf2=0.015.

Image #	Actual Size	Size after compression	C.R	Storage Saving (%)	SSIM	PSNR
Image #1	19.060 KB	10200 KB	1.8686	46.48	0.93322	46.8115
Image #2	16,085 KB	8540 KB	1.8835	46.91	0.90295	45.6925
Image #3	12,647 KB	6916 KB	1.8287	45.32	0.93134	47.2173
Image #4	10,132 KB	5311 KB	1.9077	47.58	0.89918	46.4206
Image #5	9,589 KB	4530 KB	2.1168	52.76	0.92409	47.6093
Image #6	8,250 KB	4435 KB	1.8602	46.24	0.91302	46.9432
Image #7	4,085 KB	1779 KB	2.2962	56.45	0.91487	45.9225

Image #8	2,049 KB	1390 KB	1.4741	32.16	0.90021	46.7143
Image #9	910 KB	534 KB	1.7041	41.32	0.93112	45.7872
Image #10	850 KB	520 KB	1.6346	38.82	0.92293	46.9851
Image #11	800 KB	455 KB	1.7582	43.13	0.89822	45.9343
Image #12	761 KB	383 KB	1.8471	45.86	0.92200	46.6543

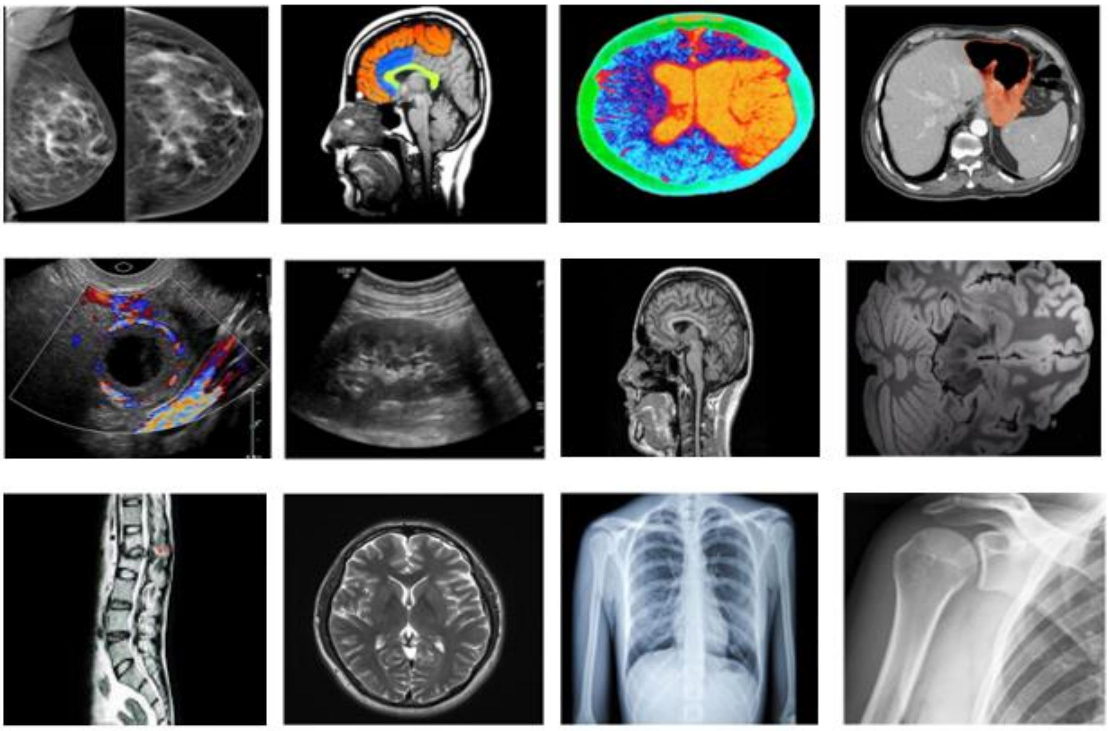


Figure 7-Tests images after compression with Qf1=Qf2=0.015.

