IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735
PP 70-78
www.iosrjournals.org

Privacy Preserving Transform Domain Encryption With Wavelet Based Compression For Biomedical Images

V.Balambigai[1]., Dr.D.Balasubramaniam [2]
[1]*PG Student, Digital Signal Processing, Department of ECE, G.K.M College of Engineering and Technology, India*
[2]*Assistant Professor, Department of ECE, G.K.M College of Engineering and Technology, India*

Abstract : *Now-a-days the medical image compression plays a major role in image processing. Even though the technology is improvised, still it needs the storage space and efficient bandwidth utilisation. In this project, a new and efficient method is proposed to develop secure image-encryption techniques which combines two techniques: encryption and compression. In this method we produces a cipher of the test image using block prediction clustering and random permutation based Cosine Number Transform for encryption and Discrete Wavelet Transform coding approach is used for image compression with lossless/ lossy state. This proposed algorithm was verified to provide a high security level. A detailed discussion for the new algorithm is discussed. Several medical images along with Digital Imaging and Communications in Medicine (DICOM) images are used to demonstrate the validity of the proposed algorithm. In this project, an efficient image compression then-encryption (CTE) system is designed; High efficient compression of the encrypted data has been realized by a Discrete Wavelet Transform(DWT) coding approach. The experimental results have shown that reasonably high level of security has been retained. The results of several experiments show that the proposed algorithm can obtain an effective cipher and high-quality image compression to achieve both security against unauthorized access during data transmission through an unsecured channel and high compression to allow for a low transmission rate.*

Keywords*: ETC, CTE, Biomedical Image Processing, Cosine Number Transform, Directional DWT, Modulo Operation.*

I. Introduction

By the increasing use of direct digital imaging systems for medical diagnostics, digital image processing becomes more and more important in health care. The storage space and efficient bandwidth utilization are major constraints in case of biomedical image processing in a telemedicine system. In a telemedicine systems it is essential to ensure the security of the transmitted biomedical images. Image encryption is the process of encoding messages or information in such a way that only authorized parties can read it.

Encryption does not prevent interception, but denies the message content to the interceptor. Transmitting images will always consume large amount of bandwidth and storing images will require hefty resources. The fundamental components of compression are redundancy and irrelevancy reduction. An algorithm is developed with high efficient image encryption and large degree of compression.

1.1 Biomedical Image Processing

Bio medical imaging is a technique is used to create the images of the human body or parts of it for clinical purposes or for studying the anatomy and physiology. They can be efficiently processed and made available at many places at the same time by means of appropriate communication networks and protocols, such as PACS and DICOM protocol. There exists a need for compression and encryption for efficient storage and for maintaing the confidentiality of the images.

Bio medical images have high pixel range of 8-16-32 bit per pixel whereas normal images ranges upto 8 bit. Biomedical image are represented in both positive as well as negative values and fraction values unlike normal images. Biomedical image resolution will be very high upto 2048x2048 and 3D images also exists. The following figure shows the multilevel response of the image DICOM and Maximum data retention images

