Sādhanā (2019) 44:28
https://doi.org/10.1007/s12046-018-1013-9

Joint medical image compression–encryption in the cloud using multiscale transform-based image compression encoding techniques

S P RAJA

Department of Computer Science and Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai 600 062, India
e-mail: avemariaraja@gmail.com

MS received 20 December 2017; revised 1 September 2018; accepted 30 September 2018; published online 19 January 2019

Abstract. The recent years have witnessed rapid strides in the use of cloud computing and its countless applications. A cloud can contain massive volumes of multimedia data in the form of images, video and audio. Cloud computing platforms confront challenges in terms of data confidentiality, message integrity, user authentication and compression. Multimedia data needs plenty of storage capacity. Consequently, there is a need for multimedia data compression to reduce data size. Compression techniques are quite reliable, offering benefits to organizations dealing with metasized data in the cloud. Compressing large quanta of data leads to superior utilization of cloud storage. Compression techniques can compress data used for storage and transmission, yet compression alone is inadequate because multimedia data shared should, of necessity, be secure. Therefore, both multimedia compression and security are mandatory in the cloud. The chief goal of this paper is to propose a new framework, comprising multiscale transforms, public key cryptography and appropriate encoding techniques, that performs joint medical image compression and image encryption in the cloud. Multiscale transforms play a lead role in image compression, and the ones discussed in this paper include wavelet, bandelet, curvelet, ridgelet and contourlet transforms. Wavelet transforms offer robust localization both in terms of time and frequency domains. Bandelet transforms offer natural images geometric regularity to help improve the efficiency of representation. Curvelet transforms handle curve discontinuities well, with ridgelet transforms being the core idea behind curvelets. Contourlet transforms capture smooth contours and edges at any orientation. The Rivest-Shamir-Adleman (RSA) algorithm is used to encrypt images to provide maximum security when they are being transferred. Encoding techniques involved in this paper comprise the Embedded Zerotree Wavelet (EZW), Set Partitioning in Hierarchical Trees (SPIHT), Wavelet Difference Reduction (WDR), and Adaptively Scanned Wavelet Difference Reduction (ASWDR). Performance parameters such as peak signal to noise ratio (PSNR), mean square error (MSE), image quality index and structural similarity index (SSIM) are used for evaluation. It is justified that the proposed framework compresses images securely in the cloud.

Keywords. Cloud computing; RSA; bandelet; wavelet; curvelet; countourlet; ridgelet; SPIHT; EZW; WDR; ASWDR.

1. Introduction

Cloud computing [1] is, arguably, the fastest-growing internet technology around today. A cloud in cloud computing can be termed as a set of hardware, networks, storage, services, and interfaces that combine to deliver assorted aspects of computing as a service. It is unnecessary to install hardware or software to use the cloud: rather, cloud applications can be used as services as and when needed. The cloud comprises volumes of computing resources, storage and data. Cloud computing is a type of computing used to share resources among cloud users. Given that lots of people and companies use services from the cloud, it is crucial to provide security as well as fast transmission/sharing of data. Consequently, cloud computing faces two key challenges: storage and security. Compression techniques are used to reduce the size of the data in the cloud and make for efficient transmission. In this paper, image compression [2] – a process to reduce storage space taken up by images – in the cloud is discussed. Image compression techniques can be classified into lossless and lossy techniques. With lossless compression, the original image is recovered in exactly the same way after decompression. Lossy compression suffers marginal data loss in the decompressed image.

1.1 *Medical image compression and encryption*

The usual steps involved in compressing an image are sub-band decomposition, quantization and encoding. Subband decomposition involves the application of the appropriate transform to the input image to obtain coefficients. Quantization refers to the process of approximating a continuous set of values in the image data with a finite (preferably small) set of values. Encoding is the process of removing statistical redundancy in a given source. Another challenge in cloud computing is data confidentiality – providing data the security it requires. Therefore, following sub-band decomposition, an appropriate cryptography algorithm is applied. Cryptography can be divided into two major categories, symmetric and asymmetric. This paper uses asymmetric key cryptography, which means that two different keys are used for encryption and decryption purposes. Encryption is the process of converting plaintext into ciphertext and decryption is its reverse.

1.2 *Related work*

Subband decomposition of an image is performed by a mathematical transform. A transform is indented to decorrelate input pixels in image compression. Certain lossy image compression techniques are based on discrete wavelet transform [3–5]. In paper [6], a compression algorithm based on the wavelet transform, the key point of the method being to reorder pixels to make way for a very smooth 1D signal. Various image compression techniques under wavelet domain is evaluated [7].

Curvelet transform [8] provides an optimally sparse representation of objects displaying a curve-punctuated smoothness. Curvelets also have microlocal features, making them especially suited to certain reconstruction problems with missing data. Elaiwat *et al* [9] presented a robust, single modality feature-based algorithm for face recognition by using curvelet transform features. In this paper, using curvelet coefficients, the authors discovered the key points in a face.

Do and Vetterli introduced the contourlet transform [10], used in image enhancement and texture classification. A new approach to the problem of video super resolution was proposed based on the contourlet transform, used to carry out preprocessing functions and obtain coefficients [11]. Two pan-sharpening methods was proposed for representing directional information and capturing the intrinsic geometrical structures of objects, based on the contourlet transform [12]. A new approach was proposed for multiresolution fusion using the contourlet transform to provide better directional edges in an image [13].