Table 2-Metrics factors with QF1=Qf2=0.025

Image #	**Actual Size**	**Size after compression**	**C.R**	**Storage Saving (%)**	**SSIM**	**PSNR**
Image #1	19.060 KB	3,974 KB	4.829	79.29	0.78002	43.8115
Image #2	16,085 KB	3,536 KB	4.5489	78.02	0.78295	41.6925
Image #3	12,647 KB	3,227 KB	3.9191	74.48	0.73034	42.8230
Image #4	10,132 KB	3,062 KB	3.3089	69.78	0.75298	41.4248
Image #5	9,589 KB	2,554 KB	3.7545	73.37	0.74009	43.6001
Image #6	8,250 KB	2,097 KB	3.9342	74.58	0.80008	43.9036
Image #7	4,085 KB	1,139 KB	3.5865	72.12	0.69904	42.9129
Image #8	2,049 KB	846 KB	2.422	58.71	0.70028	41.7333
Image #9	910 KB	387 KB	2.3514	57.47	0.80012	42.9071
Image #10	850 KB	350 KB	2.4286	58.82	0.79913	43.0039
Image #11	800 KB	250 KB	3.201	68.75	0.70906	42.1299
Image #12	761 KB	212 KB	3.5896	72.14	0.68410	41.8544

However, as long as the quantization factors be at acceptable range will provide compressed images with acceptable C.R, SSIM, and PSNR. This leads to making the algorithm flexible and can be tested until reaching the required compression ratio or image quality. The PSNR and SSIM metrics will decrease as long as values of quantization factors are increased. But even with high values for QF1 and QF2 like, 0.5 or 0.8, image quality metrics SSIM and PSNR will be acceptable. In Figure 10 and 11, we compare the PSNR and SSIM for all selected images for different values for QF1 and QF2, respectively.

As testing for compression ratio, Figure 12 shows the comparison of C.R for the tested images with different values of QF1 and QF2. As shown from Figure 12 the C.R will increase when values of QF1 and QF2 are increased.