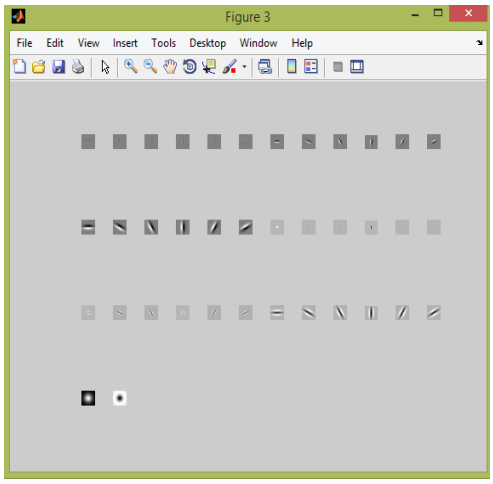


Figure1.1 Multilevel respose of the image DICOM

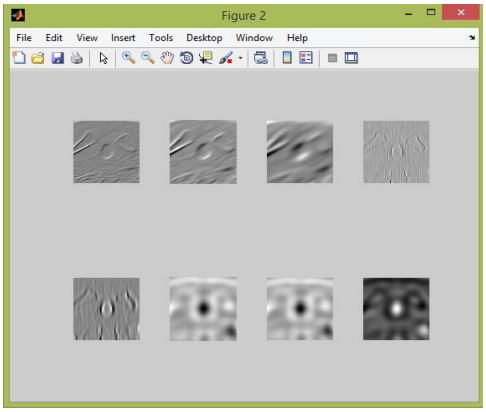


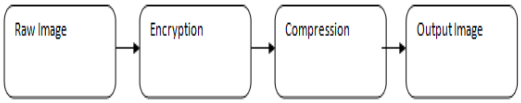
Figure1.2 Maximum data retention images

II. Literature Survey

Demijan Klinc, Carmit Hazay, Ashish Jagmohan, Hugo Krawczyk and Tal Rabin propose Compressing data encrypted with block ciphers, such as the Advanced Encryption Standard (AES) is investigated in "On compression of data encrypted with block ciphers". Wei Liu, Wenjun Zeng, Lina Dong and Qiuming Yao discussed a novel multi-resolution based approach which makes it possible by temporal side information and spatial side information reduction is proposed in"Resolution progressive compression of encrypted grayscale images". Xinpeng Zhang in his work "Lossy compression and iterative reconstruction for encrypted image" uses Pseudorandom permutation to encrypt an image and compressed using lossy compression. Encrypted images are efficiently compressed by discarding the rough and fine information of coefficients. Zhang X, Feng G and Qian Z proposes a simple modulo-256 addition for encryption and hardmard transform is used for compression. In the encryption phase, the original pixel values are masked by modulo-256 addition with pseudorandom numbers that are derived from secret key. After the encrypted data is decomposed into a down sampled sub image in their work "Scalable coding of encrypted image".

III. Existing Method

ETC (ENCRYPTION THEN COMPRESSION) approach generally use the physical encryption techniques to encrypt the images for security purpose where it can be easily decrypted by intruders, which makes it difficult to share the confidential information and optimal techniques are used for compressing the images where the compression is made up to a small extent which makes the user difficult to send the large amount of data in the limited bandwidth. Thus the compression techniques used will not be helpful to obtain the desired compressed image and it makes unsecure environment while transferring the data between the users.



3.1 Limitation

- It can be easily decrypted by intruders, making it hard to share the confidential information
- It makes the user difficult to send the large amount of data in the limited bandwidth.
- Compression ratio is less
- Complex in nature

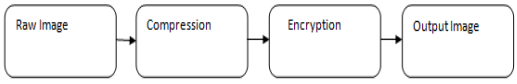
3.2 Challenges

- Medical images cannot be precisely segmented due to their low contrast and high noise content.
- Image cross sections of objects lack clear shape and boundary.
- Invariability exists for most of the anatomical parts.
- Not many techniques are available to deal with the semantic gap and sensory gap

It is well-known that the appearance and statistical properties of medical images are influenced by acquisition settings, scanner technology and often proprietary post-processing techniques. Medical image security is devoted to provide mainly one or many of the following requirements: confidentiality (only authorized persons can access patient data), integrity (the proof that the medical information has not been modified) and authentication. These changes can have a huge impact on the performance of common image processing techniques, such as image encryption, image compression or computer-aided detection (CAD).

IV. Proposed Method

Compression then encryption algorithm is preferred for biomedical image transmission in telemedicine system. In CTE approach the compression algorithm reduces the entropy of the image. Encryption scrambles the image so as to avoid the structure being detected. Due to the large size of the biomedical image, size reduction is obtained before encryption to avoid the computaional complexity.