Ridgelet transform was introduced [14] as a sparse expansion for functions on continuous spaces that are smooth, away from discontinuities along lines. Le Pennec and Mallat [15] introduced the bandelet transform. It is an excellent multiscale geometric analysis method utilizing the known geometric information of images to improve approximation ability. Compared with other transforms, it has unique features such as multiscale analysis, time-frequency localization, directionality and anisotropy. It also offers certain properties like strict sampling and adaptability, indispensable for image representation.

After image decomposition, a public key cryptography methodology titled RSA is applied to the coefficients obtained. Rivest-Shamir-Adleman proposed a public key cryptosystem named RSA [16] using two keys, one for encryption and the other for decryption. An RSA cryptosystem was proposed with a large key size and modular multiplier architecture [17]. A scheme referred to as a dual RSA was proposed [18] with the advantage of reducing the need for the keys' storage requirements. The dual RSA provides blind signatures and authentication and, compared to the normal RSA, better security. Various approaches were presented to implement RSA crypto-accelerators with four fundamental architectures, demonstrating that RSA can be applied in image processing and to error-correcting codes [19].

After the coefficients are encrypted, a coding process is applied to reduce the overall number of bits required to represent an image. For coding, the EZW algorithm was proposed [20] which is one of the first and most powerful encoding algorithms built on wavelet-based image compression. The core of the EZW compression is the exploitation of self-similarity across different scales of an image wavelet transform.

Said and Pearlman introduced [21, 22] the set partitioning in hierarchical trees (SPIHT) technique, an efficient yet computationally simple image compression algorithm, using which the highest PSNR values for given compression ratios for a variety of images can be obtained.

A drawback of the SPIHT is that it implicitly locates the position of significant coefficients. It is difficult to perform operations, such as region selection on compressed data, which depend on the exact position of significant transform values. Another encoding technique called the wavelet difference reduction (WDR) was proposed by Tian and Wells [23] and encodes the locations of significant wavelet transform values. The WDR can produce perceptually superior images, especially at high compression ratios.

James Walker [24, 25] introduced the adaptively scanned wavelet difference reduction (ASWDR) algorithm, used to modify the scanning order used by the WDR to enhance performance. The ASWDR adapts the scanning order to predict the locations of new, significant values. If a prediction is right, the output specifying that location will only be a sign of the new significant value, and the reduced binary expansion of the number of steps will be empty. A secure encrypted compression method was proposed that achieves a good compression ratio [26].

1.3 *Motivation and justification of the proposed approach*

A novel feature-based photo album compression scheme was proposed [27] for cloud storage using local features instead of pixel values to discover relationships between images. This method adapts content-based feature matching. A new compression scheme was proposed [28] which does not compress images pixel by pixel but describes them instead and retrieves them from the database through descriptors. The wavelet transform is used to compress images in cloud computing. This paper uses the wavelet transform and different multiscale transforms to analyze their performance in compressing images in the cloud. A hierarchical scheduling optimization scheme in the hybrid cloud was proposed [29] which takes advantage of cloud users' interaction.

Performance of wavelets and bandelets were analyzed [30] by comparing them with conventional coding methods. In [31], features obtained from the contourlet transform are compared with those from the wavelet transform for image texture classification, showing that the accuracy of the contourlet transform in image acquisition conditions is better than that of the wavelet transform. A new method for image denoising was proposed [32] by combining wavelet and curvelet transforms.

Offering users data security is the biggest challenge in cloud computing. Cloud computing adoption framework (CCAF) was devised [33] for securing cloud data. The CCAF framework blocks Trojans and Sundry viruses. Issues and challenges confronting cloud computing security were presented [34, 35] alongside ideas on the development of cloud security methods. Security issues in cloud computing platforms were presented [36] taking into consideration five parameters including confidentiality, integrity, availability, accountability, and privacy-preservability. A survey of all attribute-based encryption (ABE) schemes was performed [37] and created a comparison table of the key criteria for these schemes in CLOUD applications. A scheme titled ciphertext-policy attribute-based ENCRYPTION (CP-ABE) was proposed [38] for encryption that can rise to the challenge of secure data sharing in CLOUD COMPUTING WITH an efficient file hierarchy attribute-based encryption scheme.

Compression along with security becomes a great deal for the researchers. A review of compression in information security is presented [39] in the aspects of theoretical and application oriented. Simultaneous compression and encryption in an image is one of the most widespread applications. Medical image compression should not affect the quality of the image. A predictive image coding method is proposed [40] which protect the quality of the medical image even after performing the compression by preserving the diagnostically important region of the given medical image. Self encryption methods [41] were also proposed in image processing applications.

From the above literature survey, it is plain that compression and security are the greatest challenges in cloud computing. Hence the motivation in this paper is to present a new holistic methodology for both compression and security in the cloud. The proposed methodology provides excellent security and image compression results.

1.4 *Outline of the proposed work*

The proposed work has adopted the following method. Medical images are taken, the selected transform applied to it and the coefficients obtained. Later, the image compression encoding technique is applied to get the compressed bits. The reverse is done to revert to the input image. The outline of the approach is shown in figure 1.