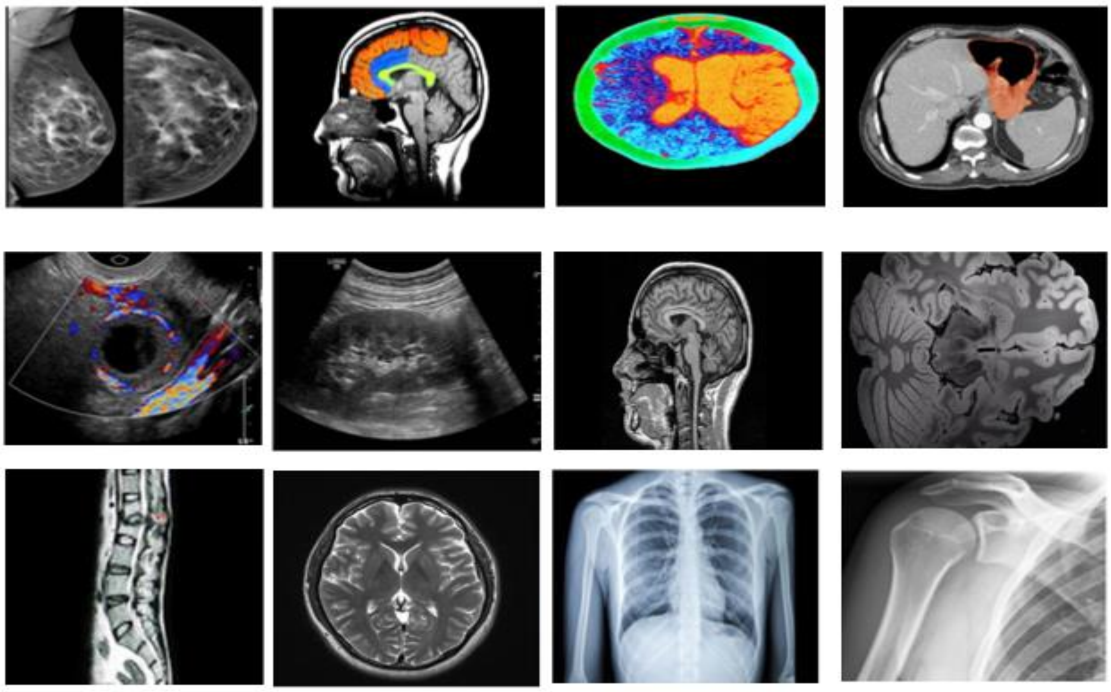


Figure 8-Tests images compression with QF1=QF2=0.025.

Table 3- Metrics factors with QF1=QF2=0.5

Image #	Actual Size	Size after compression	C.R	Storage Saving (%)	SSIM	PSNR
Image #1	19.060 KB	810 KB	23.5309	95.75	0.64049	31.0162
Image #2	16,085 KB	645 KB	24.938	95.99	0.61134	30.4501
Image #3	12,647 KB	476 KB	26.5693	96.24	0.61909	31.2380
Image #4	10,132 KB	346 KB	29.2832	96.59	0.58882	32.7753
Image #5	9,589 KB	309 KB	31.0324	96.78	0.60029	29.9870
Image #6	8,250 KB	210 KB	39.2857	97.45	0.63527	31.9114
Image #7	4,085 KB	173 KB	23.6127	95.76	0.62402	32.9035
Image #8	2,049 KB	109 KB	18.7982	94.68	0.59099	29.9593
Image #9	910 KB	90 KB	10.1111	90.11	0.6091	30.1002
Image #10	850 KB	83 KB	10.241	90.24	0.63713	29.5411
Image #11	800 KB	76 KB	10.5263	90.5	0.61009	29.8118
Image #12	761 KB	68 KB	11.1912	91.06	0.61009	30.9456