4.1 Compression Method

Here wavelet based decomposition is used for image compression. Based on bio medical characteristics any of low or high frequency bands will be retained for size reduction. A forward DWT separates a given discrete signal into a low-pass L and a high-pass H signal by means of a dyadic wavelet filter bank and down-sampling operations. It is possible to improve transform efficiency by making use of directional wavelet transforms. Modifying the previously defined classic or non-directional DWTD to make it directional requires the prediction function and the update function to accept more generic direction vectors

4.2 Discrete wavelet transform (dwt) compression of image

The compression of the file I_e needs to be performed in the encrypted domain. The schematic diagram of lossless compression is shown in the fig.3.2. A forward 1D-DWT separates a given discrete signal into a low-pass L and a high-pass H signal [44] by means of a dyadic wavelet filter bank and down-sampling operations. The resulting low-pass output signal is a scaled version of the original signal with half the number of samples. The high-pass signal contains the missing high frequency information needed to allow reconstruction with an inverse 1D-DWT. It is important to note that the DWT is critically sampled

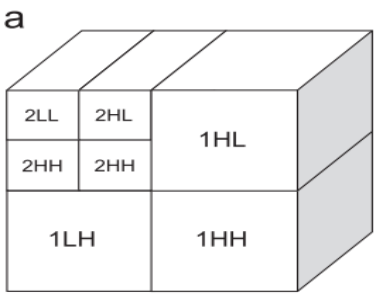


Fig.4.1 Basic architecture for compression

The resulting low-pass output signal is a scaled version of the original signal with half the number of samples. The high-pass signal contains the missing high frequency information needed to allow reconstruction

with an inverse DWT. After decomposing into low and high and low frequency components, the region of interest is retained and remaining are removed. The ROI depends upon the requirement for clinical analysis.

4.3 Quantizing

The normalization factors are computed from the synthesis wavelet filters such that for one decomposition level, the total noise energy is preserved in the reconstructed image, when quantizing the coefficients with very high-rate scalar uniform quantizers and assuming that the quantization noise on the wavelet coefficients is white. Hence, even if the input is given by integer numbers, the output of the filtering operations is no longer guaranteed to be integer. Moreover, due to its limited representation precision, floating point arithmetic is not exact and thus inherently introduces approximation errors, meaning that both the prediction and the update functions are irreversible in practice. In order to ensure perfect reversibility of the transform, one needs to define specialized prediction and update functions that rely on integer calculus alone to prevent rounding errors.

4.4 Image Encryption Technique:

The design of the encryption algorithm should simultaneously consider the security and the ease of compressing the encrypted data, the image encryption scheme operated over cosine number transform (CNT). CNT is defined over algebraic structures with a finite number of elements (a finite field), only modular arithmetic is needed for computing the transform. Consequently, the computation of a CNT is considerably sensitive to changes in the vector being transformed. In other words, two slightly different vectors may have significantly distinct CNTs, which is desirable for cryptographic applications. This does not occur for real- or complex-valued transforms, such as the ordinary Fourier transform and its variants, which are mainly applied in image encryption techniques implemented in the optical domain.

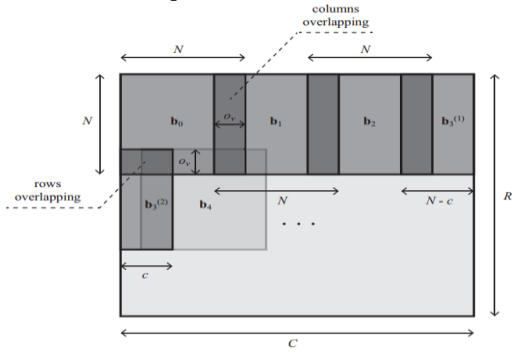


Fig.4.2 Block Selection and Overlapping in the Proposed Image Encryption Scheme

4.5 Cosine number transform:

The number of times the CNT is applied to each image block depends on a secret-key, which can be easily encoded as a sequence of bits. The encryption is completed after the whole image is processed twice using the described procedure; the decryption is carried out by applying, in the reverse order, the same steps used in the encryption. CNT is defined over algebraic structures with a finite number of elements for obtaining energy compaction of the image. It is the generalized form discrete cosine transform that can be applied to fractions and negative numbers. The computation of a CNT is considerably sensitive to changes in the vector being transformed. The number of times the CNT is applied to each image block depends on a secret-key, which can be easily encoded as a sequence of bits. The encryption is completed after the whole image is processed twice using the described procedure. The image is divided in overlapping blocks of desired size. The overlapping size and fashion is user defined. Then the security is added - by applying simple modulo arithmetic on the overlapping blocks. The decryption is carried out by applying, in the reverse order, the same steps used in the encryption.

