EAI Endorsed Transactions
on Scalable Information Systems
Research Article EAI.EU

Performance Evaluation of Symmetrical Encryption Algorithms with Wavelet Based Compression Technique

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

[1] Research Scholar, Computer Science & Engineering Department, Banasthali University, Banasthali, India.
[2] Dean & Professor, Department of Electronics, Banasthali University, Banasthali, India.
[3] Professor, Department of Electronics & Communication Engg. Vaagdevi College of Engineering., Warangal, India.

Abstract

To overcome the different issues connected with security and limited bandwidth during transmission of images, compression and encryption play an important role. To measure the effect on the performance of compression technique followed by encryption techniques is a challenging task. In this paper, biorthogonal discrete wavelet transform (DWT) technique is proposed for compression which is followed by advanced encryption standard (AES) and data encryption standard (DES) technologies to achieve secure transmission of data. The performances of DWT-AES and DWT-DES Compression-encryption (CE) algorithms are analyzed based on statistical and differential parameters. We illustrate the authentication of results by applying the proposed CE algorithms over five standard test images and also by comparing with different state of the art methods. The results show that combination of DWT-DES CE methodology provides high quality of reconstructed image with robustness against different attacks.

Keywords: Compression-encryption (CE), DWT-AES, DWT-DES, Security, attacks

Received on 04 March 2020, accepted on 19 May 2020, published on 28 May 2020

doi: 10.4108/eai.13-7-2018.164825

*Corresponding author. Email: ermcet1981@gmail.com

1. Introduction

As the use of internet to transmit the information from sender to receiver is increasing in our daily lives. Security and bandwidth are the two important parameters during transmission of information. The large size information needs compression of data so that it can be transmit with limited bandwidth and minimal transmission time [1]. Every sender also wants to secure the information from various unethical attacks during transmission. To provide the security to transmitting data during transmission, encryption is performed [2]. So, compression and encryption are the two important methods during transmission of data where compression reduces the need of higher transmission bandwidth by minimizing the redundancy of data and encryption provides security to information against different attacks [3][4]. Compression and encryption, both processes are having key importance for secure transmission of images over minimal bandwidth. Compression and encryption processes can be used in either order i.e. compression prior to encryption or compression after the encryption. The advantages of using compression algorithm before applying encryption algorithms are as follows [5]:

A. It reduces the possibility of decoding of encrypted image by hackers.
B. It reduces the encryption/decryption algorithms execution time.
C. It reduces the misuse of cryptanalysis.

On the basis of redundancy removal methodology, the compression techniques are classified in two categories as Lossless and Lossy compression. Lossless compression

methods, like Arithmetic coding, LempelZiv algorithm, Entropy Encoding, Run Length coding, and Huffman coding, produce original image from compressed image during reconstruction without any loss of information [6]. The lossless compression removes minimum amount of redundancy from the original image and by this it has low compression ratio [7]. On the other hand, however lossy compression methods, like discrete cosine transform, discrete wavelet transform, fractal algorithm, Block Truncation coding etc., allows the reconstruction of original image from compressed image but the quality of reconstructed image will be degraded based upon the threshold used but with higher compression ratio [5]. If a system needs compression of image data up to a great extent with little compromise in image quality at receiver end then the lossy compression methods are advantageous.

The wavelet transform is used to find the better compression ratio by transforming the image data from time space domain to time frequency domain [8][9]. Multi resolution image analysis can be performed by using wavelet transform. In this paper, discrete wavelet transform (DWT) is used for compression of image because it decomposes an image into lower resolutions and works on the principle of thresholding [10]. DWT also offers time-frequency localization through which error occurring due to thresholding can be minimized. In DWT the transformation is performed on entire image so that at low bit rate correlation can not be lost between subbands [11].

In this paper, the combination of compression and encryption is used to remove redundant data and to provide security to the image during transmission. The main contributions of this paper are as follows:

(i) The performance evaluation is carried out in two ways:
- Image is compressed using DWT based compression algorithm. 5th level DWT Biorthogonal based lossy compression algorithm is used for compression.
- DWT based compressed image is followed by encryption algorithms. Symmetric encryption algorithms AES and DES are used for encryption of image.

(ii) The effect on performance parameters, i.e. peak signal to noise ratio (PSNR), mean square error (MSE), structural similarity index metric (SSIM) and computational time during execution of compression-encryption algorithms is analysed.

(iii) The efficiency of AES and DES symmetrical encryption algorithms over DWT compressed image is also compared on the basis of Number of Pixels Change Rate **(**NPCR) and Unified Averaged Changed Intensity **(**UACI), Correlation coefficient, Key sensitivity analysis and Entropy analysis.