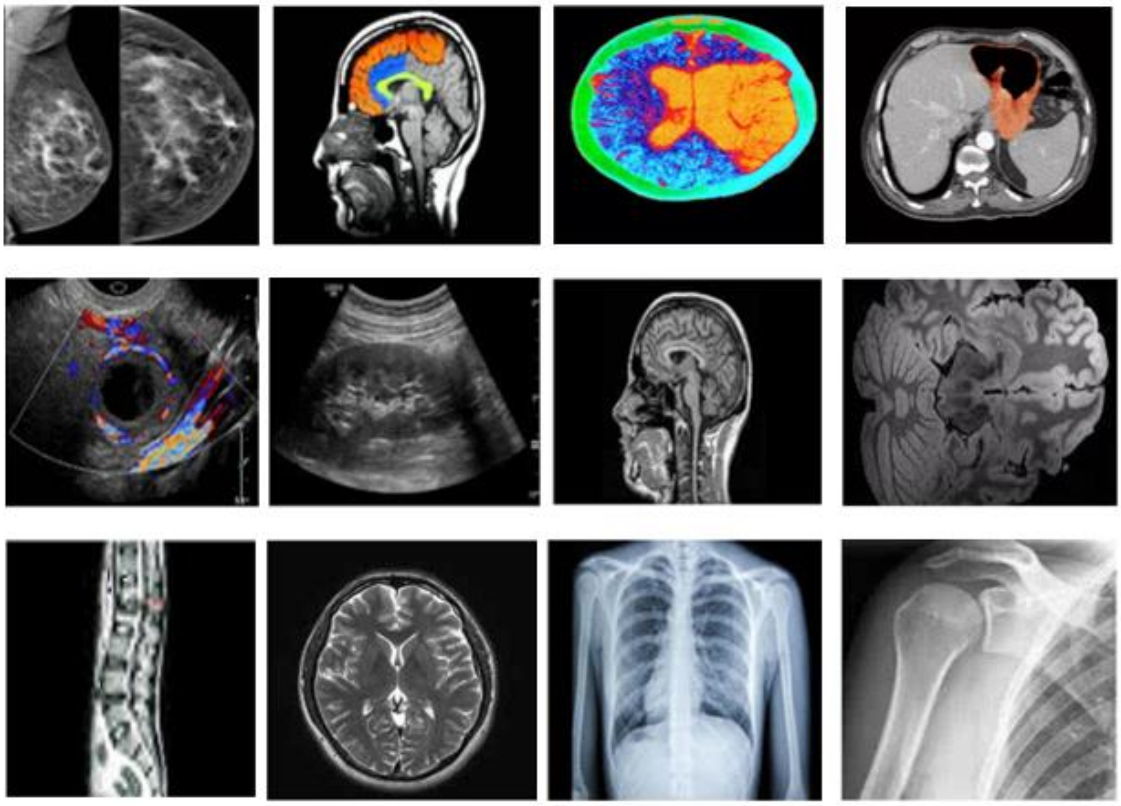


Figure 9- Tests images compression with QF1=Qf2=0.5

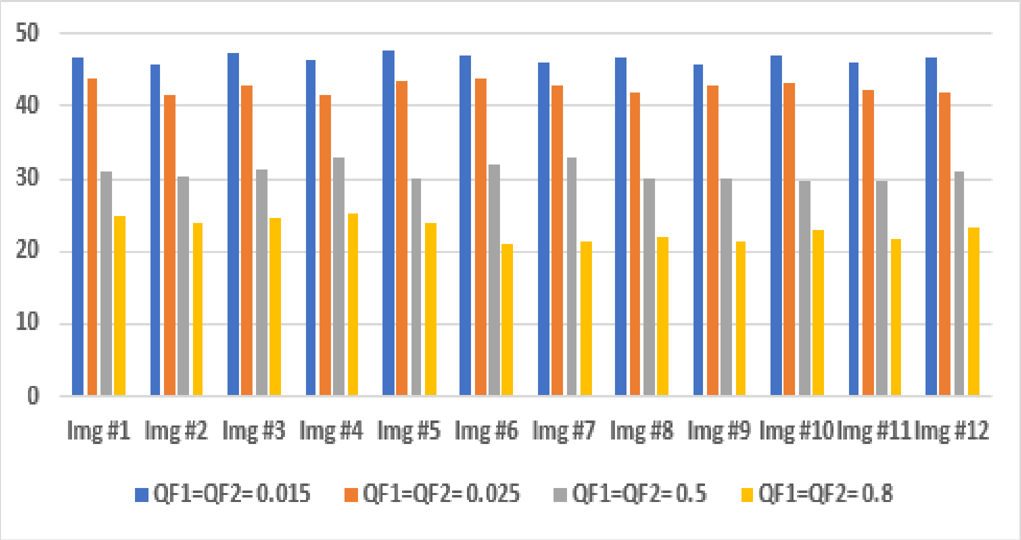


Figure 10- PSNR comparison among four selected quantization factors

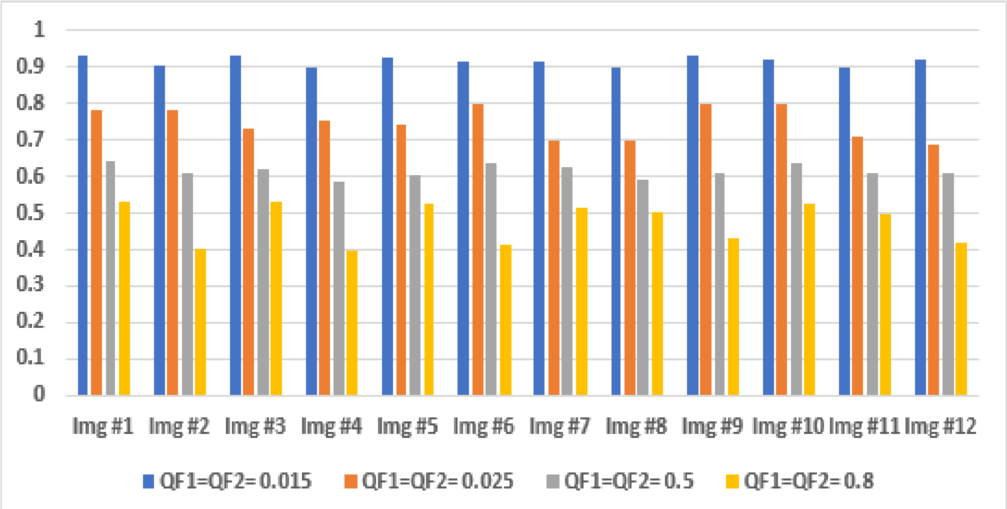


Figure 11-SSIM comparison among four selected quantization factors.

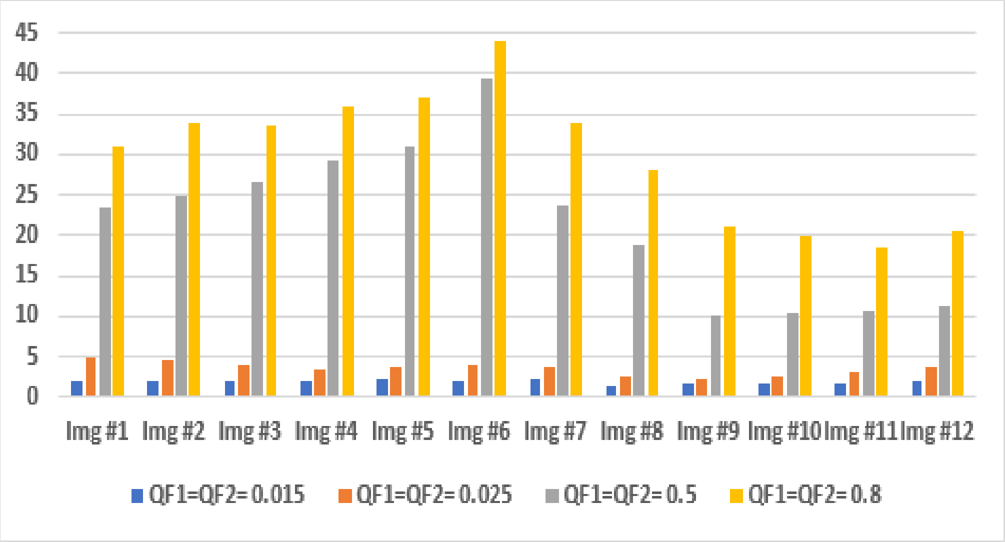


Figure 12- C.R comparison among four selected quantization factors.

5.2 Security Analysis

The use of a compression scheme ensures satisfactory storage-saving but cannot ensure any security over transmission channel, causing data vulnerable to hacking during its transmission. Although the compression method may guarantee a little security because it produces a scrambled data, just knowing the compression algorithm will reveal contents of image, so implementation of encryption algorithms is essential. In this scheme, data integrity is ensured, and its confidentiality and authentication are guaranteed. However, data disclosure and access to its contents require presence of encryption keys to be effective, so, on the assumption that keys are preserved secret, confidentiality and integrity are confirmed. Also, the algorithm derives its security from robustness of RSA and digital signature techniques. However, security analysis is realized through the following services.