4.6 Encryption scheme:

The first step of the encryption procedure is to choose the prime p, which characterizes the finite field GF(p) where the CNT is defined. If the pixels assume integer values ranging from Pmin to Pmax, we have to choose pZPmax Pmin þ1; this avoids that two different values are treated as being the same value, after a modulo p reduction. The second step is to define a CNT over the chosen field GF(p). It is necessary to choose an element **ζ (GF)** or a unimodular element **ζ (GF)**, such that **ζ (GF)** = 2N.

This determines the CNT length, N, and, consequently, the dimensions of the image block to be processed in the scheme, N N. The processing of each image block in the encryption procedure depends on a secret-key, which is a K-length vector of integers denoted by

$$\mathbf{k} = [k_0, k_1, \ldots, k_{K-2}, k_{K-1}]$$

4.7 Key space:

The key space should be sufficiently large to make brute-force attack unfeasible. In our simulations, each component of the secret-key k given in Eq. The less positive integer l1 such that $C^{l}1\ 1 = I$ is $l^1 = 17$; 974; 594; the less positive integer l2 such that Cl2 2 = I is greater than 108. Thus, in both cases, we can use as secret-key a vector k whose elements are integers in the range2 [1, 256]. In our experiments, we employ the randomly generated key

$$\mathbf{k} = [10, 217, 239, 174, 194, 190, 101, 168,$$
$$44, 181, 9, 71, 12, 25, 210, 178, 81, 243, 9, 112],$$

It can be encoded using 8 bits. Therefore, the key has a total of 160 bits, which satisfies the general requirement of resisting brute-force attack [2]. Naturally, larger keys could be employed in the proposed scheme just increasing the length of k or the range along which each of its components is taken.

$$E(x) = \frac{1}{P}\sum_{i=1}^{P} x_i;$$

x_i is the value of the ith selected pixel and yi is the value of the correspondent adjacent pixel. It is expected that an image, before being submitted to the encryption, has correlation coefficient close to 1; it is desirable that the correlation coefficient of a ciphered image be as close to 0 as possible.

4.8 Block-based intra-band prediction:

The remaining correlations can be effectively exploited by applying a block-based intra-band prediction scheme to further reduce the energy of the sub-bands. We note that the earlier work only exploits intra-band redundancies in 2D slices, yet showing improvements of up to 15% in bit-rate reduction compared to JPEG 2000 2D for lossless compression.

In light of our search to try to improve the overall compression efficiency for medical volumetric datasets, it is relevant to test the performance of such an intra-band prediction scheme in combination with and compared to the presented volumetric and directional extensions. Thus, based on [2] a generic block-based prediction step was implemented to take place just before EBCOT encodes each sub-band.

4.9 Image recovery:

Two rounds of the previously explained procedure are applied to the whole image. That is, after the last block in the bottom right corner of the image is processed, a new block in the top left corner of the image must be taken, following the described overlapping rules. The processing of the whole image is repeated, until the last block in the bottom right corner of the image is reached again. This increases the difficulty of brute-force and differential attacks. The decryption procedure consists in applying the same steps of the encryption scheme in the reverse order. The last block processed in the encryption must be the first block processed in the decryption. The ith block bi is recovered from

$$\mathbf{b}_i = \left(\mathbf{C}^T\right)^{k_i \pmod K} \cdot \mathbf{b}_i' \cdot (\mathbf{C})^{k_i \pmod K}.$$

4.9 Security And Performance Analysis:

The key stream controlling the random permutation of C_k is generated using a stream cipher. This implies that key stream could be different even for the same image encrypted at different section hence the only attack model applicable to the proposed encryption scheme is the cipher text only attack, in which the attacker can only access the cipher txt and attempts to recover the original image.

The feasibility of compressing the encrypted image without secret key allows any attacker to apply the same compression strategy on the encrypted data, and the size of the resulting file has already been a statistical indicator of the original image.