(iv) Histogram analysis is performed to show that encrypted image has no statistical similarity with original image and reconstructed images are similar with original images.

In this paper, Literature review which comprises the different techniques for image compression and encryption and their outcomes is incorporated in section 2. The different algorithms (DWT, AES, DES) used in this study are explained in section 3. Results with performance evaluation parameters are illustrated in section 4. Conclusion and future work are presented in section 5.

2. Literature review

As the need of secure transmission of information over communication channel with minimum use of bandwidth is growing rapidly, a variety of research in the field of compression and encryption of information is taking place. In 2015 Wang et al. [12] have proposed DWT transformation on input image using Bior 2.2 wavelet filters with 3 level of decomposition. Resulted sub bands LL and (LH, HL, HH) are encrypted using stream cipher and permutation method respectively. Results show that compression ratio is 4.461 and PSNR is the range of 30-35 dB for different 512x512 pixel size test images. In 2016 Tong et al. [13] have proposed a compression-encryption technique by combining lifting wavelet transform (LWT) and set partitioning hierarchical tree (SPIHT) followed by chaotic sequence generation symmetrical encryption scheme. Authors have shown that proposed technique is highly sensitive to plain text and have excellent key sensitivity. Entropy value of five test images are in range of 7.5 to 7.99 and compression ratio is 50%. In 2017 S. Gonge et al. [14] have also proposed a watermarking technique for digital 2D images using combination of discrete wavelet transform and advanced encryption standard. In 2017 ahmad et al. [15] have proposed a image encryption algorithm based on orthogonal matrices and chaos theory. Authors have recovered original image from AWGN interrupted received image. The PSNR is about 40dB, NPCR is 99.1% and UACI is 15.4%. Here the PSNR is having moderate value so quality of decompressed image is average but since UACI is lower than the threshold value that is 33%, then proposed algorithm is lacking in security during transmission. In 2017 E. Setyaningsih et al. [5] have presented a review paper on performance of different compression and encryption methodologies. The performance of two hierarchies, one is cryptographic techniques followed by compression and second is compression followed by encryption process, are analysed. Compression followed by encryption process shows better performance in terms of security and reconstruction of image. In 2017 Kumar and Vaish [16] proposed a combined CE methodology for fast and secure transmission of image. The first step is the DWT transformation process and then pseudo random encryption process (PRNG) is applied. The test results demonstrate that the use of biorthogonal wavelet filter produces better compression performance. Authors show that PSNR and compression ratio for Lina test image under biorthogonal compression method are 45.66 dB and 0.2883 respectively. In 2019 S. ambadekar et al. [17] have proposed a technique for digital watermarking using DWT and encryption technology. Authors have used watermark embedding algorithm to provide digital signature at the transmitting end and watermark extraction algorithm is used at receiver end to extract the digital signature. The multi resolution DWT is used to transform the watermarked embedded image and input image for compression. The multi resolution DWT also provides simplicity in embedding and extracting digital water marking. Author presented PSNR more than 50dB with security of data from different attacks. In 2019 P. Ramasamy et al.[18] have proposed an enhanced logistic map (ELM), a different form of chaotic map with state of the art encryption techniques. Authors have shown the encryption efficiency through histogram analysis, differential analysis and statistical

analysis. In 2020 Anand et al. [19] have proposed an improved watermark technique to protect medical images from unethical attacks during transmission. In this technique Hamming code is applied to text watermark. The combinations of two types of encryption, chaotic and hyper chaotic, and three types of compression techniques, Huffman, LZW and Hybrid, are analysed in terms of PSNR, compression ratio, SSIM, NPCR and UACI. In 2020 Guodeng Ye et al. [20] proposed an encryption algorithm based on compressive sensing and information hiding technology. After applying DWT to plain image, confusion sequence using logistic tent map is applied for encryption. Authors have validated the results through key space analysis, Histograms analysis. The quality of reconstructed images are analysed based on PSNR values for different test images.

From the literature review it is observed compression prior to encryption process has tremendous advantages and the performance measurement of CE algorithms must be analysed. The proposed techniques must be capable to reproduce the original image after decryption-decompression process for faithful reproduction of original image and secure transmission, compression and encryption performance parameters must attain their threshold values.

3. Fundamental knowledge and proposed algorithms

3.1. Image Transformation

With the fast advancement of remote detection development, a great deal of image data can be put on viably which causes massive load on limited structures and frameworks. Thus, image compression strategies are right now critical for image storing and correspondence. Since the lossy compression method can make much higher compression ratios than the lossless ones, various lossy compression methodologies like, discrete cosine change (DCT), pyramid coding, vector quantization, and fractal coding, discrete wavelet transform (DWT) etc., have been developed.