5.2.1 Data Origin Authentication

It is crucial to receiver to make sure received images are accessed from sender who is indeed source of data and indeed verified. So, nobody has acted as an authenticated user and sent fake data. To achieve that, data source authentication is applied through creating a digital signature. Before sending compressed image, sender computes hash value and signs it using his private key. When the file has been received, receiver will compute its hash value and decrypt sent hash value using sender's public key and compare them. Unless using key pair of authenticated sender, the comparison process will fail because the key association will fail. This can prove data is really sent from sender himself and data source authenticity.

5.2.2 Confidentiality and Integrity

The proposed scheme guarantees medical images confidentiality and integrity over the network and in the storage. The medical image is encrypted using receiver's public key, so to decrypt data private key is needed to discover or modify data. This will inhibit attackers from disclosure contents of medical images. So, data confidentiality and integrity are well-kept to sender. Moreover, digital signature is used to verify data integrity. The digital signature can verify to detect any attempt to modify the image is noticeable. Any modification in the file over the Internet will produce various digital signature making all data disclosure attempts are exposed. If any attempt to modify secured image, as well as the digital signature, can be identified and the effect is passed to the sender.

5.2.3 Security Attacks

All teleconsultation or tele-diagnosis services are accessed through The Internet. There is a threat that data could be hacked over the Internet. An attacker may attempt to eavesdrop image in its transmission to disclosure or change its contents. Data encryption makes data unreadable, so any attack, either was passive or active, is prevented. Also, digital signature makes any passive or active attack are detectable. Brute force attacks are presented in different ways like: decrypting data and testing if the output is meaningful data. Here, the compression process will provide scrambled data so, attacker should first decrypt data and then decompress it to see if the meaningful output is presented. This will be time-consuming, and moreover, if attacker has no impression of data compression earlier, cryptanalysis will not solve it.

6. CONCLUSION AND FUTURE WORKS.

In this study, we have suggested a novel medical images compression–encryption system using DWT, quantization, adaptive arithmetic coding, RSA, and SHA-256 techniques. The proposed system preserves the main advantages inherent in compression and cryptography disciplines. The sequence of compression then encryption provides less processing time for the encryption process through eliminating the redundant data. Image compression process bases on multiple techniques that are DWT, AAC, and quantization process not only provides high C.R, but more of that it gives good quality of image after decompression process with a satisfying PSNR and SSIM metrics. On the other side, the encryption process will take advantages of RSA and SHA-256 to secure medical images and verify their integrity and authenticity through creating the digital signature. The experimental analysis shows that the suggested compression-encryption system efficiently compresses, and encrypts medical images from different modalities. The results verify that the suggested scheme is efficient, secure and robust to compress-encrypt images. It resists passive and active attacks like brute-force attacks and noise attacks. Also it can verify integrity and authenticity of image data in storage and on transmission channel.

For more efficiency, through exploits parallel or clustering processing system to enhance speed of compression-encryption process in real time applications. Also, adaptability of quantization factors should be enhanced automatically by using machine learning algorithms to determining the optimal quantization factors according to image quality.

References

[1] Sh., Akram, and B. Meshram, "Security issues in cloud computing," Intelligent Computing and Networking. Springer, Singapore. 63-77, 2021.

[2] Nehad H. Hussein, "Cloud-Based Efficient and Secure Scheme for Medical Images Storage and Sharing using ECC and SHA-3," In: 2nd Scientific Conference of Computer Sciences (SCCS), Iraq. IEEE, p. 109-115, 2019.

[3] Ibrahim, A., George, L. E., & Hassan, E. K., "Color Image Compression System by using Block Categorization Based on Spatial Details and DCT Followed by Improved Entropy Encoder" Iraqi Journal of Science, 3127-3140, 2020.

[4] Gan, Z., Chai, X., Zhang, J., Zhang, Y., & Chen, Y., "An Effective Image Compression–Encryption Scheme Based on Compressive Sensing (CS) and Game of Life (GOL)" Neural Computing and Applications, 32(17), 14113-14141, 2020.

[5] Arora, Kitty, and Manshi Shukla., "A Comprehensive Review of Image Compression Techniques" International Journal of Computer Science and Information Technologies 5, no. 2: 1169-1172, 2014.

