EAI EndorsedTransactions
on Energy Web

Research Article EAI.EU

Performance Analysis of DCT Based Lossy Compression Method with Symmetrical Encryption Algorithms

Neetu Gupta[1,*], Ritu Vijay[2] and Hemant Kumar Gupta[3]

[1] Research Scholar, Computer Science & Engineering Department, Banasthali University, Banasthali, India. ermcet1981@gmail.com
[2] Dean & Professor, Department of Electronics, Banasthali University, Banasthali, India. rituvijay1975@yahoo.co.in
[3] Professor, Department of Electronics & Communication Engg. Vaagdevi College of Engineering., Warangal, India. drhemantgupta18@gmail.com

Abstract

In the modern era, the issues pertaining with secured, fast and efficient image transmission with limited bandwidth are challenging task. This provides a platform to the researcher to work on image compression-encryption (CE) methodologies. To influence the degree of compression, this paper presents a DCT based compression algorithm using luminous quantization followed by advanced encryption standard (AES) and data encryption standard (DES) encryption methods. In this paper, the effect of encryption over compressed image in terms of PSNR and SSIM is analysed. Efficiency of the AES and DES encryption algorithms are compared based on key space, histogram and differential analysis. The experiment is performed on five different test images. From the results, it is observed that DCT-AES combination of compression-encryption algorithms gives higher resistance to redundant data and provides better security to information during transmission.

Keywords: AES, compression-encryption, DCT, DES, SSIM, PSNR.

Received on 02 February 2020, accepted on 09 April 2020, published on 14 April 2020

doi: 10.4108/eai.13-7-2018.163976

*Corresponding author. Email:ermcet1981@gmail.com

1. Introduction

In recent years, the advancement in information science and technology broadly affects the human daily life. The size of digital data is growing rapidly in order to achieve images of high quality. As a consequence, it requires large space to store and larger bandwidth for transmission over communication channel. Although there is rapid advancement in computer technology for storage techniques, but much of the time, it requires reducing digital data storage so that data can be transmitted faster with limited bandwidth over communication line. The image compression facilitates to transmit large size images with minimal bytes and to restore the image with good quality on reception. Redundant and irrelevant information is removed during image compression using lossy or lossless compression [1]. In lossy image compression redundant information is completely discarded so image quality degrades after reconstruction [2]. Lossless image compression method ensures the transmission of image data with full information and better quality [3].

In modern era of digital data technology, the data transmission through electronic media provides the exchange of information with state of security and secrecy. The cryptographic mechanism provides secure transmission of information or image. In cryptography mechanism the original data is scrambled with a security key to accomplish privacy and integrity of data [4]. In encryption, at the transmitter side, the information or image is encoded with a key, and the original information can be revealed at receiver side through decryption using same key which is used for encryption [5].

On a fundamental level, compression and encryption are two limiting frameworks. Encryption guarantees that transmitted information is trustworthy and essential by changing over it from comprehensible into muddled data with the use of an encoding system [6]. Compression methodology attempts to diminish the size of moved or set away data by finding and emptying duplicate segments of confirmation or instances of data [7]. Nevertheless, compression and encryption are two important steps during processing of image data and both the processes are significantly related. For secure transmission of image with minimum bandwidth, image compression and encryption processes must be used simultaneously [8]. The focuses are to create a more diminutive data size; better quality of data during reconstruction and fasten transmission of data over limited bandwidth with security.

In this paper, we have used the compression technique before encryption because the utilization of compression algorithm before applying encryption algorithm will decrease facsimile part of information which is inclined for cryptanalytic misuse [9]. Likewise, compression of data can accelerate the encryption procedure, and corresponding decoding procedure will construct the plaintext. Since the data compression eliminates repetition of data and also since cryptanalysis utilizes frequency analysis concept that depends on redundant data findings so to use first compression before encryption reduces the viability of cryptanalytic assaults [10].

This paper is having further 5 sections. Section 2 comprises the literature review in which various researches on image compression and encryption methodologies is discussed. Section 3 describes fundamental knowledge about discrete cosine transform (DCT), AES, DES algorithms and performance evaluation parameters. Section 4 illustrates the proposed algorithms. Results and discussions are presented in section 5. Finally, Section 6 includes conclusion and future works.

2. Literature review

Loussert et al. [11] have proposed a hybrid compression and encryption model. In this paper, the compression is based on DCT transformation while the encryption is based on bit XOR operation where finger prints are used as a key. These methods are applied on various samples of data and results shows that if transmission time increases then the processed data is more secure and robust against different cryptanalytic attacks.

Krikor et al. [1] have proposed a encryption algorithm which reduces the process of computation for big size images. In this algorithm the encryption is performed on small stream of bits instead of encrypting full image. In proposed method the image is decomposed in 8x8 blocks. DCT transformation method is applied to transform the 8x8 block of image in frequency domain from spatial domain. The stream cipher i.e. nonlinear back shift register method is used to encrypt the high frequency image blocks. The proposed encryption uses a 48 bits key. For encryption of image using nonlinear shift register method by generating pseudorandom sequence first 32 bits are utilized and to randomize the image remaining 16 bits are used to develop rows and columns. The result shows that the proposed algorithm of encrypting small stream of bits is having high security than if full image data is encrypted.

Gupta and Silakari [12] presented compression and encryption algorithms using chaos theory. In this paper the compression algorithm is used before the encryption process for faster transmission of data. Curvelet transformation is used for compression which removes redundancy in image data. The experimental results shows that the average PSNR is more than 30dB, average entropy is nearly 8, NPCR is more than 99% and UACI is above 33%. These results show that the proposed method gives better transmission performance in terms of security and speed.

Li and Lo [13] recommended a method for hybrid compression and encryption for JPEG image. The motive of this paper is to increase the encryption power with maintaining the compression efficiency. In this paper AC coefficient encryption, DC coefficient encryption and orthogonal transform transformation operation of encryption algorithm are utilized. In this paper sign-flip into butterflies operation on 8x8 DCT transform blocks is applied. The testing result shows that the proposed algorithm shows better security of image from statistical and replacement attacks.

Alfalou et al. [14] have proposed a methodology to perform compression, encryption with fusion of multiple images simultaneously. In this proposed algorithm DCT method is adopted and spectral fusion is utilized simultaneously as per the properties of DCT, spectral filtering, and quantization of encoded frequency. The study shows that the encryption efficiency can be improved if the rotation angle of every block varies randomly just before the fusion. Biometric locks are used to increase encryption efficiency. The results show that the presented algorithm gives the compression ratio of 50% which is higher than the conventional method.