Since in JPEG compression methods, large number of bits is assigned to low frequency data and few numbers of bits remains to represent the high frequency data [21]. This mismatch in assigning the bits to low frequency and high frequency data tends to increase in blocking artifacts. This shortcoming of JPEG compression methods can be overcome by using discrete wavelet transform [11].

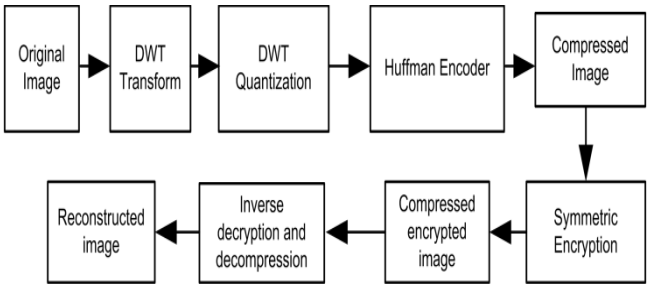


Figure 1. Block diagram of proposed architecture

In discrete wavelet transform, the wavelets are sampled to transform them in discrete form. In this paper, Biorthogonal DWT based compression algorithm is proposed to receive the discrete signal in less redundant form.

3.2 Proposed Biorthogonal DWT compression algorithm

The proposed technique of DWT based compression method decomposes the original image into coefficients called sub bands using biorthogonal 4.4 with 5^{th} level of decomposition and resulting coefficients are compared with a threshold value.

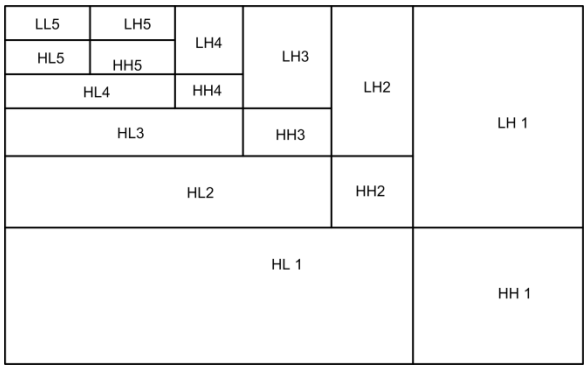


Figure 2. Wavelet filter decomposition

DWT 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. The following steps are used for compression of original image.

Step 1: Original image is loaded into workspace of MATLAB and if original image is colored then it is converted into gray scale using

Rgb2gray(orig_I)

Step 2: Biorthogonal wavelet filter "bior 4.4" is used to decompose the original image into subbands. In the proposed methodology, 5 level of decomposition is applied using command

[c,s]=wavedec2(Orig_I,5,Lo_D,Hi_D)

Step 3: Computation of four low pass and high pass decomposition levels are achieved using command

[Lo_D,Hi_D,Lo_R,Hi_R] = wfilters('bior4.4')

Step 4: A Threshold level is selected for quantization of sub bands using

Floor(.4 * OrigSize 2)

The coefficients which are below than threshold level are marked at 0 level and the coefficients above the threshold level are encoded using Huffman encoder.

Step 5*:* Calculate SSIM, Compression Ratio, PSNR and MSE for compressed image.

Step 6: Compressed image is encrypted using AES or DES encryption techniques.

3.3 AES based proposed algorithm for encryption

AES encryption algorithm is used to provide security to transmitted information. AES is based on the block cipher and works on blocks which are having group of bits of fixed length [14]. In AES algorithm, the first input is of 128 bits block and second input is 128 bit key.