1.5 *Organization of the paper*

The rest of the paper is organized as follows. Multiscale transforms are discussed in section 2, and the RSA algorithm in section 3. Image compression encoding techniques are discussed in section 4, and the experimental results are given in section 5. Performance evaluation is presented in section 6, and conclusions are provided in section 7.

2. Multiscale transforms

2.1 *Discrete Wavelet Decomposition (DWT)*

The DWT is computed by successive low-pass and high-pass filters, applied to each row of an image one by one so that low-frequency components and high-pass components are computed. The low-pass filter is related to the scaling function that produces coarse approximations. High-pass components are placed beside low-pass ones. The high-pass filter produces detailed information on an image, a procedure done for all rows to obtain wavelet coefficients. In one level DWT, the resultant image is decomposed into four subbands: LL, HL, LH and HH. Here, L = Low and H = High. The LL subband has significant information and all the others less so. Wavelet transforms have numerous applications in image denoising, fingerprint verification, speech recognition and medicine.

2.2 *Curvelet and ridgelet transforms*

The ridgelet transform is a two-step process, involving the calculation of the discrete Radon transform and an application of a wavelet transform. The primary application of the ridgelet transform is to represent objects with line singularities, and is used in other applications where images contain edges and straight lines. The curvelet transform, on the other hand, is most suitable for objects with curves.

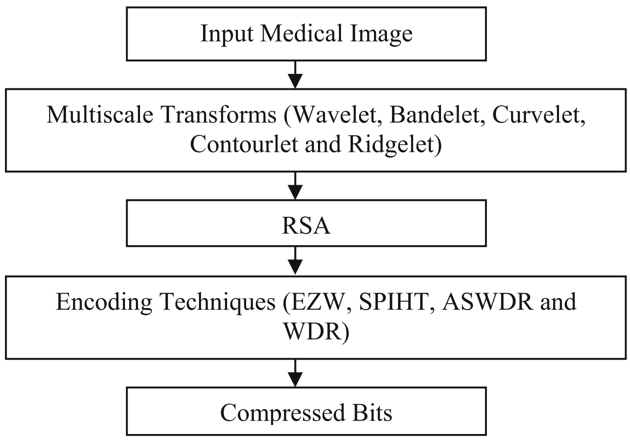

Figure 1. Outline of the proposed approach.

Multiple wavelet coefficients are required to account for edges in the ridgelet transform but the minimal number is needed to account for them in the curvelet transform. For the curvelet transform, the image is initially partitioned into sub-images and the ridgelet transform applied to them. The curvelet transform has applications in image denoising, image enhancement and compressed sensing.

Steps in the curvelet transform include subband decomposition, smooth partitioning, renormalization and ridgelet analysis. Subband decomposition involves the given input image being filtered into subbands, a step used to divide the image into several resolution layers, each containing details of different frequencies. Smooth partitioning is a collection of smooth windows, localized around dyadic squares. With renormalization, each square in the previous step is renormalized to unit scale. Finally, each square is analyzed with the ridgelet system.

2.3 *Contourlet transform*

The contourlet transform comprises two major stages: subband decomposition and directional transform. The Laplacian pyramid (LP) was used for subband decomposition and directional filter banks (DFB) for directional transform. In the Laplacian pyramid, the spectrum of the input image is divided into lowpass and highpass subbands. The lowpass subband is downsampled by two, both horizontally and vertically, and passed onto the next stage. The highpass subband is further separated into several directions by directional filter banks. The contourlet transform has applications in image enhancement, radar despeckling and texture classification.

2.4 *Bandelet transform*

First-generation bandelet transform was introduced [42] based on a 2-D separable wavelet transform. The given image is initially segmented into macroblocks like a quadtree structure, and the geometric flow of each macroblock determined. Wavelet functions are warped to adapt to the flow line of each macroblock and bandeletization performed to resolve problems with the vanish moment of the scaling function. Finally, a separable 2D wavelet transform is performed.

Second generation bandelet transforms – used in such areas as image fusion, image denoising and image segmentation – involve the initial performance of the multiscale transform with 2-D orthogonal or biorthogonal wavelets. The best quadtree decomposition is constructed for each highpass subband through the quadtree division method and the bottom-up CART (classification and regression trees) algorithm. The best geometric flow direction is found for all the quadtree division blocks obtained according to the Lagrangian penalty function method. Finally, a 1-D wavelet transform is applied to the 1-D discrete signal, acquired by an orthogonal projection and a reordering of the wavelet coefficient, according to the best geometric flow direction of each quadtree division block, thereby obtaining the coefficients of the bandelet transform.

3. RSA

The coefficients obtained from multiscale transforms are encrypted using the RSA algorithm. The following steps in the RSA are used for key generation, encryption and decryption.

1. Select two large prime numbers, referred to as p and q.
2. Compute $N = p * q$, where $ø(N) = (p - 1)(q - 1)$.
3. Choose an odd integer e that is relatively prime to $ø(N)$ and not 1, where $1 < e < ø(N)$, $gcd(e, ø(N)) = 1$.
4. Now calculate d to be the multiplicative inverse of ‘e’ modulo ‘ø(N)’ where $e.d = 1 \bmod ø(N)$ and $0 \leq d \leq N$.
5. The ordered pair (e, n) is the RSA public key used for encryption and the ordered pair (d, n) is the RSA private key used for decryption.
6. Encryption is done as $C = M^e \bmod N$ where $0 \leq M < N$. C is the encrypted message and M is the original message.
7. Decryption is done as $M = C^d \bmod N$ where $0 \leq M < N$.