[6] Bello-Cerezo, Raquel, Francesco Bianconi, Antonio Fernández, Elena González, and Francesco Di Maria, "Experimental Comparison of Color Spaces for Material Classification" Journal of Electronic Imaging 25, no. 6: 061406, 2016.

[7] C. MariSelvi and A. Kumar, "A Modified Encryption Algorithm for Compression of Color Image" International Journal of Recent Development in Engineering and Technology, vol. 2, no. 3, pp. 94–98, 2015.

[8] N. A. Kale and S. B. Natikar, "Secured Mobile Messaging for Android Application, " International Journal of Advance Research in Computer Science and Management Studies, vol. 2, no. 11, pp. 304– 311, 2014.

[9] H. K. Aujla and R. Sharma, "Designing an Efficient Image Encryption Then Compression System with Haar and Daubechies Wavelet" International Journal of Computer Science and Information Technologies (IJCSIT), vol. 5, no. 6, pp. 7784–7788, 2015.

[10] .M. Arunkumar and S. Prabu, "Implementation of Encrypted Image Compression using Resolution Progressive Compression Scheme" International Journal of Computer Science and Mobile Computing (IJCSMC), vol. 3, no. 6, pp. 585–590, 2016.

[11] Kumar, Manoj, and Ankita Vaish, "An Efficient Encryption-Then-Compression Technique for Encrypted Images Using SVD," Digital Signal Processing: 81-89, 2017.

[12] Darwish Saad Mohamed, "A modified Image Selective Encryption-Compression Technique Based On 3D Chaotic Maps and Arithmetic Coding," Multimedia Tools and Applications: 1-24, 2019.

[13] Setyaningsih, Emy, and Retantyo Wardoyo, "Review of Image Compression and Encryption Techniques," International Journal of Advanced Computer Science and Applications 8, no. 2: 83-94, 2017.

[14] Mahendiran, N. and Deepa, C. A, "Comprehensive Analysis on Image Encryption and Compression Techniques with the Assessment of Performance Evaluation Metrics" SN Computer Science, Springer, 2.1: 1-12, 2021.

[15] Wahab, O. F. A., Khalaf, A. A., Hussein, A. I., & Hamed, H. F., "Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques" IEEE Access, 9, 31805-31815, 2021.

[16] P. Dang and P. Chau, "Image Encryption for Secure Internet Multimedia Applications" IEEE Trans. on Consumer Elect., 46: 395-403, 2006.

[17] C. Pang, "An Image Encryption Algorithm Based on Discrete Wavelet Transform and Two Dimension Cat Mapping, " International Conference on Networks Security, Wireless Communications and Trusted Computing. 2, 711-714, 2009.

[18] W. Juan, "Image Encryption Algorithm Based on 2-D Wavelet Transform and Chaos Sequences" Intrernational. Conference on Computational Intelligence and Software Engineering, 2020.

[19] Samson, Ch, and V. U. K. Sastry, "An RGB Image Encryption Supported by Wavelet-Based Lossless Compression," International Journal of Advanced Computer Science and Applications 3, no. 9, 2012.

[20] W. M. Rahmawati, A. Saikhu, and A. E. Kompresi, "Implementation of Algorithm for Medical Images Compression-Encryption using DCT and SHA-1, " Journal of Technologies POMITS, vol. 2, no. 1, pp. 1–4, 2013.

[21] Sudesh, A. Kaushik, and S. Kaushik, "A Two Stage Hybrid Model for Image Encryption and Compression to Enhance Security and Efficiency, " in International Conference on Advances in Engineering & Technology Research (ICAETR -2014), pp. 1–5, 2014.

[22] L.H. Gong, K.D. Qiu, C.Z. Deng, N.R Zhou, "An Optical Image Compression and Encryption Scheme Based On Compressive Sensing And RSA Algorithm" Opt Lasers Eng, 121, PP. 169-180, 2019.