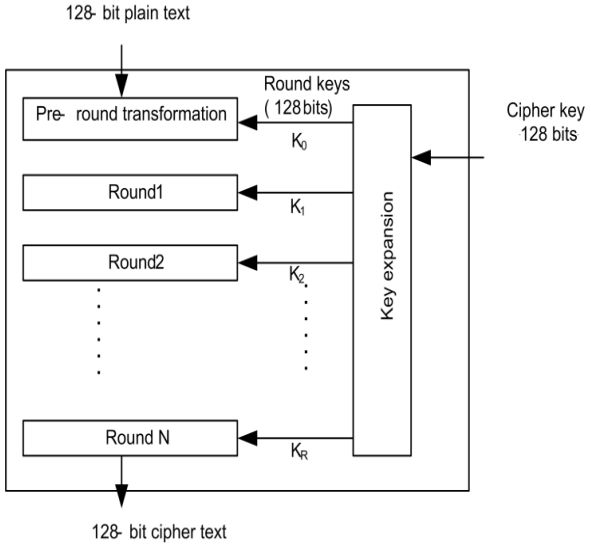


Figure 3. AES algorithm architecture for key size of 128 bits

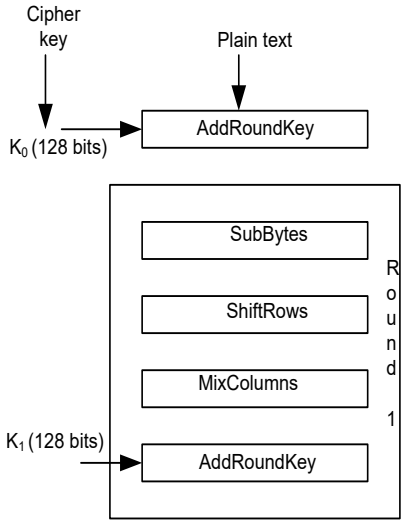


Figure 4. Every round steps in AES encryption algorithm

For encryption and decryption of an image data, AES encryption technology uses a round function. In our scheme total no. of rounds are 14.

Step 1: 16 byte key is expanded using
temp=SubBytes(circshift(temp,-1));
temp=bitxor(temp,[2^(i/8-1),0,0,0]');
Step 2: One time initialization of 128 bit block is done using:
state=AddRoundKey(state,w(:,1:4));
state(:,k)=bitxor(state(:,k),w(:,k));
Step 3: By using state=Sbox(state+1);
S-box (substitution table), bytes are substituted.
Step 4: By using various offsets, the rows of state array are shifted.
state(2,:)=circshift(state(2,:),-1);
Step 5: Data of each column in state array are mixed. Using command
State(a)=bitxor(bitxor(bitxor(xtime(state(a),14),xtime(state (a+1),11)),xtime(state(a+2),13)),xtime(state(a+3),9));
Step 6: Round key to the state is added using
state=AddRoundKey(state,w(:,4*(k-1)+1:4*k));
Step 7: step 3 to step 6 are repeated 14 times.

Increase in key length provides better security but it also increases the execution time.

3.4 DES based proposed algorithm for encryption

The Data Encryption Standard (DES) is an encryption algorithm to provide security to the information during its transmission. In DES encryption algorithm plain text bits are divided in group of 64 bits called as one block and each block of 64 bits is encrypt by a key of length 56 bits [22]. Initial key having 64 bits but every 8^{th} bit of the key is discarded before the DES process begins. So, 8,16,24,32,40,48,56 and 64 bit positions are discarded and key length becomes 56 bits. Input binary data is divided into blocks of size 64 bits that is encrypted by using key of length 56 bits. DES encryption methodology is based on two fundamental steps: Confusion (substitution) and diffusion (transposition). In Data encryption standard algorithm, 16 identical rounds are performed and each round consists following operations:

Table 1. Compression permutation of 64 bit key

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Table 2. Initial permutation on 64 bit plain text

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	33	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Step 1: In key Schedule process 56 bit key is generated from 64 bit key using compression permutation. Compression permutation is done according to Table 1.
Generate different 48 bit key from 56 bit key during each round makes DES highly secure.

```
[k28(m+1:end),k28(1:m)];
lHKey = KeyS(lHKey,RK(i));
rHKey = KeyS(rHKey,RK(i));
k48 = [lHKey ,rHKey];
```

Step 2: Before the first round, initial permutation (IP) is performed on 64 bit plain text in which jugglery of bit positions is carried out as mentioned in Table 2.
Step 3: In second step, IP produces left plain text (LPT) and right plain text (RPT), each of 32 bits.
Step 4: Each LPT and RPT will face 16 rounds of encryption process. In each round, the encryption process has following operations:

- 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.
  mixed_R=KM(expended_R,subKeys(i,:))
- Using S- box substitution 48 bit input is substituted in 32 bits Right plain text.

  subst_R = SBOX(mixed_R);
- 32 bit right plain text data is permuted and then XORed with 32 bit left plaintext.

  permut_R=PBOX(reshape(subst_R',1,32));
  R{i+1} = xor(L{i},permut_R);
- Encrypted LPT and RPT are recombined and final permutation (FP) is performed which produces 64 bits cipher text.

Step 5: Reverse process is applied for decryption. during decryption process subkeys are used in reverse order.