4. Encoding techniques

4.1 *EZW*

In the EZW, the bitstream is embedded and coefficients ordered, based on significance and precision, so it can be truncated according to the bit-rate need. It efficiently makes use of the similarity between subbands of similar orientation and attains significant data reduction. However, the EZW has certain drawbacks in that a single embedded file is unable to deliver the best performance at all target bit rates. The EZW uses a zerotree structure and a scanning order to scan the image. The EZW process consists of three stages: significance map, dominant stage and subordinate stage. The significance map involves the choosing of an initial threshold t_0 using the following condition (1),

$$t_0 = 2^{\log_2(\max(|\Upsilon(x,y)|))} \tag{1}$$

where Max represents the maximum coefficient value in the image and $\Upsilon(x, y)$ represents the wavelet coefficient.

There are two passes used to code an image. The first pass, called the dominant pass, is where the image is scanned and a symbol outputted for every coefficient. If the coefficient is larger than the threshold a **P** (positive) is coded, else an **N** (negative) is coded. If the coefficient is the root of a zerotree, a **T** (zerotree) is coded and, finally, if the coefficient is smaller than the threshold but not the root of a zerotree, a **Z** (isolated zero) is coded. The second pass is the subordinate pass that determines the magnitude of the coefficients already found to be significant. If the magnitude of the coefficient is in the upper half of an old cell, 1 is provided, else 0. An example of EZW implementation is shown in figure 2.

4.2 *SPIHT*

SPIHT is the most efficient of all algorithms where wavelet-based image compression is concerned. It is optimized for progressive image transmission and produces a fully embedded coded file. It uses a pyramid structure known as the spatial orientation tree [21, 22], where a wavelet transform is applied to an image. In the spatial orientation tree, four facets are defined before processing the algorithm. They are O(i,j), D(i,j), H(i,j) and L(i,j).

64	-35	49	10	7	13	-12	7
-31	24	14	-13	3	4	6	-1
15	14	4	-12	5	-7	3	9
-10	-8	-14	9	4	-2	3	2
-5	9	-1	47	4	6	-2	2
3	0	-3	2	3	-2	0	4
2	-3	6	-4	3	6	3	6
5	11	5	5	0	3	-4	3

Dominant Pass 1	PNZTPTTTTZTTTTTTTPTT
Subordinate Pass 1	1010

Figure 2. An example of the EZW.

O(i,j) refers to the set of coordinates of all offsprings of node (i,j), that is, only children. D(i,j) refers to the set of coordinates of all descendants of node (i,j), that is, children, grandchildren, etc. H(i,j) refers to the set of all tree roots, that is, parents. L(i,j) is obtained from D(i,j) – O(i,j), which means all descendents except the offspring.

The SPIHT algorithm maintains three lists: list of insignificant pixels (LIP), list of significant pixels (LSP), and list of insignificant sets (LIS). The algorithm has three phases: initialization, sorting pass and refinement pass. In initialization, all the coefficients are present in the LIP and n is calculated using the following formula, shown in (2). LSP remains empty and LIS contains the Ds of roots referred to as type A entries.

$$n = [\log_2(\max|\mathrm{coeff}|)] \tag{2}$$

In the sorting pass, for each entry in the LIP, the SPIHT performs significance testing by using the following formula (3).

$$S_n(\tau) = \begin{cases} 1 & \max\limits_{(i,j)\in\tau}\left|C_{i,j}\right| \geq 2^n \\ 0 & \text{Otherwise} \end{cases} \tag{3}$$

If the result of the significance test (based on (3)) is 1, it indicates that a particular test is significant, so the coefficient is moved to LSP and coded. Otherwise it is 0, indicating that the particular coefficient is insignificant. Insignificant sets are moved to LIS. The SPIHT sorting pass is shown in figure 3. In the refinement pass, the n-th most significant bit is output based on each entry (i,j) available in the LSP (except those added in the last sorting pass with the same n). Finally, n is decremented by 1 and the steps repeated until n = 0. An example of the SPIHT algorithm is shown in figure 4.

4.3 *WDR*

The WDR conducts a significance pass and a refinement pass for each bit plane. A wavelet transform is first applied to the image, and the bit-plane-based WDR encoding algorithm for the wavelet coefficients is carried out thereafter. In the significance pass, an initial threshold value T is chosen so that all transform values are put into a significant test. A wavelet coefficient is termed significant when the value is greater than or equal to the threshold value. It is otherwise termed insignificant.

The distinguishing feature of the WDR is its difference reduction method. For example, if the significant values found in the significant pass are 3, 5, 9, 24, 45, the WDR works with the successive differences (that is, 3, 2, 4, 15, 21) instead of working with these values. In this list, the first number is termed the starting index and each successive number that follows is the number of steps needed to reach the next index.