Zhiqianga et al. [15] have proposed a combined image compression and encryption for JPEG images. The encryption algorithm uses a chaotic based operation. The results shows that the proposed algorithm giving better compression ratio with better security during transmission.

Goel, N et al.[16] has combined the lossy and lossless compression methods. DCT is used for lossy compression and Huffman coding is used for lossless compression methodology. Logistic map method is used to perform symmetric encryption process. This paper presents a pictorial view of logistic map dimension which have been used as pseudorandom numbers. This paper shows that many shortcomings of dictionary-scrambling-based encryption technique can be overcome by using proposed methodology. The researcher has used low contrast images as test data and it gives high PSNR values.

Ou et al. [17] have developed an hybrid compression encryption algorithm to process the image data. In this paper DWT is combined with the Haar wavelet transform without quantizer to perform the compression process. The AES algorithm is used for encryption purpose. The motive of this paper is to develop an algorithm by which high compression ratio can be generated for compressed images without disturbing the security concern. By this method the image data can be transmitted on lower bandwidth with security. The proposed method is applied on six gray scale images having different sizes and it also shows that the reconstructed images are efficient and having high quality.

Shen H., L. Zhang et al. [18] have proposed an burgeoning compressive sensing based baysian dictionary learning algorithm. Authors have used this algorithm to overcome the problem of dead pixel strips in MODIS. These dead pixel strips are spread over large area of satellite images in band 6 and corrupt the products of MODIS. Authors have demonstrated the efficiency of proposed algorithm on Terra and Aqua images.

Zhou N., Zhang A. et al. [19] have proposed a method for hybrid compression and encryption to provide easy distribution and storage of the encryption key. In this algorithm, the input image is divided in four blocks and pixels of two adjacent blocks are randomly exchanged by random matrices. These random matrices are bounded by measurement matrices. Authors have shown that proposed algorithm provide better security and moderate compression efficiency.

3. Fundamental knowledge

3.1. Image Transformation

The image transformation represents transforming of image data from one domain to another domain. During image transformation the data sequence of image is transformed from spatial domain to frequency domain or vice versa. This transformation enables the extraction of various features of image that may not be detected in spatial domain. In every transformation technique data should be divided into sub bands which are having least dependence on each other.

In this paper, DCT based compression algorithm is proposed for compressing the image data. The proposed DCT based compression algorithm designed to operate $M \times N$ block sizes. During DCT transformation, block is divided in to two bands, one is low frequency band which has important visual information of the image and another band is high frequency band which has texture and details of the image. The DCT operates a block B of $M \times N$ samples and creates Z, which represent $M \times N$ block of coefficients. The high frequency coefficients are least important than lower frequency coefficients because high frequency coefficients values are usually closed to zero. In this research, for designing the DCT based compression algorithm, the high frequency band is removed. The DCT of an $M \times N$ sample block is represented as:

$$C(u,v) = \alpha_u \alpha_v + \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} I(x,y) \cos\frac{\pi(2x+1)u}{2M} \cos\frac{\pi(2y+1)v}{2N} \quad (1)$$

$$I(x,y) = \alpha_u \alpha_v + \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} C(u,v) \cos\frac{\pi(2x+1)u}{2M} \cos\frac{\pi(2y+1)v}{2N} \quad (2)$$

Where

$$\alpha_u = \begin{cases} \frac{1}{\sqrt{M}}, & u = 0 \\ \frac{2}{\sqrt{M}}, & 1 \le u \le M-1 \end{cases} \qquad \alpha_v = \begin{cases} \frac{1}{\sqrt{N}}, & v = 0 \\ \frac{2}{\sqrt{N}}, & 1 \le v \le N-1 \end{cases}$$

The values $C(u,v)$ are called the DCT coefficients of image.

The result of the DCT transformation for a block in the spatial domain is a set of frequencies that are arranged in a zigzag ascending order as shown in Figure 2. The frequency located at *f (0, 0)* is the lowest frequency and is called the DC value. This value represents the general style of the block and considered to be the most important frequency amongst all the other frequencies in the block. The rest of the frequencies range from low to high in a zigzag pattern and are called the AC values. The AC values contain the details of the block which range from general to fine details, as we progress forward in the zigzag order.

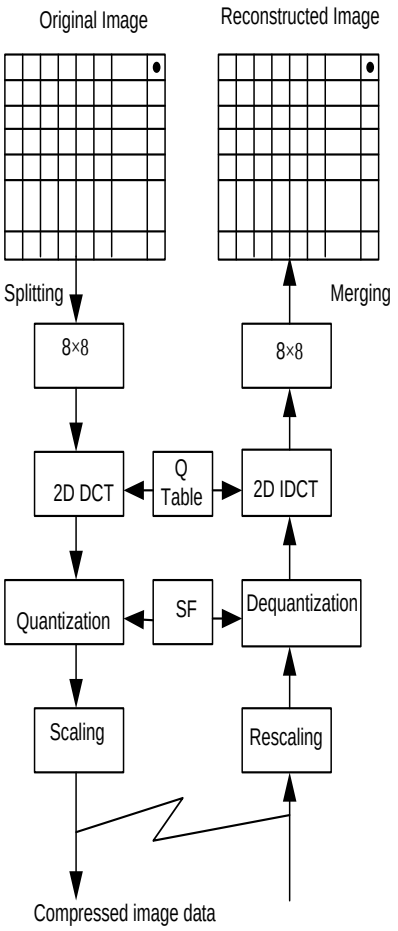


Figure 1. Block diagram of the JPEG-based DCT scheme

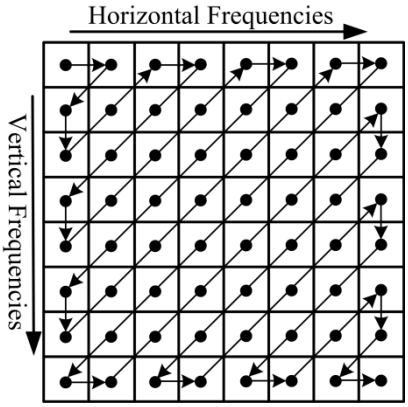


Figure 2. Sequence of an 8×8 frequency block, from low to high

3.2 DCT based compression algorithm

DCT has block artifacts that can be minimized by selecting small size of block. By using 8x8 block size and applying quantization minimize each pixel value 0 to 32 so 5 bits needed to represent pixel value.