V. Results And Discussion

The project is implemented in MatLab. It has often been considered as an excellent environment by fast algorithm development. An X-ray Computed Tomography image is composed of pixels, whose brightness corresponds to the absorption of X-rays in a thin rectangular slab of the cross-section, which is called a 'voxel'. The pixel region tool provided by MatLab superimposes the pixel region rectangle over the image displayed in the tool defining the group of pixels that are displayed, in extreme close-up view, in the Pixel Region tool window. The Pixel Region tool shows the pixels at high magnification, overlaying each pixel with its numeric value.

5.1 Selection Of Input Image

The image set contained abnormalities encountered in a Western hospital in daily clinical practice and the abnormal CXRs in the JSRT dataset contained a single pulmonary nodule. All images were rescaled to a width of 1024 pixels. Fig. 1 shows one abnormal example image from each source, depicted with the original DICOM window center /width settings.. http://www.jsrt.or.jp/jsrt-db/eng.php

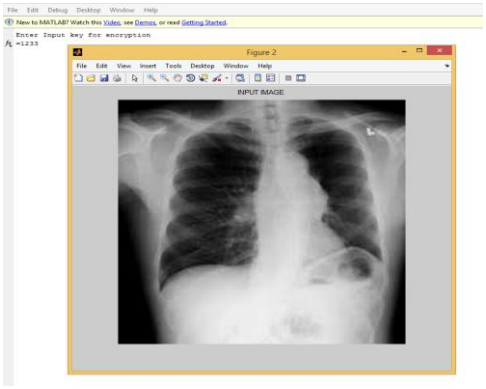


Fig.5.1 Selected of input image

The fig.5.2 shows the selection of input images which has to be processed in the MATLAB GUI. Rescaled abnormal TB lung image with the width of 1024 pixels. DICOM window contained a single pulmonary nodule with focal lesions to represent TB.

5.2 PERFORMANCE EVALUATION- Compression

Following input selection, image compression is carried out. Parameters like compression ratio, PSNR value, MSE, SSIM are evaluated. The lossless compression is carried by forwarding all 1D-DWT separated bands as a discrete signal into a low-pass L and a high-pass H signal by means of a wavelet filter bank and down-sampling operations.

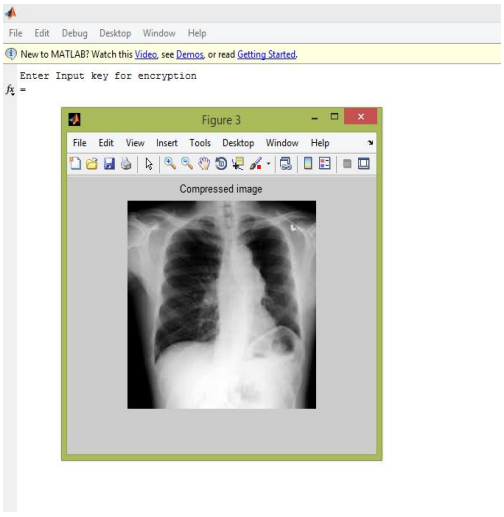


Figure 5.2 Compressed image

The resulting low-pass output signal is a scaled version of the original signal with half the number of samples. The high-pass signal contains the missing high frequency information needed to allow reconstruction

with an inverse 1D-DWT. It is important to note that the DWT is critically sampled and this high-pass signal is used for lossy compression. For the following implementation, let us assume we are dealing with a standard 2D array of data or matrix. The dimensions of the correct image matrix and the dimensions of the degraded image matrix must be identical.

5.3 Performance Evaluation- Encryption

A key of desired value is set and then the image is encrypted with it. At the reception side the encrypted image shall be decrypted by using the same key. Here each pixel is encoded using 8 bits. Therefore, the key has a size equal ant to macro block used for CNT transform, which satisfies the general requirement of resisting brute-force attack. ere larger keys are employed in the proposed scheme just increasing the length of k or the range along which each of its components is taken.