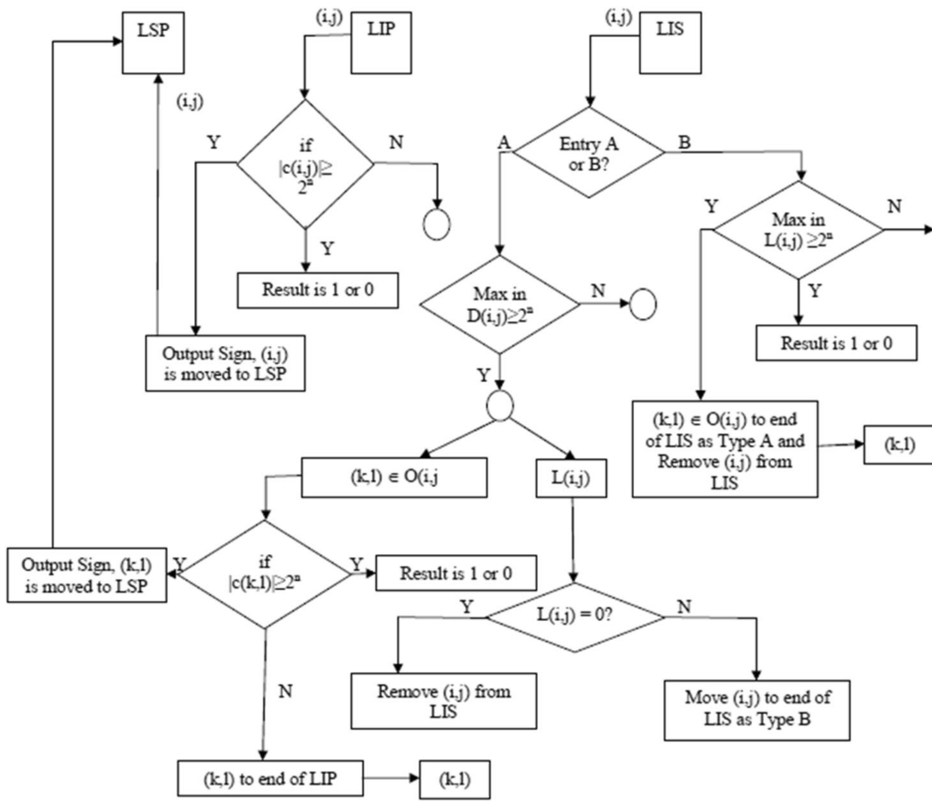

Figure 3. SPIHT sorting pass.

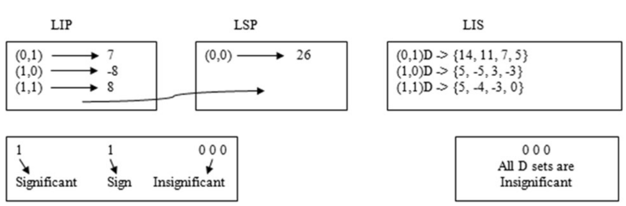

Figure 4. An example of SPIHT implementation: After first sorting and refinement pass.

The binary expansions of the successive differences above are $(11)_2$, $(10)_2$, $(100)_2$, $(1111)_2$, and $(10101)_2$. The most significant bit (1) is the same for all the binary expansions above. Consequently, it will be dropped and the signs of the significant transform values used instead, termed as $+ 1 + 0 - 00 + 111$ _0101, following which the symbols are encoded.

The second pass is the refinement pass that determines the magnitude of the coefficients already found to be significant. For instance, if an old significant transform value's magnitude lies in the interval [34, 50] and the present threshold is 8, then the magnitudes lies in either (34, 42) or (42, 50). If the magnitude of the coefficient is in the upper half of the old cell, then 1 is provided or else 0 is.

4.4 *ASWDR*

The ASWDR algorithm is a simple modification of the WDR algorithm. Initially, a wavelet transform is applied to an image. Secondly, the transformed values are scanned through linear ordering by choosing a scanning order. The scanning order is a zig-zag through subbands from lower to higher. Thereafter, an initial threshold T is chosen such that at least one transform value has a magnitude greater than or equal to T and all transform values have magnitudes less than 2T.

The algorithm has two passes, the first being the significance pass. In this pass, a transformed value greater than or equal to the present threshold is referred to as significant and encoded, based on the difference reduction method. The second pass is the refinement pass in which refinement bits are recorded for significant transform values determined using larger threshold values. This generation of refinement bits is the standard bit-plane encoding used in embedded codecs. After the refinement pass, a new scanning order is chosen.

5. Experimental set-up

Input images such as CT Skull, MRI and Mammogram (shown in figure 5) are taken for the experiment and multiscale transforms applied to them to obtain coefficients.

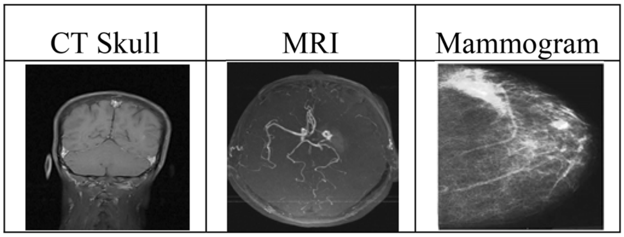

Figure 5. Input medical images.

The number of the decomposition level is four. The bi-orthogonal wavelet transform and filters like the pyramidal directional filter bank and the atrou-quad filter are used in the experiment to obtain the coefficients. After applying multiscale transforms, the RSA encryption algorithm is used to encrypt the coefficients, thereafter given to the appropriate encoding technique.