1. Gray scale image is taken as input to compress. If original Input image is coloured then converted into gray scale image.
2. Each pixel value is subtracted by 128 to put 0 in the middle of the range.
3. Then resultant matrix is divided into blocks of size 8x8.
4. DCT is applied to each block to convert pixels in the spatial domain into coefficients in the frequency domain. DCT element (0,0) is the average value of the block the other element tells about spectral power present at each spatial frequency.
5. Less important DCT coefficient are wiped out by using quantization.
6. Linearize the 64 element of each block using zigzag scanning and apply run length encoding.
7. Encodes the numbers using Huffman encoding.
8. Compressed image is encrypted using AES.

3.3 AES algorithm for encryption

AES has flexibility in key length. Same plaintext block size can use 128 bit, 192 bit key or 256 bit key for different no. of rounds respectively 10, 12 or 14. This feature of AES makes it more secure against cryptanalysis attacks. Al l operations are performed on entire byte rather than on each bit of plaintext and key. AES algorithm steps involve one-time initialization process followed by processes in 10 rounds.

A. One time initialization process

- In the first step16 byte key is expanded into 176 bytes in the form of 11 arrays of size 4*4.
- Original 16 byte key is copied into first array of 4 words w [0] to w [3].
- For remaining 10 array if word index i is multiple of 4 then substitute, Rotate and constant functions are performed.
- If word index is not multiple of 4 then simply perform XOR operation between w [i-1] and w [i-4].
- In Rotate function contents of the word is shifted by one byte.
- Byte in a word is substituted using S-Box.
- Resulting bytes are XORed with constant function.
- After expanding 16 byte key, 16 bytes plaintext is copied in column order into a 4*4 two dimensional array. This array word is XORed with first array of expanded key.

After completion of pre-round transformation, following 4 steps are repeated 10 times.

- Using S-box generated plain text byes are replaced.
- Bytes in each row of the substituted plaintext are rotated by row no.
- Using Galois field multiplication mix column operation is performed on generated bytes. Resulting matrix is *XORed* with the key for this round.

In reverse order the same process is executed for decryption.

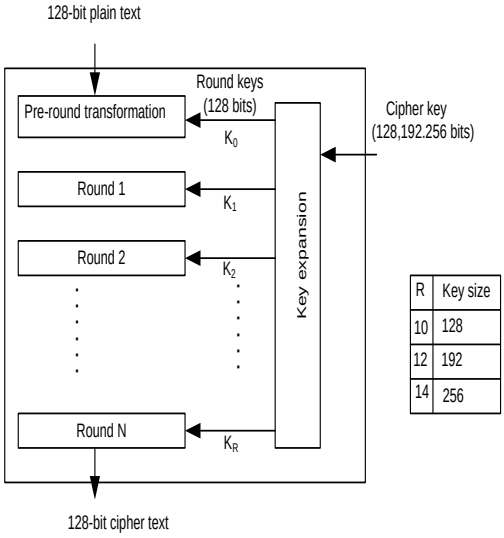


Figure 3. Block diagram representation of AES encryption process

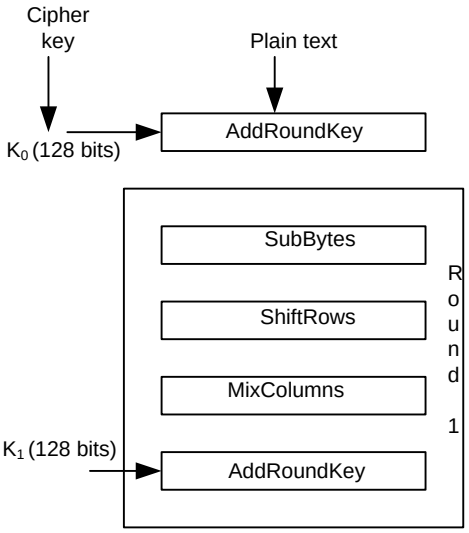


Figure 4. Every round steps in AES encryption algorithm

3.4 DES Algorithm for encryption

The Data Encryption Standard (DES) is a block cipher symmetric key cryptographic algorithm, which is published in January 1977 by the US National Bureau of Standards [2], [3]. Input binary data is divided into blocks of size 64 bits that is encrypted by using key of length 56 bits. Confusion (substitution) and diffusion (transposition) are the Basic fundamentals of cryptography that is used in DES. In Data encryption standard algorithm, initially 64 bits in a block is permuted where jugglery of bit positions

take place. 64 bits permuted data is divided into two halves each of 32 bits that is known as left plaintext and right plaintext. 16 identical rounds are performed on these two blocks using the key. These 16 identical rounds consist of key transformation, permutation and substitution and finally XOR operation. After completing 16 rounds final permutation is performed.

During each round following operations are performed:

- In key transformation process different 48 bit key is generated using compression permutation.
- Generate different 48 bit key during each round makes DES highly secure.
- Right plaintext data of 32 bits is expanded to 48 bits using expansion permutation.
- This 48 bit expanded data is XORed with 48 bit key.
- Using S- box substitution 48 bit input is substituted in 32 bits Right plain text.
- 32 bit right plain text data is permuted and then XORed with 32 bit left plaintext.
- Reverse process is applied for decryption.
- During decryption process subkeys are used in reverse order