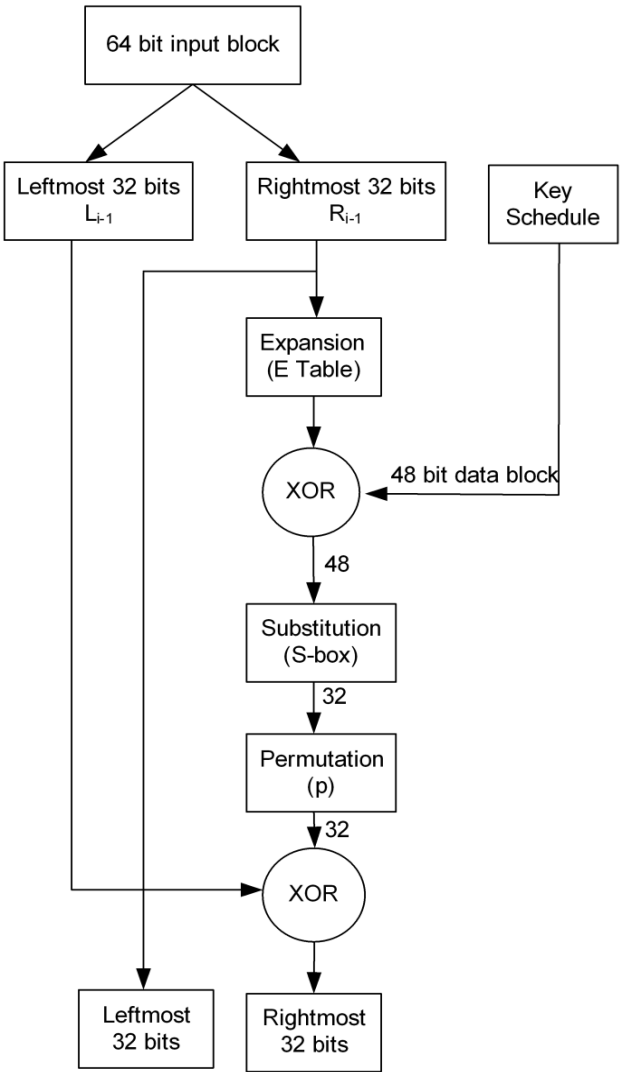


Figure 5. Block diagram representation of DES encryption algorithm

4. Results and performance analysis

Image compression technology reduces the redundancy of data but the efficiency and effectiveness of lossy compression methodology are the major concern because some amount of informative data is discarded by lossy compression methods. PSNR and MSE are the parameters which are used to evaluate the efficiency and effectiveness of compression technology. SSIM is also an important performance evaluation parameter which provides similarity between compressed and original images. The high values of PSNR and SSIM while small value of MSE indicate less destruction in reconstructed image with respect to original image.
During image encryption, pixel values of an image are changed in irregular manner so that there should be no correlation between encrypted image and original image. If the original image and encrypted image are uncorrelated then no feature of the original image can be extracted by unauthorized attacks during transmission of image. Correlation coefficients, entropy, key sensitivity and differential analysis are used to evaluate the performance of an Image encryption algorithm.
In this experimental study, the experiments are performed on two dimensional digital standard images. Five digital test images as Baboon, Boat, Lina, Pepper and Barbara are used to evaluate the performance of CE algorithms. Standard test images are downloaded from SIPI standard data base. All five test images are of .BMP format and gray scale color scheme having size of 512 × 512. To minimize the cost of security, the encryption algorithms are performed after applying the compression algorithms. The performances of CE algorithms are evaluated under three scenarios which are listed below:
Scenario 1: Only compression through proposed DWT based algorithm is applied on test images
Scenario 2: Compression-encryption through Proposed DWT-AES based algorithms is applied on test images
Scenario 3: Compression- encryption through proposed DWT-DES based algorithms is applied on test images.
The five standard grayscale test images Baboon, Boat, Lina, Pepper and Barbara are represented in row 1 of Fig 6. The second row in Fig. 6 is showing the histograms of original input test images. It is observed that histogram of input

images showing sharp rise and sharp falls in pixel distribution at various points of intensity. Row 3 of Fig. 6 is representing the compressed images of corresponding input test images.