6. Performance evaluation

6.1 *Performance metrics*

In this paper, the results of multiscale transforms with encoding techniques are compared using parameters such as peak signal to noise ratio (PSNR), mean square error (MSE), image quality index and structural similarity index (SSIM). The PSNR formula is shown below:

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{255^2}{MSE}\right) \tag{4}$$

The MSE represents the cumulative squared error between the compressed and the original image. The mean square error is calculated using the following formula

$$MSE = \frac{\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}\left(\hat{x}_{i,j} - x_{i,j}\right)^2}{\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}\left(x_{i,j}\right)^2} \tag{5}$$

where $x_{i,j}$ is the original image and $\hat{x}_{i,j}$ the decompressed image.

The SSIM index can be viewed as a quality measure of one of the images being compared, provided the other image is regarded as being of perfect quality. It is calculated using the following formula:

$$\mathrm{SSIM(x,y)} = \frac{\left(2\mu_x\mu_y + c_1\right)\left(2\sigma_{xy} + c_2\right)}{\left(\mu_x^2 + \mu_y^2 + c_1\right)\left(\sigma_x^2 + \sigma_y^2 + c_1\right)} \tag{6}$$

μ_x the average of x, μ_y the average of y, c_1 and c_2 are constants, σ_{xy} the covariance of x and y, σ_x^2 the variance of x, σ_y^2 the variance of y

If the row number and column number of the image are N and M, then the overall normalized quality index is:

$$\mathrm{Q} = \frac{1}{N * M}\sum\nolimits_{i=1}^{N}\sum\nolimits_{j=1}^{M} Q_{ij} \tag{7}$$

6.2 *Performance analysis and discussion*

The performance of different multiscale transforms and encoding techniques in cloud-based medical image compression is analyzed. The PSNR, MSE, SSIM, image quality index, Time and Space values are shown in table 1, it is found that the ASWDR and SPIHT with the bandelet transform attain high PSNR values and low MSE values when compared to other combinations. Bandelet and curvelet transforms perform well with all encoding techniques, producing high PSNR values. The bandelet transform gives images geometrical regularity and is used to analyse their edges and textures. The wavelet transform does offer geometrical regularity but its advantage lies chiefly in image fidelity.

Next to the bandelet transform, the curvelet transform performs competently, approximating edge discontinuity well. Likewise, the contourlet transform also performs reasonably well, with better features - such as edges, lines and contours - than the wavelet transform. Table 1 demonstrates that the image quality index and SSIM values are good for the SPIHT and ASWDR encoding techniques and the bandelet transform, the latter producing values like 0.99. Similarly, the curvelet transform also provides good values.

Combining encryption with image compression supports compression consummately. Encryption does not affect the time complexity of the overall process. It is found from the experiments that the RSA supports image compression most effectively (see table 1). The time and memory space taken for the proposed approach is less. So it is justified that the proposed joint compression and encryption operation does not make any delay in the overall process.

Table 1. Performance of the proposed approach.

	CT						MRI						Mamo					
Encoding techniques	PSNR (db)	MSE	IQI	SSIM	Space (kb)	Time (s)	PSNR (db)	MSE	IQI	SSIM	Space (kb)	Time (s)	PSNR (db)	MSE	IQI	SSIM	Space (kb)	Time (s)
Wavelet transform																		
SPIHT	31.54	45.55	0.571	0.925	21.42	3.627	29.19	78.18	0.669	0.915	19.43	4.459	30.79	54.19	0.609	0.785	18.32	4.886
EZW	26.21	155.6	0.672	0.765	22.16	3.014	22.92	332.1	0.783	0.870	21.25	3.846	24.43	234.2	0.905	0.845	19.92	4.273
WDR	35.47	18.43	0.686	0.966	20.35	4.102	31.67	44.20	0.792	0.968	18.71	4.934	31.76	43.29	0.702	0.820	18.32	5.361
ASWDR	35.50	18.31	0.670	0.960	20.31	4.149	34.34	23.89	0.780	0.970	18.13	4.981	36.92	13.19	0.900	0.940	18.19	5.408
Bandelet transform																		
SPIHT	54.26	0.24	0.99	0.99	22.69	3.581	54.77	0.21	0.99	0.99	20.27	4.318	54.71	0.21	0.99	0.99	18.49	4.851
EZW	40.15	06.27	0.99	0.99	21.94	3.358	39.94	06.58	0.99	0.99	21.58	3.961	40.66	05.58	0.99	0.99	20.06	4.537
WDR	46.45	01.46	0.99	0.99	20.37	4.119	46.31	01.52	0.99	0.99	19.41	5.026	47.03	01.28	0.99	0.99	18.57	5.375
ASWDR	53.12	0.317	0.99	0.99	20.62	4.162	53.23	0.308	0.99	0.99	18.27	5.031	53.14	0.315	0.99	0.99	18.42	5.428
Curvelet transform																		
SPIHT	36.90	13.27	0.918	0.973	21.58	3.498	36.96	13.08	0.936	0.974	19.57	4.731	36.76	13.70	0.974	0.984	18.64	4.954
EZW	41.97	04.12	0.963	0.989	22.25	3.395	42.47	03.67	0.973	0.990	21.49	3.814	42.24	03.87	0.988	0.993	20.52	4.285
WDR	33.97	26.00	0.864	0.951	21.03	4.294	33.94	26.24	0.890	0.950	18.84	4.958	34.06	25.48	0.95	0.970	18.48	5.164
ASWDR	38.24	09.75	0.920	0.970	20.59	4.618	38.39	09.40	0.940	0.970	18.59	4.937	37.94	10.44	0.970	0.980	18.27	5.208
Contourlet transform																		
SPIHT	31.54	45.55	0.57	0.920	22.49	3.840	29.19	78.18	0.66	0.910	19.58	4.859	30.79	54.19	0.60	0.780	18.61	4.948
EZW	29.02	81.33	0.48	0.870	21.95	3.746	26.00	163.01	0.53	0.830	22.04	3.219	27.96	103.79	0.39	0.650	19.92	4.375
WDR	12.18	2965	0.51	0.790	20.53	4.481	28.05	84.90	0.49	0.800	18.57	4.946	19.47	672.5	0.54	0.780	18.47	5.258
ASWDR	14.33	2395	0.67	0.690	20.42	4.293	34.34	23.74	0.62	0.710	18.49	4.895	25.45	185.30	0.68	0.720	18.49	5.416
Ridgelet transform																		
SPIHT	28.37	94.53	0.342	0.567	21.25	3.629	28.55	90.59	0.379	0.537	20.18	4.473	26.09	159.9	0.147	0.367	18.49	4.954
EZW	30.41	58.69	0.455	0.554	22.54	3.851	30.68	55.38	0.499	0.532	22.04	3.861	27.69	151.8	0.231	0.543	19.92	4.375
WDR	28.74	86.84	0.358	0.579	20.59	4.593	28.89	83.81	0.398	0.550	19.57	4.942	26.32	151.4	0.158	0.374	18.37	5.269
ASWDR	30.44	58.66	0.457	0.650	21.07	4.250	30.70	55.34	0.503	0.632	19.42	4.975	27.71	109.9	0.232	0.445	18.48	5.384