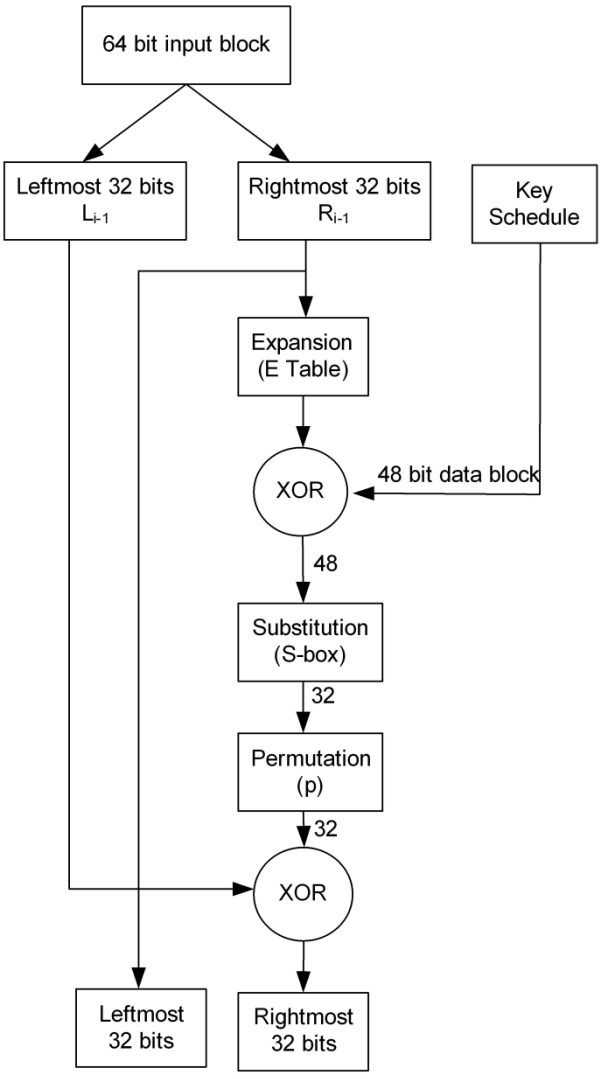


Figure 5. Block diagram representation of DES encryption algorithm

4. Performance evaluation metrics

Image compression reduces the size of transmitted or storage data but the challenge is to have no destruction in reconstructed image at receiver end. Peak signal to Noise ratio (PSNR) and Structural similarity index (SSIM) are the two important features of image compression technique. For a good image compression technique the compressed image must have high values of PSNR and SSIM. Image encryption algorithms change the pixel value of an image. These changes in pixel values must be maximum and be in an irregular manner. The encrypted image must contain totally random patterns so that no feature of original image can be extracted by these random patterns. The encrypted image must have low correlation with original image.

4.1 The image compression performance parameters

The quality of compressed image can be measured by calculating PSNR in dB and SSIM in percent. PSNR is defined as the ratio of square of input image size and the Mean Square Error (MSE). The image quality and PSNR are directly proportional to each other i.e. as PSNR increases the compressed image quality also increases.

$$\text{PSNR} = 10\ log_{10}\ \frac{M\times N\}^2}{MSE} \quad (3)$$

The Mean Square Error can be expressed as,

$$\text{MSE} = \frac{1}{M\times N} \sum_{X=1}^{M} \sum_{Y=1}^{N} [f(x,y) - g\ (x,y)]^2 \quad (3.1)$$

Where $f(x,y)$ and $g(x,y)$ denotes the original and reconstructed pixel respectively, and the images are of size $M \times N$.

Structural Similarity Index (SSIM) evaluates the similarity between processed image and original image. The SSIM depends on luminance, contrast and structural term. The overall index is a multiplicative combination of the three terms.

$$SSIM(x,y)=[l(x,y)]^{\alpha}.[c(x,y)]^{\beta}.[s(x,y)]^{\gamma} \quad (4)$$

$$l(x,y) = [2\mu_x\mu_y + c_1]/[\mu_x^2 + \mu_y^2 + c_1] \quad (4.1)$$

$$c(x,y) = [2\sigma_x\ \sigma_y + c_2]/[\sigma_x + \sigma_y + c_2] \quad (4.2)$$

$$s(x,y) = [\sigma_{xy} + c_3]/[\sigma_x\sigma_y + c_3] \quad (4.3)$$

Where μ_x , μ_y are the moment about the mean for x and y respectively and σ_x^2 , σ_y^2 are variance of x and y respectively. α, β and γ are the weights. $c_1 = (k_1L)^2$ and $c_2 = (k_2L)^2$ are two variables and $L = 2^{bits\ per\ pixel} - 1$, showing the dynamic range of pixel values.

4.2 The image encryption performance parameter

The motive behind the encryption of data is to protect the information from brute force attacks. In encryption algorithms, the original image is substituted by encrypted images and both the images i.e. original image and encrypted image are uncorrelated with each other. The performance of an image encryption algorithm is evaluated

based on key space analysis, histogram analysis and differential analysis.

Key space analysis

The key-space analysis of an encryption algorithm is the wide range of possible keys that can be utilized for data encoding using that algorithm. To make the brute force attack infeasible, the range of the keys must be suitably large so that key space can be large.

Histogram analysis

For a better security of the transmitted information the encryption algorithm should not provide any statistical alignment between encrypted image and original image. The pixel value distribution of an image can be viewed with the help of histogram analysis. The histogram of original image has sharp rises and sharp falls while the histogram of encrypted image has uniform distribution. Both the histograms of encrypted image and original image have no statistical similarities.

Differential analysis

The encrypted image should be sensible to small changes in input image. The linkage between original image and encrypted image can be analyzed by modifying only single pixel in original image and observe the variation in cipher image. If the variations in cipher image are significant with respect to small changes in original image, then the encrypted image is secure from differential attacks.

When one-pixel value is change in original image then Number of Pixels Change Rate **(**NPCR) gives difference in pixel values of two generated cipher text in terms of percentage. To show resistance of algorithm against differential attack percentage value should greater than 99%.

Consider the two cipher-images, C^1 and C^2, whose corresponding plain images have only one pixel difference the NPCR of these two images is defined as

$$NPCR\ (C^1, C^2) = \sum_{i,j} \frac{D(i,j)}{M \times N} \times 100\ \% \qquad (5)$$

Where M×N defines the size of image and $D(i,j)$ is defined as

$$D(i,j) = \begin{matrix} 0,\ if\ C^1(i,j) = C^2(i,j) \\ 1,\ if\ C^1(i,j) \neq C^2(i,j) \end{matrix} \qquad (6)$$

Unified Averaged Changed Intensity **(**UACI) gives averaged changed intensity difference between original and modified cipher text images. The mathematical formula of UACI is given by

$$UACI\ (C^1, C^2) = \quad _{i,j} \frac{C^1(i,j) - C^2(i,j}{M \times N} \times 100\% \qquad (7)$$

5. System environment

The computer system used in this simulation is Windows10, and the simulation software used is MATLAB 2018B.

6. Results and discussions

In this paper the digital images which are two-dimensional digital data are selected for experimental purpose. The test data set contains 5 digital images on which experiments have been performed. The standard images like Baboon, Boat, Lina, Pepper and Barbara are used in this article. All images are gray scale having size of *512 × 512* and .BMP format. In this article, compression algorithms are applied first and then compressed images are encrypted. It can be seen from literature review that the cost of security is minimum if compression is performed before encryption [20]. In this research three different case studies are analyzed:

Case 1: images are only compressed through DCT based algorithm,

Case 2: images are compressed-encrypted through DCT-AES based algorithms

Case 3: images are compressed encrypted through DCT-DES based algorithms.