[23] Anand, Ashima, and Amit Kumar Singh, "An improved DWT-SVD domain watermarking for medical information security" Computer Communications 152: 72-80, 2020.

[24] M. Sharma and S. Gandhi, "Compression and Encryption: An Integrated Approach" International Journal of Engineering Research & Technology (IJERT), vol. 1, no. 5, pp. 1–7, 2012.

[25] Abdmouleh, Med Karim, Ali Khalfallah, and Med Salim Bouhlel, "Crypto-compression scheme based on the DWT for medical image security," International Journal of Computational Vision and Robotics 9, no: 340-350, 2019.

[26] J. Ahmad, M. A. Khan, S. O. Hwang, and J. S. Khan, "A Compression Sensing and Noise-Tolerant Image Encryption Scheme Based on Chaotic Maps and Orthogonal Matrices" Neural Computing and Applications, 2016.

[27] T. Chen, M. Zhang, J. Wu, C. Yuen, and Y. Tong, "Image Encryption and Compression Based on Kronecker Compressed Sensing and Elementary Cellular Automata Scrambling" Optics & Laser Technology, vol. 84, pp. 118–133, 2016.

[28] J. Deng, S. Zhao, Y. Wang, L. Wang, H. Wang, and H. Sha, "Image Compression-Encryption Scheme Combining 2D Compressive Sensing with Discrete Fractional Random Transform" Multimedia Tools and Applications, 2016.

[29] N. Zhou, S. Pan, S. Cheng, and Z. Zhou, "Image Compression–Encryption Scheme Based on Hyper-Chaotic System and 2D Compressive Sensing" Optics & Laser Technology., vol. 82, pp. 121–133, 2017.

[30] M. Hamdi, R. Rhouma, and S. Belghith, "A Selective Compression-Encryption of Images Based on SPIHT Coding and Chirikov Standard Map" Signal Processing, vol. 131, pp. 514–526, 2018.

[31] Jagannadham, D. B. V.; Raju, G. V. S.; Narayana, D. V. S., "Novel performance analysis of DCT, DWT and fractal coding in image compression" In: Data Engineering and Communication Technology. Springer, Singapore. p. 611-622, 2020.

[32] Mohammed, F. G., and Al-Dabbas, H. M., "Application of WDR Technique with Different Wavelet Codecs for Image Compression" Iraqi Journal of Science, 2128-2134, 2018.

[33] Yousif, Ruaa Ibrahim, and Nassir Hussein Salman, "Image Compression Based on Arithmetic Coding Algorithm," Iraqi Journal of Science, 329-334, 2021.

[34] Chang, Jer-Ming, Jian-Jiun Ding, and Heng-Sheng Lin, "Adaptive Prediction, Context Modeling, and Entropy Coding Methods for CALIC Lossless Image Compression," In 2019 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS), pp. 349-352. IEEE, 2019.

[35] Kawaguchi, Naoki, and Atsushi Osa., "Simulation of Image Enhancement by Stochastic Resonance in The Human Vision System," In International Workshop on Advanced Image Technology (IWAIT), vol. 11049, p. 1104933, 2019.

[36] Ammah, Paul Nii Tackie, and Ebenezer Owusu., "Robust Medical Image Compression Based On Wavelet Transform and Vector Quantization," Informatics in Medicine Unlocked 15: 100183, 2019.

[37] Nehad H. Hussein, "Digital Image Authentication Algorithm Based on Fragile Invisible Watermark and MD-5 Function in the DWT Domain" Journal of Engineering, 21.4: 21-41, 2015.

[38] Agrawal, S., Patel, M., & Sinhal, A., "An Enhance Security of the Color Image Using Asymmetric RSA Algorithm" In Proceedings of International Conference on Communication and Computational Technologies (pp. 279-286). Springer, Singapore, 2021.