7. Conclusion

In this paper, a new framework is proposed for medical image compression and encryption in the cloud. This work successfully identifies the performance of multiscale transforms, encoding techniques and the supporting encryption algorithm with compression. It is observed that the bandelet transform produces favorable results with all encoding techniques, clearly improving the results of image compression and encryption when compared to other transforms. The bandelet transform is based on the geometric flow of the image and the warped wavelet. The advantage of the bandelet transform is that it can obtain the warped basis adaptive to the image's edge direction. Further, it is established that the SPIHT and ASWDR encoding techniques produce high PSNR and low MSE values with all multiscale transforms. It is, therefore, concluded that the bandelet transform provides excellent results in joint medical image compression and encryption.

References

[1] Armbrust M, Fox A, Griffith R, Joseph A D, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I and Zaharia M 2010 A view of cloud computing. *Commun. ACM.* 53: 50–58
[2] academic.regis.edu
[3] Antonini M, Barlaud M, Mathieu P and Daubchies I 1992 Image coding using wavelet transform. *IEEE Trans. Image Process*. 1(4): 205–220
[4] Daubechies I 1990 The wavelet transform, time frequency localization and signal analysis. *IEEE Trans. Inf. Theory* 36(9): 961–1005
[5] Mallat S 1998 *A wavelet tour of signal processing*. New York: Academic Press
[6] Ram I, Cohen I and Elad M 2014 Facial image compression using patch-ordering-based adaptive wavelet transform. *IEEE Signal Process. Lett.* 21(10): 1270–1274
[7] Suruliandi A and Raja S P 2015 Empirical evaluation of EZW and other encoding techniques in the wavelet based image compression domain. *Int. J. Wavelets Multiresolution Inf. Process.* 13: 2
[8] Candes E J and Donoho D 1999 Curvelets—a surprisingly effective nonadaptive representation for objects with edges. In: A Cohen, C Rabut and L Schumaker (Eds) *Curves and Surface Fitting: Saint-Malo.* Vanderbilt University Press, Nashville, pp. 105–120
[9] Elaiwat S, Bennamoun M, Boussaid F and El-Sallam A 2014 3-D face recognition using curvelet local features. *IEEE Signal Process. Lett.* 21(2): 172–175
[10] Do M N and Vetterli M 2009 The contourlet transform: an efficient directional multiresolution image representation. *IEEE Trans. Image Process.* 14(12): 2091–2106
[11] Ashouri Z and Shirani S 2013 Video super resolution using contourlet transform and bilateral total variation filter. *IEEE Trans. Consum. Electron.* 59(3): 604–609
[12] El-Mezouar M C, Kpalma K, Taleb N and Ronsin J 2014 A pan-sharpening based on the non-subsampled contourlet transform: application to Worldview-2 imagery. *IEEE J. Sel. Top. Appl. Earth Obs. Remote Sens.* 7(5): 1806–1815
[13] Kishor Upla P, Manjunath Joshi V and Prakash Gajjar P 2015 An edge-preserving multiresolution fusion: use of contourlet transform and MRF prior. *IEEE Trans. Geosci. Remote Sens.* 53(6): 3210–3220
[14] Candes E J and Donoho D L 1999 Ridgelets: a key to higher-dimensional intermittency? *Phil. Trans. R. Soc. Lond. A.* 357(1760): 2495–2509
[15] Le Pennec E and Mallat S 2005 Sparse geometric image representations with bandelets. *IEEE Trans. Image Process.* 14(4): 423–438
[16] Rivest R, Shamir A and Adleman L 1978 A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* 21(2): 120–126
[17] Huang X and Wang W 2015 A novel and efficient design for an RSA cryptosystem with a very large key size. *IEEE Trans. Circuits Syst. II Express Briefs* 6(10): 972–976
[18] Sun H M, Wu M E, Ting W C and Jason Hinek M 2007 Dual RSA and its security analysis. *IEEE Trans. Inf. Theory* 53(8): 2922–2933
[19] Aaron Cohen E and Keshab Parhi K 2011 Architecture optimizations for the RSA public key cryptosystem: a tutorial. *IEEE Circuits Syst. Mag.* 11(4): 24–34