The fig. 6 is showing the pictorial representation of the Original images and processed images. Column 1 is showing the original images of Baboon, Boat, Lina, Pepper and Barbara which are used as test images. Column 2 is representing the histogram of corresponding original images. It has been observed that there are sharp rise and falls in histogram of original images. DCT based algorithm is used to perform the compression process of original image and compressed images are represented in Column 3. To secure the image information from brute force attacks, AES algorithm is used for encrypting the original compressed image. The encrypted images are shown in column 4 corresponding to 5 test images and their corresponding histograms are represented in column 5. From column 5 it has been analyzed that histograms of compressed encrypted images are flat in nature with respect to histogram of original images.

The compressed encrypted images are decompressed and decrypted by using inverse DCT transformation and inverse AES algorithm respectively in order to get the original image. After decompression and decryption the results are graphically represented in column 7 of Fig. 6 with their histograms in column 6. From the comparison of column 2 and column 6 it can be observed that the histograms of original image and processed image are similar in nature.

Fig. 7 is also showing the pictorial representation of original images with their corresponding histograms. Again the DCT based compression is used to compress the original image. Now DES algorithm is used to encrypt the DCT based compressed images. Again the results are shown for same 5 test images which are used in DCT-AES based compression and encryption process. In both the processes i.e. DCT-AES and DCT-DES, compression algorithm is implemented prior to implementing the encryption algorithm. The histograms of unprocessed original images are having sharp rise and falls while the DCT-AES compressed encrypted images are having flat continuous histogram which is defined at every frequency. Original image and decompressed decrypted images are

analyzed based on their histograms and it is found that both the images and corresponding histograms are similar.

6.1 DCT-AES Compression-encryption algorithm results

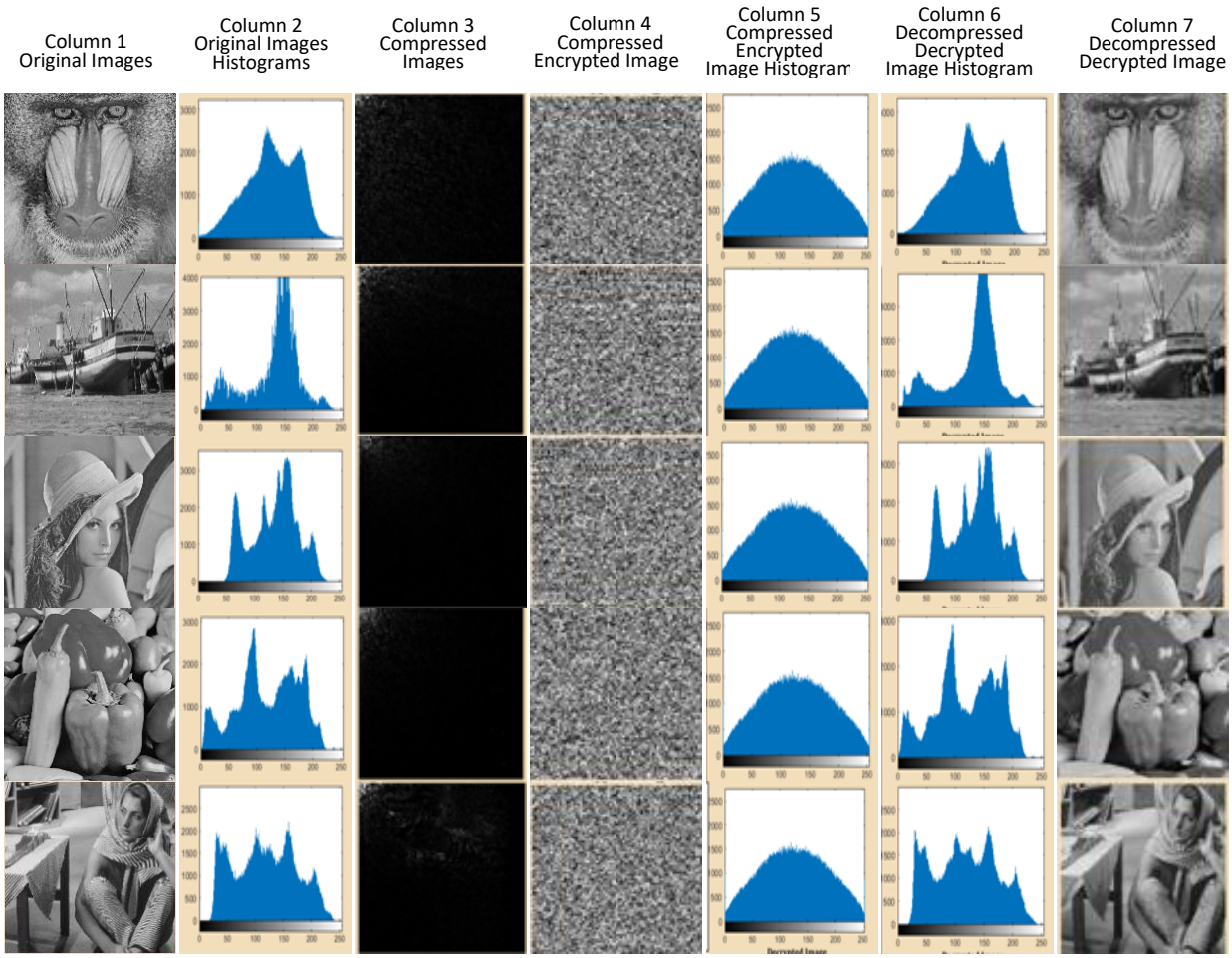
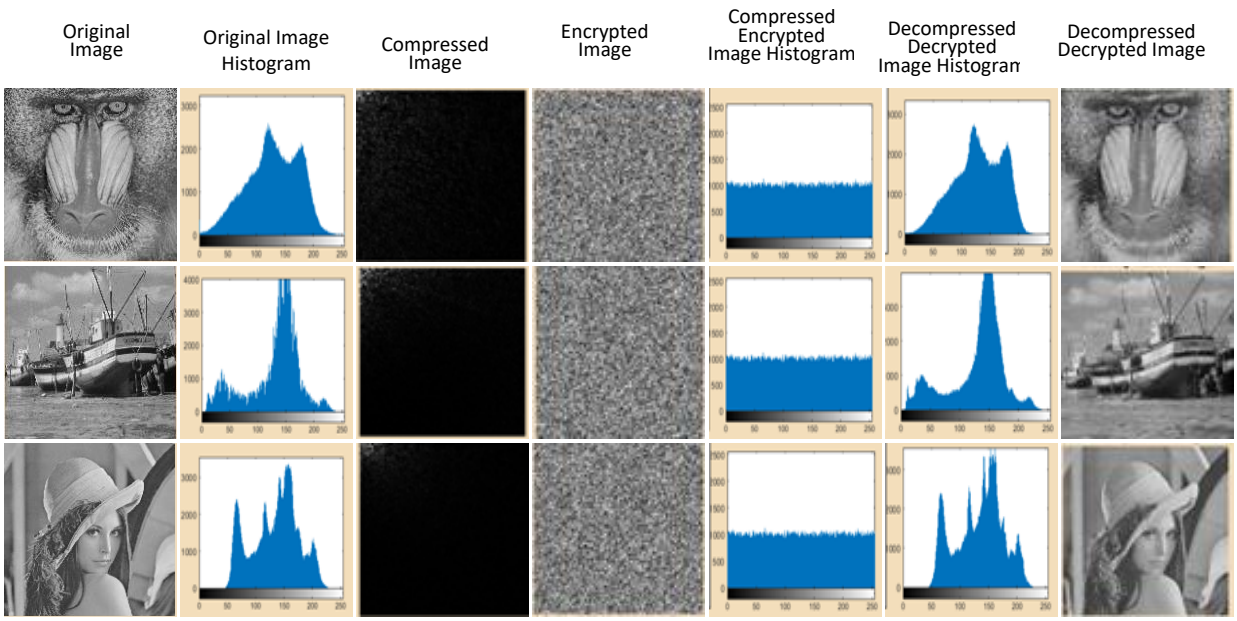