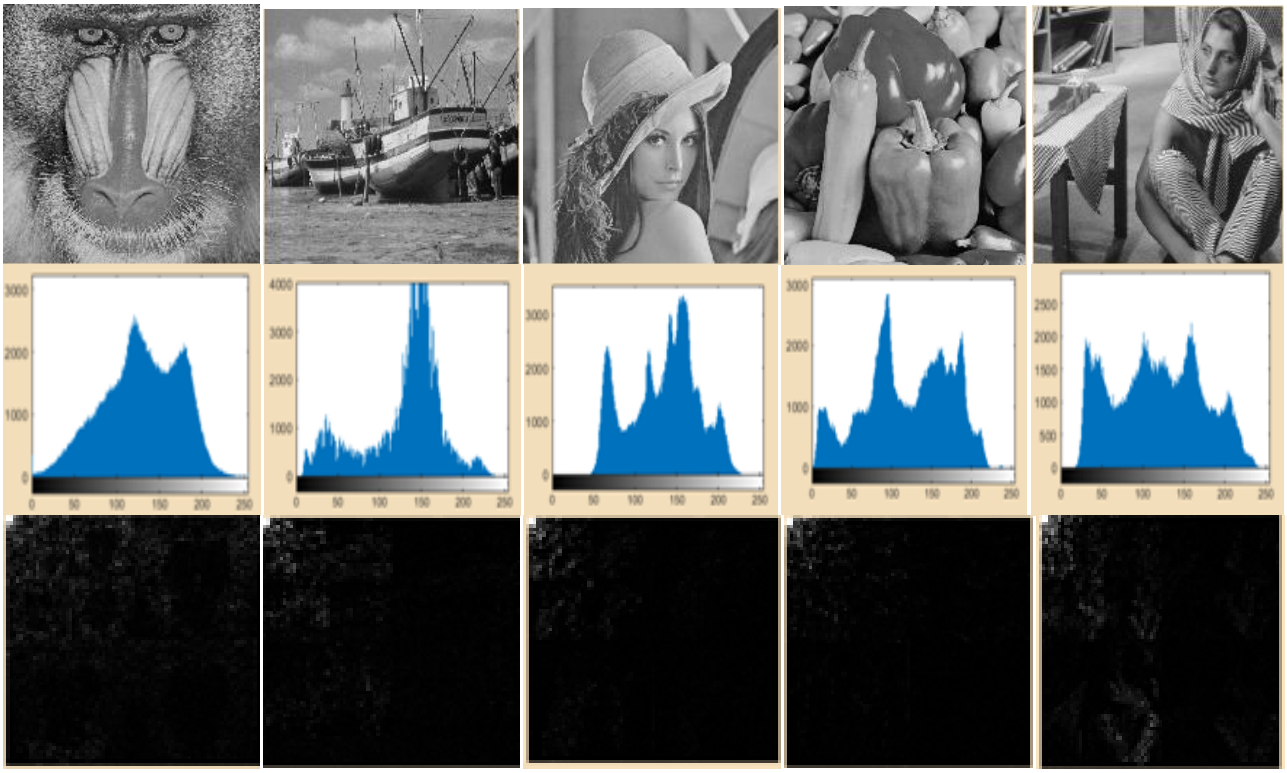


Figure 6. Row 1 original images Baboon, Boat, Lina, Pepper, Barbara (Curtsey SIPI data base), Row 2 Histograms of corresponding original Images, Row 3 Corresponding compressed image using biorthogonal DWT.

4.1 The image compression performance parameters

The quality of reconstructed image from lossy compression algorithm can be access by calculating PSNR and MSE. PSNR is the ratio of square of maximum possible pixel values of an image and mean square error MSE. The quality of reconstructed image will be better if PSNR value lies in the range of 30dB to 50dB or more [23].

$$\text{PSNR} = 10\ log_{10}\ \frac{M\times N\}^2}{MSE} \qquad (1)$$

Here, $M\times N$ represents maximum possible pixel value of image.

Comparison of PSNR values of five test images under above discussed three cases is shown in Table 3. It is observed that the PSNR under compression-encryption schemes is higher than the PSNR under only DWT compression methodology. It can be observed that if encryption is performed after compression of image, then PSNR value of compressed image can be increased. Table 3 also indicates that the combination of DWT-DES compression-encryption algorithm has higher PSNR than DWT-AES combination of cryptanalysis.

The quality of reconstructed image is inversely proportional to MSE i.e. the compressed image quality increases as the MSE decreases [5]. The Mean Square Error can be expressed as,

$$\text{MSE} = \frac{1}{M\times N}\ \sum_{X=1}^{M}\ \sum_{Y=1}^{N}\ [I(x,y) - h\,(x,y)]^2 \qquad (2)$$

Where $I(x,y)$ and $h(x,y)$ represents the original and reconstructed pixel respectively.

The comparison of mean square error (MSE) is represented in Table 4. By analysing the different values of MSE, it can be concluded that if only compression is applied on test images, the MSE occurs in the range of 5-20%, but if this DWT compressed image is encrypted through symmetrical encryption algorithms, the MSE reduces to a great extent. The DWT-AES compression-encryption algorithms has MSE 0.16-0.25% while DWT-DES combination provides MSE in the range of 0.128-0.136%. It can be concluded that DWT-DES combination of CE algorithms gives minimum MSE as desired during transmission of images.