The number of times the CNT is applied to each image block depends on a secret-key, which can be easily encoded as a sequence of bits. Here we used single round. The encryption is completed after the whole image is processed using the described procedure. Input image divided into 8x8 image macro block to be processed with 8-point cosine number transform. Image blocks selection is done with predefined sequence and permutated both row and column wise based on a secret-key, which is a unique vector of integers.

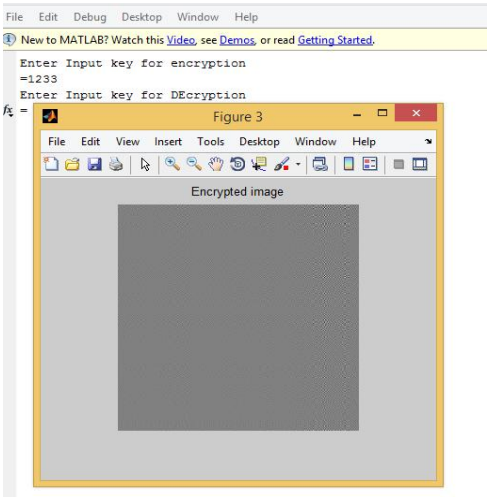


Fig.5.3 Implementation of encryption with row & column permutation keys

The fig.5.3 shows the encrypted image of the given input which is obtained by performing a random permutation in the input image.

5.4 Decrypted input image

The number of times the CNT is applied on each macro block of image block with a secret-key, which can be easily reversed as a sequence of bits. The decryption is carried out by applying, in the reverse order, the same steps used in the encryption.

The fig.5.4 shows the decrypted image of the given encrypted input which is obtained by using the corresponding key.

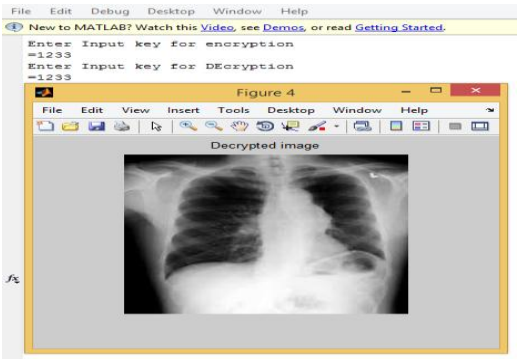


Figure 5.4 Decrypted input image

5.5 Reconstructed Image
5.6 He reconstruced /image is obtained by applying the inverse process of compression method used.
5.7

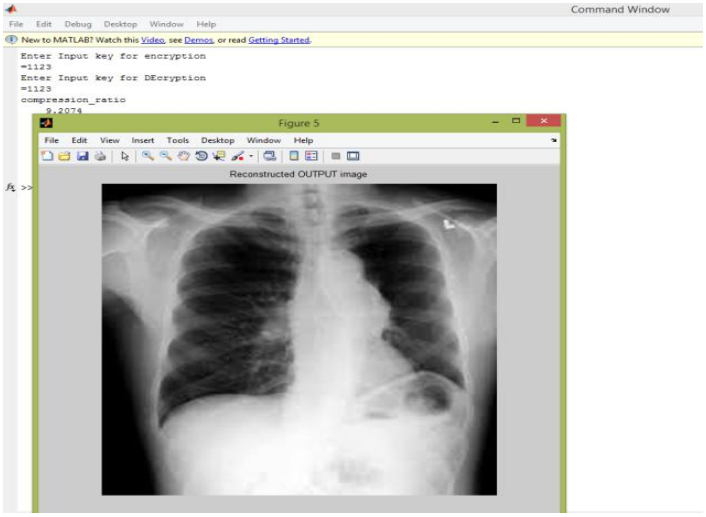


Figure5.5 Reconstructed image

5.6 Parameter exraction

The structural similarity (**SSIM**) index is a method for measuring the similarity between two images.
The mathematical representation of the **PSNR** is as follows:

$$PSNR = 20\log_{10}\left(\frac{MAX_f}{\sqrt{MSE}}\right)$$

Where the **MSE** (Mean Squared Error) is:

$$MSE = \frac{1}{mn}\sum_{0}^{m-1}\sum_{0}^{n-1}\|f(i,j) - g(i,j)\|^2$$

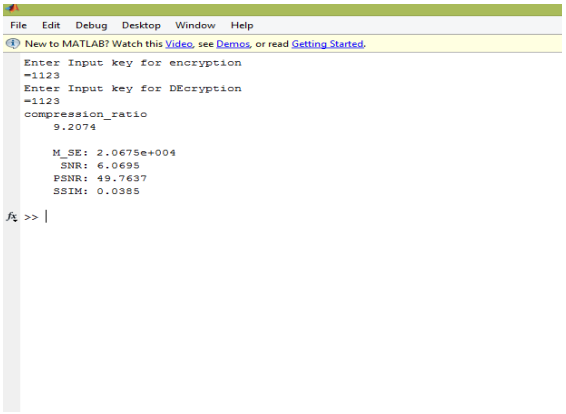


Figure5.6 Parameter extraction

VI. Conclusion And Future Work

In this project, an efficient image Encryption-then-Compression (ETC) system is designed; the image encryption has been achieved via CNT and random key space permutation. High efficient compression of the encrypted data has been realized by a DWT coding approach. The experimental results have shown that reasonably high level of security has been retained. The coding efficiency of our proposed compression method on encrypted images is very close to that of the state- of-the-art lossless image codec's, which receive original, unencrypted images as inputs.

In this project, an efficient image Encryption-then-Compression (ETC) system is designed; the image encryption has been achieved via CNT and random key space permutation. High efficient compression of the encrypted data has been realized by a DWT coding approach. The experimental results have shown that reasonably high level of security has been retained. The coding efficiency of our proposed compression method on encrypted images is very close to that of the state- of-the-art lossless image codec's, which receive original, unencrypted images as inputs.

Refferences

[1]. H.K. Huang, PACS and Imaging Informatics: Basic Principles and Applications, Wiley, USA, 2010 (ISBN: 978-0-470-37372-9).
[2]. L.W. Goldman, Principles of CT: multislice CT, J. Nucl. Med. Technol. 36 (2008).
[3]. C.H. Riedel, J. Zoubie, S. Ulmer, J. Gierthmuehlen, O. Jansen, ThinSlice reconstructions of nonenhanced CT images allow for detection of thrombus in acute stroke, Stroke: J. cereb. circul. 43 (2012) 2319–2323.
[4]. W.B. Pennebaker, J.L. Mitchell, JPEG Still Image Data Compression Standard, 1st edition, Kluwer Academic Publishers, 1992.
[5]. ISO/IEC 10918-1 j ITU-T Rec. T.81, Information Technology – Digital Compression and Coding of Continuous-tone Still Images, 1992.
[6]. ISO/IEC 15444-1 j ITU-T Rec. T.800, Information Technology - JPEG 2000 Image Coding System: Core Coding System, 2002.
[7]. R. Leung, D. Taubman, Transform and embedded coding techniques for maximum efficiency and random accessibility in 3-d scalable compression, IEEE Trans. Image Process. 14 (2005) 1632–1646.
[8]. B. Huang, Satellite Data Compression, Springer, SpringerLink, Bücher, 2011.
[9]. I. Blanes, J. Serra-Sagrista, M. Marcellin, J. Bartrina-Rapesta, Divide-andconquer strategies for hyperspectral image processing: a review of their benefits and advantages, IEEE Signal Process. Mag. 29 (2012) 71–81.
[10]. X. Wu, N. Memon, Context-based, adaptive, lossless image coding, IEEE Trans. Commun. 45 (1997) 437–444.
[11]. M.J. Weinberger, G. Seroussi, G. Sapiro, The LOCO-I lossless image compression algorithm: principles and standardization into JPEG-LS, IEEE Trans. Image Process. 9 (2000) 1309–1324.
[12]. ISO/IEC 14495-1 j ITU-T Rec. T.87, Information Technology – Lossless and Near-lossless Compression of Continuous-tone Still Images: Baseline, 1998.
[13]. T. Wiegand, G.J. Sullivan, G. Bjntegaard, A. Luthra, Overview of the h.264/avc video coding standard, IEEE Trans. Circuits Syst. Video Techn. 13 (2003) 560–576