Figure 6. columns 1-3 are original Images (Courtesy of SIPI image data base), original image histogram, DCT based compressed image respectively, column 4 is AES encrypted image, column 5 is compressed-encrypted image histogram, column 6 is decompressed-decrypted image histogram, and column 7 is decompressed-decrypted image.

6.2 DCT-DES Compression-encryption algorithm results



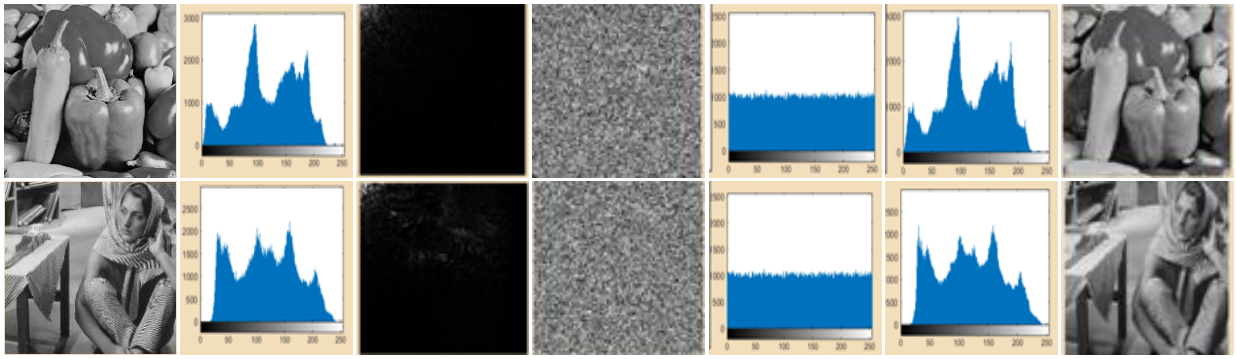


Figure 7. columns 1-3 are original Images (Courtesy of SIPI image data base), original image histogram, DCT based compressed image respectively, column 4 is DES encrypted image, column 5 is compressed-encrypted image histogram, column 6 is decompressed-decrypted image histogram, and column 7 is decompressed-decrypted image.

Table 1. Comparison of PSNR values

Image File	Our Proposed Methods			Comparative data from other research schemes	
	Only Compression through DCT	Compression - encryption DCT-AES	Compression - encryption DCT-DES		
Baboon	23.797	31.706	29.5847	22.19 (EZW technique) Ref. [21]	22.26 (WDR technique) Ref. [21]
Boat	30.3878	36.4433	35.1293	30.7580 Ref. [22]	X
Lina	33.0825	38.8256	37.5876	30.68 Ref. [23]	22.62 Ref. [24]
Pepper	33.7247	40.0179	38.7292	31.24 Ref. [7]	23.59 Ref. [21]
Barbara	28.15	36.57	34.65	22.92 (EZW technique) Ref.[21]	25.79 (WDR technique) Ref.[21]

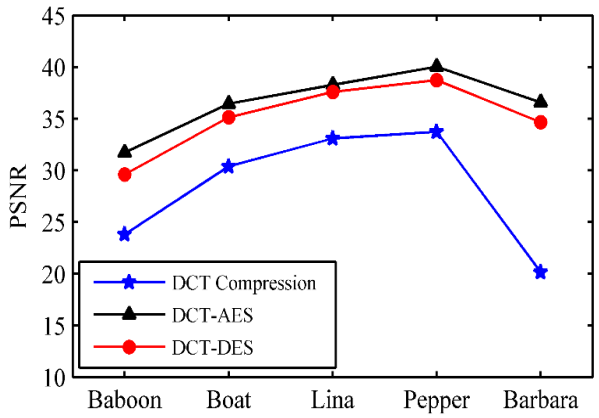


Figure 8. Graphical representation of comparison of PSNR values

Table 1 compares the PSNR value for 5 test images under three case studies. It is observed that PSNR value increases while the encryption process is applied after compression. The value of PSNR during DCT-AES and DCT-DES compression-encryption process is greater than 30dB which shows that human visual system can not identify the difference between original image and processed image [25].

The increase in PSNR value in DCT-AES compression-encryption algorithm is higher than the DCT-DES. Fig. 8 is showing the graphical representation of PSNR values for all five test images.