SSIM is a parameter which gives the similarity index of reconstructed image and original image. The SSIM depends on luminance, contrast and structural term. The overall index is a multiplicative combination of the three terms.

$$SSIM(x,y)=[l(x,y)]^{\alpha}.[c(x,y)]^{\beta}.[s(x,y)]^{\gamma} \qquad (3)$$

$$l(x,y) = [2\mu_x\mu_y + c_1]/[\mu_x^2 + \mu_y^2 + c_1] \qquad (3.1)$$

$$c(x,y) = [2\sigma_x\ \sigma_y + c_2]/[\sigma_x + \sigma_y + c_2] \qquad (3.2)$$

$$s(x,y) = [\sigma_{xy} + c_3]/[\sigma_x\sigma_y + c_3] \qquad (3.3)$$

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.

Table 5 showing the comparison of SSIM for different test images under three different scenarios as discussed earlier in this paper.

SSIM for DWT compression algorithm,which showing the similarity index of decomressed image by inverse DWT algorithm and original images, has the values 81.7% to 95.9%. The SSIM of DWT-AES CE algorithms, which shows the similarity index of decrypted-decomressed image and original image, is in the range of 99.78% to 99.95%. SSIM for DWT-DES CE algorithms having range from 99.89% to 99.95%, which is better than DWT-AES combination of cryptanalysis.

Table 3. Comparison of PSNR for different compression encryption techniques

Image File	Our Proposed Methods			Comparative data from other research schemes	
	Only Compression through DWT	CE through DWT-AES	CE through DWT-DES		
Baboon	26.75	54.98	56.90	22.19 (EZW technique) Ref. [24]	22.26 (WDR technique) Ref. [24]
Boat	35.51	54.97	56.88	30.7580 Ref. [25]	X
Lina	40.15	53.77	56.63	30.68 Ref. [26]	22.62 Ref. [27]
Pepper	40.53	53.68	56.36	31.24 Ref. [28]	23.59 Ref. [24]
Barbara	34.83	54.49	56.99	22.92 (EZW technique) Ref.[24]	25.79 (WDR technique) Ref.[24]

Table 4. Comparison of MSE for different Compression encryption techniques

Image File	Our Proposed Methods			Comparative data from other research schemes	
	Only Compression through DWT	CE through DWT-AES	CE through DWT-DES		
Baboon	11.73	0.168	0.132	0.2698 Ref. [18]	0.1711 Ref. [18]
Boat	18.30	0.207	0.133	X	X
Lina	5.56	0.242	0.128	0.883 Ref. [29]	0.2750 Ref. [30]
Pepper	5.14	0.249	0.136	0.2368 Ref. [18]	0.0995 Ref. [18]
Barbara	19.9013	0.215	0.130	X	X

Table 5. Comparison of SSIM for different compression encryption technique

Image File	Methods			Comparative data from other research schemes	
	Only Compression through DWT	CE through DWT-AES	CE through DWT-DES		
Baboon	0.817702	0.999556	0.999557	0.8756 Ref. [25]	0.9288 Ref. [31]
Boat	0.905299	0.998824	0.999201	0.8353 Ref. [25]	0.6949 Ref. [32]
Lina	0.956227	0.997832	0.99893	0.8495 Ref. [25]	0.9239 Ref. [31]
Pepper	0.959776	0.997845	0.998891	0.8215 Ref. [25]	0.9409 Ref. [31]
Barbara	0.9347	0.9987	0.9993	0.9885 Ref. [19]	0.9858 Ref. [19]

4.2 Image encryption performance parameter

Image encryption is an important step before the transmission of image data. Image encryption minimizes the possibility to capture the information by fictitious attacks. The encrypted image should have random pattern of encryption and extraneous from original image. The quality of encryption algorithm can be analyzed with the help of statistical analysis as well as differential analysis.

A. Statistical Analysis:

Statistical analysis has its importance in analyzing the efficiency of encryption algorithms against statistical attacks. The different statistical tests are performed which are explained below:

(i) Histogram analysis

Histogram of an image represent the pixel intensity values means it shows the graphical representation of number of pixels with respect to different intensity values of corresponding image. In this research 8 bit gray scale images are taken as experimental images which have 256 different intensities so the histogram of input images will show the 256 intensities and corresponding pixel distribution. The histogram of input images will have sharp rise and falls and since the encrypted image is coded with

binary bits so histogram of encrypted image will have uniform distribution of pixels over different intensities.