[20] Shapiro J M 1993 Embedded image coding using zerotrees of wavelet coefficients. *IEEE Trans. Signal Proc*. 41(12): 3445–3462
[21] Said A and Pearlman W A 1993 Image compression using the spatial-orientation tree. In: *IEEE Int. Symp. on Circuits and Systems, Chicago, IL*, pp. 279–282
[22] Said A and Pearlman W A 1996 A new, fast, and efficient image codec based on set partitioning in hierarchical trees. *IEEE Trans. Circuits Syst. Video Technol.* 6(3): 243–250
[23] Tian J and Wells R O 1998 Embedded image coding using wavelet difference reduction. In: P Topiwala (Ed.) *Wavelet Image and Video Compression*, vol. 450. Norwell, MA: Kluwer, pp. 289–302
[24] Walker J S and Nguyen T Q 2000 Lossy image codec based on adaptively scanned wavelet difference reduction. *Opt. Eng.* 39: 1891–1897
[25] Walker J S 2001 *Wavelet-Based Image Compression. Transforms and Data Compression Handbook*. Boca Raton: CRC Press LLC
[26] Prasad B and Mishra K 2013 A combined encryption compression scheme using chaotic maps. *Cybern. Inf. Technol.* 13(2): 75–81
[27] Shi Z, Sun X and Wu F 2014 Photo album compression for cloud storage using local features. *IEEE J. Emerg. Sel. Top. Circuits Syst.* 4(1): 17–28
[28] Yue H, Sun X, Yang J and Wu F 2013 Cloud-based image coding for mobile devices—toward thousands to one compression. *IEEE Trans. Multimed.* 15(4): 845–857
[29] Li C and Li L Y 2015 Hierarchical scheduling optimization scheme in hybrid cloud computing environments. *J. Circuits Syst. Comput.* 24: 8

[30] Mallet S and Peyre G 2007 A review of bandelet methods for geometrical image representation. *Numer. Algorithms* 44(3): 205–234

[31] Javidan R, Masnadi-Shirazi M A, Azimifar Z and Sadreddini M H 2008 A comparative study between wavelet and contourlet transform features for textural image classification. In: *3rd International Conference on Information and Communication Technologies: From Theory to Applications*, pp. 1–8

[32] Li Y, Zhang S and Hu J 2010 Combining curvelet transform and wavelet transform for image denoising. In: *Advanced Intelligent Computing Theories and Applications. With Aspects of Artificial Intelligence Lecture Notes in Computer Science* 62(16), pp. 317–324

[33] Chang V and Ramachandran M 2015 Towards achieving data security with the cloud computing adoption framework. *IEEE Trans. Serv. Comput.* 9(1): 138–151

[34] Tari Z, Yi X, Premarathne U S and Bertok P 2015 Security and privacy in cloud computing: vision, trends, and challenges. *IEEE Cloud Comput.* 2(2): 30–38

[35] Guan Z T and Yang T T 2015 Research on challenges and security of access control models for mobile cloud computing. In: *Proceedings of 2015 International Workshop on Wireless Communication and Network*

[36] Xiao Z and Xiao Y 2013 Security and privacy in cloud computing. *IEEE Commun. Surv. Tutor.* 15(2): 843–859

[37] Shabir M Y, Iqbal A, Mahmood Z and Ghafoor A 2016 Analysis of classical encryption techniques in cloud computing. *Tsinghua Sci. Technol.* 21(1): 102–113

[38] Wang S, Zhou J, Liu J K and Yu J 2016 An efficient file hierarchy attribute-based encryption scheme in cloud computing. *IEEE Trans. Inf. Forensics Secur.* 11(6): 1265–1277

[39] Zhang Y, Zhang L Y, Zhou J, Liu L, Chen F and He X 2016 A review of compressive sensing in information security field. *IEEE Access Green Commun. Netw. 5G Wirel.* 4: 2507–2519

[40] Chikkannan E and Ramakrishnan K 2017 Feed-forward neural network-based predictive image coding for medical image compression. *Arab. J. Sci. Eng.* S13369-017-2837-z: 2191–4281

[41] Sadh R, Mishra N and Sharma S 2016 Dual plane multiple spatial watermarking with self encryption. *Sadhana* 41(1): 1–14

[42] Peyré G and Mallat S 2005 Surface compression with geometric bandelets. ACM transactions on graphics. *Proc. ACM Siggraph* 24(3): 601–608