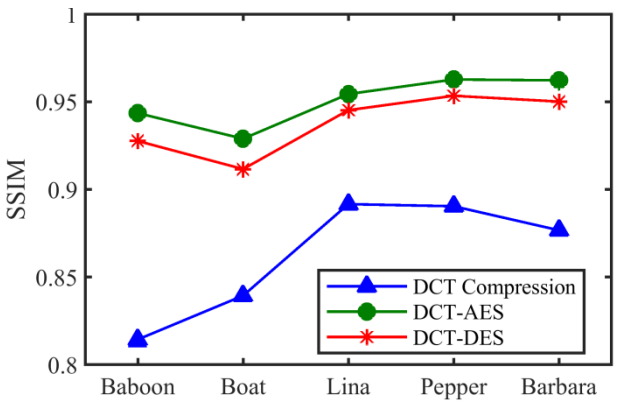


Figure 9. Graphical representation of comparison of SSIM values

Table 2. Comparison of SSIM values

Image File	Our Proposed Methods			Comparative data from other research schemes	
	Only Compression through DCT	Compression - encryption DCT-AES	Compression - encryption DCT-DES		
Baboon	0.8144	0.9435	0.9276	0.8756 Ref. [22]	0.9288 Ref. [26]
Boat	0.8394	0.9289	0.9116	0.8353 Ref. [22]	0.6949 Ref. [27]
Lina	0.8916	0.9544	0.9452	0.8495 Ref. [22]	0.9239 Ref. [26]
Pepper	0.8904	0.9627	0.9534	0.8215 Ref. [22]	0.9409 Ref. [26]
Barbara	0.8767	0.9622	0.9501	X	X

Table 2 compares the Structural similarity index (SSIM) for five test images under three case studies. It is observed that under case 1 the SSIM value is low. As the value of SSIM should be high for efficient reconstruction of image at receiver side so if the DCT compression algorithm followed by AES and DES encryption algorithms (Case studies 2 and 3) are implemented then the value of SSIM increases. From the table 2 it can also be observed that SSIM attains higher value under case 2 in compare with case 3. Fig. 9 is showing the graphical representation of SSIM for only compression and compression-encryption processes for various test images.

Table 3. Comparison of NPCR values

Image File	Our Proposed Method		Comparative data from other research schemes	
	Compression -encryption DCT-AES	Compression -encryption DCT-DES		
Baboon	0.9971	0.9961	0.9960 Ref. [28]	0.9961 Ref. [29]
Boat	0.9959	0.9955	0.9960 Ref. [28]	X
Lina	0.9962	0.995	0.9960 Ref. [28]	0.9958 Ref. [12]
Pepper	0.995	0.9956	0.9961 Ref. [28]	0.99608 Ref. [29]
Barbara	0.9954	0.9951	X	X

NPCR and UACI are two important parameters which are used here for differential analysis of encryption algorithm. In this paper two different encryption algorithms AES and DES are used to encrypt the compressed image. The comparison of NPCR and UACI during AES and DES algorithms is shown in table 3 and table 4 respectively. The value of NPCR and UACI must be greater than 99% and 33% respectively for providing better security to image during transmission. From the table 3 and table 4, it is observed that in both the encryption algorithms the values of NPCR and UACI is higher than the threshold limit for all 5 test images.

The values of NPCR and UACI during DCT-AES compression-encryption algorithms are higher than the DCT-DES compression-encryption algorithms. The graphical representation of NPCR and UACI for both the compression-encryption algorithms for different test images is shown in Fig. 10 and Fig. 11 respectively.

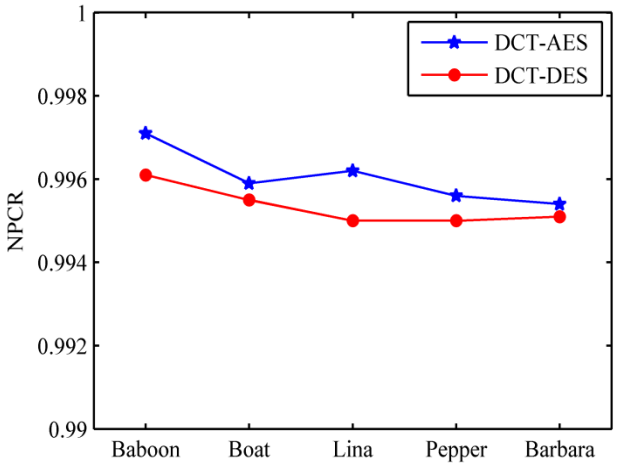


Figure 10. Graphical representation of comparison of NPCR values

Table 4. Comparison of UACI values

Image File	Our Proposed Method		Comparative data from other research schemes	
	Compression -encryption DCT-AES	Compression - encryption DCT-DES		
Baboon	0.3353	0.3345	0.33442 Ref. [28]	0.33464 Ref. [29]
Boat	0.3367	0.3352	0.33452 Ref. [28]	X
Lina	0.3349	0.3334	0.33456 Ref. [28]	0.33467 Ref. [29]
Pepper	0.3386	0.3369	0.33468 Ref. [28]	0.33468 Ref. [29]
Barbara	0.3392	0.3381	X	X

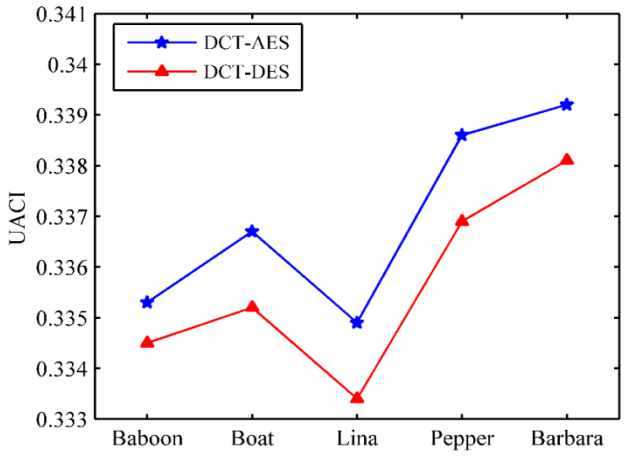


Figure 11. Graphical representation of comparison of UACI values

7. Conclusion and future research

In this paper, we present a DCT based compression algorithm for compressing the image. The compressed image is encrypted by two different encryption algorithms AES and DES. The efficiency of proposed compression-encryption methods is analyzed through PSNR, SSIM, NPCR and UACI. From the results it is observed that combination of DCT-AES compression-encryption algorithm provides higher values of PSNR and SSIM. From both the combinations of compression-encryption methodology, the value of NPCR and UACI is larger than 99% and 33% respectively but DCT-AES combination provides higher NPCR and UACI in comparison with DCT-DES combination. It has been authenticated that the DCT-AES combination of compression-encryption algorithm capable of removing redundancy in image data effectively and also provides better security during transmission.

The proposed research can be further implement and analyse on colour images as well as on high quality satellite images. The presented research can also be further extended on encryption followed by compression methodology.

References

[1] L. Krikor, S. Baba, T. Arif, and Z. Shaaban, "Image encryption using DCT and stream cipher," *Eur. J. Sci. Res.*, vol. 32, no. 1, pp. 48–58, 2009.

[2] X. Zhang, "Lossy Compression and Iterative Reconstruction for Encrypted Image.," *Inf. Forensics Secur.*, pp. 53–58, 2011.

[3] S.S.Maniccama N.G.Bourbakis, "Lossless image compression and encryption using SCAN," *Pattern Recognit.*, vol. 34, no. 6, pp. 1229–1245, 2001.

[4] M. Yang, N. Bourbakis, and S. Li, "Data-image-video encryption," *IEEE Potentials*, vol. 23, no. 3. pp. 28–34, Aug-2004.

[5] M. A. Al-Khasawneh, S. M. Shamsuddin, S. Hasan, and A. A. Bakar, "An Improved Chaotic Image Encryption Algorithm," in *2018 International Conference on Smart Computing and Electronic Enterprise, ICSCEE 2018*, 2018.

[6] X. Zhang, "Lossy compression and iterative reconstruction for encrypted image," *IEEE Trans. Inf. Forensics Secur.*, vol. 6, no. 1, pp. 53–58, Mar. 2011.

[7] F. Hu, C. Pu, H. Gao, M. Tang, and L. Li, "Image compression and encryption scheme based on deep learning," *Nauk. Visnyk Natsionalnoho Hirnychoho Universytetu*, no. 6, pp. 142–148, 2016.

[8] P. A. J. Rani, "Encryption-then-Compression Techniques : A Survey," pp. 675–679, 2016.

[9] M. Morales-Sandoval and C. Feregrino-Uribe, "A hardware architecture for elliptic curve cryptography and lossless data compression," in *Proceedings - 15th International Conference on Electronics, Communications and Computers, CONIELECOMP 2005*, 2005, vol. 2005, pp. 113–118.

[10] M. Sharma and S. Gandhi, "Compression and Encryption : An Integrated Approach," *Int. J. Eng. Res. Technol.*, vol. 1, no. 5, pp. 1–7, 2012.

[11] A. Loussert, A. Alfalou, R. El Sawda, and A. Alkholidi, "Enhanced System for Image ' s Compression and Encryption by Addition of Biometric Characteristics," *Int. J. Softw. Eng. Its Appl.*, vol. 2, no. 2, pp. 111–118, 2008.

[12] K. Gupta and S. Silakari, "Novel Approach for fast Compressed Hybrid color image Cryptosystem," *Adv. Eng. Softw.*, vol. 49, pp. 29–42, 2012.

[13] P. Li and K. T. Lo, "Joint image compression and encryption based on alternating transforms with quality control," in *2015 Visual Communications and Image Processing, VCIP 2015*, 2016.

[14] A. Alfalou, C. Brosseau, N. Abdallah, and M. Jridi, "Assessing the performance of a method of simultaneous compression and encryption of multiple images and its resistance against various attacks," *Opt. Express*, vol. 21, no. 7, p. 8025, 2013.

[15] Z. Li, X. Sun, C. Du, and Q. Ding, "JPEG algorithm analysis and application in image compression encryption of digital chaos," in *Proceedings - 3rd International Conference on Instrumentation and Measurement, Computer, Communication and Control, IMCCC 2013*, 2013, pp. 185–189.

[16] N. Goel, B. Raman, and I. Gupta, "Chaos based joint compression and encryption framework for end-to-end communication systems," *Adv. Multimed.*, vol. 2014, 2014.

[17] S. C. Ou, H. Y. Chung, and W. T. Sung, "Improving the compression and encryption of images using FPGA-based cryptosystems," *Multimed. Tools Appl.*, vol. 28, no. 1, pp. 5–22, Jan. 2006.

[18] H. Shen, X. Li, L. Zhang, D. Tao, and C. Zeng, "Compressed

sensing-based inpainting of aqua moderate resolution imaging spectroradiometer band 6 using adaptive spectrum-weighted sparse bayesian dictionary learning," *IEEE Trans. Geosci. Remote Sens.*, vol. 52, no. 2, pp. 894–906, Feb. 2014.

[19] N. Zhou, A. Zhang, F. Zheng, and L. Gong, "Novel image compression-encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing," *Opt. Laser Technol.*, vol. 62, pp. 152–160, 2014.

[20] E. Setyaningsih and R. Wardoyo, "Review of Image Compression and Encryption Techniques," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 2, 2017.

[21] S. P. Raja and A. Suruliandi, "Performance evaluation on EZW & WDR image compression techniques," in *2010 IEEE International Conference on Communication Control and Computing Technologies, ICCCCT 2010*, 2010, pp. 661–664.

[22] C. Agarwal, A. Mishra, and A. Sharma, "A novel gray-scale image watermarking using hybrid Fuzzy-BP N architecture," *Egypt. Informatics J.*, vol. 16, no. 1, pp. 83–102, Mar. 2015.

[23] N. Zhou, S. Pan, S. Cheng, and Z. Zhou, "Image compression-encryption scheme based on hyper-chaotic system and 2D compressive sensing," *Opt. Laser Technol.*, vol. 82, pp. 121–133, Aug. 2016.

[24] N. Zhou, A. Zhang, J. Wu, D. Pei, and Y. Yang, "Novel hybrid image compression-encryption algorithm based on compressive sensing," *Optik (Stuttg).*, vol. 125, no. 18, pp. 5075–5080, Sep. 2014.

[25] S. Tedmori and N. Al-Najdawi, "Lossless image cryptography algorithm based on discrete cosine transform," *Int. Arab J. Inf. Technol.*, vol. 9, no. 5, Sep. 2012.

[26] H. Wang, X. Xiao, X. Peng, Y. Liu, and W. Zhao, "Improved image denoising algorithm based on superpixel clustering and sparse representation," *Appl. Sci.*, vol. 7, no. 5, 2017.

[27] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Trans. Image Process.*, vol. 13, no. 4, pp. 600–612, Apr. 2004.

[28] Y. Wang, K. W. Wong, X. Liao, and G. Chen, "A new chaos-based fast image encryption algorithm," *Appl. Soft Comput. J.*, vol. 11, no. 1, pp. 514–522, Jan. 2011.

[29] Y. Zhang, "The unified image encryption algorithm based on chaos and cubic S-Box," *Inf. Sci. (Ny).*, vol. 450, pp. 361–377, Jun. 2018.