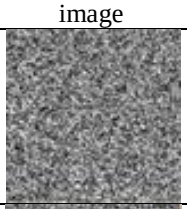
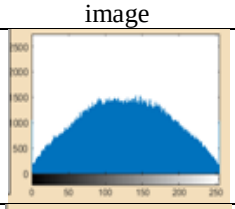
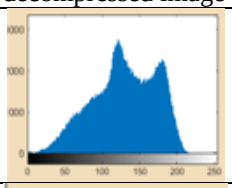
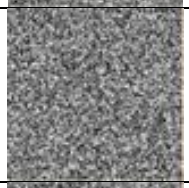
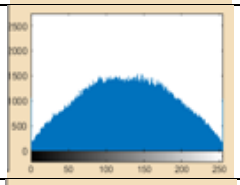
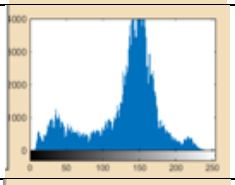
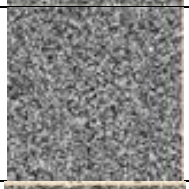
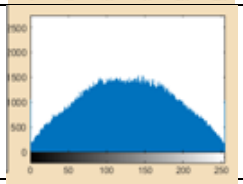
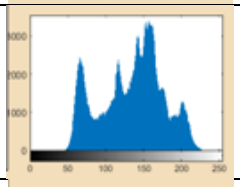
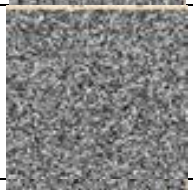
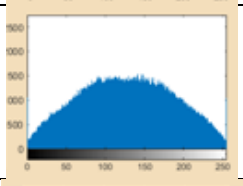
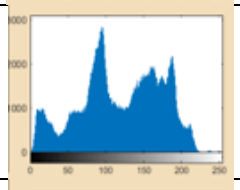
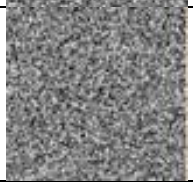
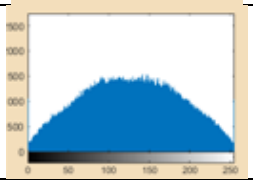
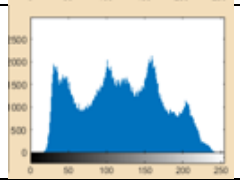
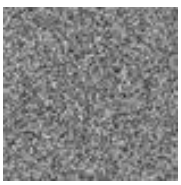
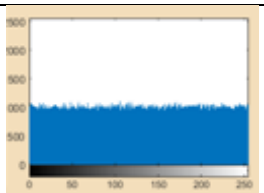
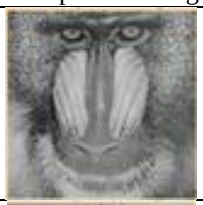
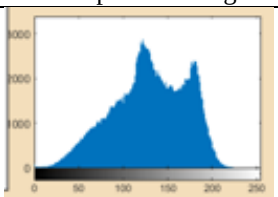
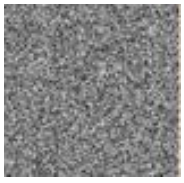
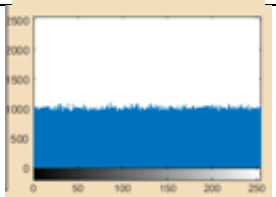
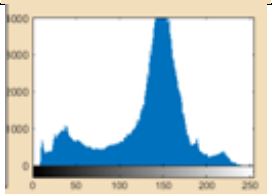
	DWT-AES compression-encryption			
Image title	Compressed-encrypted image	Histogram of CE image	Decrypted-decompressed image	Histogram of decrypted-decompressed image
Baboon				
Boat				
Lina				
Pepper				
Barbara				

Figure 7. Column 2 and column 3 are DWT-AES compressed-encrypted image and its corresponding histograms respectively with respect to images as in column 1; Column 4 and Column 5 are decrypted-decompressed image and its corresponding histograms with respect to images as in column 1.

Fig. 7 and Fig. 8 are showing the pictorial representation of DWT-AES and DWT-DES joint compression-encryption outputs respectively. It can be viewed that these compressed encrypted histogram are having uniform response in comparison with histogram of original input images shown in row 2 of Fig. 6.

The features of decrypted and decompressed image i.e. reconstructed image can not be compared with features of input image using human eyes. So, the histogram of reconstructed image is also represented in column 5 of Fig. 7 and Fig. 8. It can be observed by comparing the histograms of input original test images and reconstructed images, that all 5 input test images are recovered effectively.

	DWT-DES compression-encryption			
Image title	Compressed-encrypted image	Histogram of CE image	Decrypted-decompressed image	Histogram of decrypted-decompressed image
Baboon				
Boat				

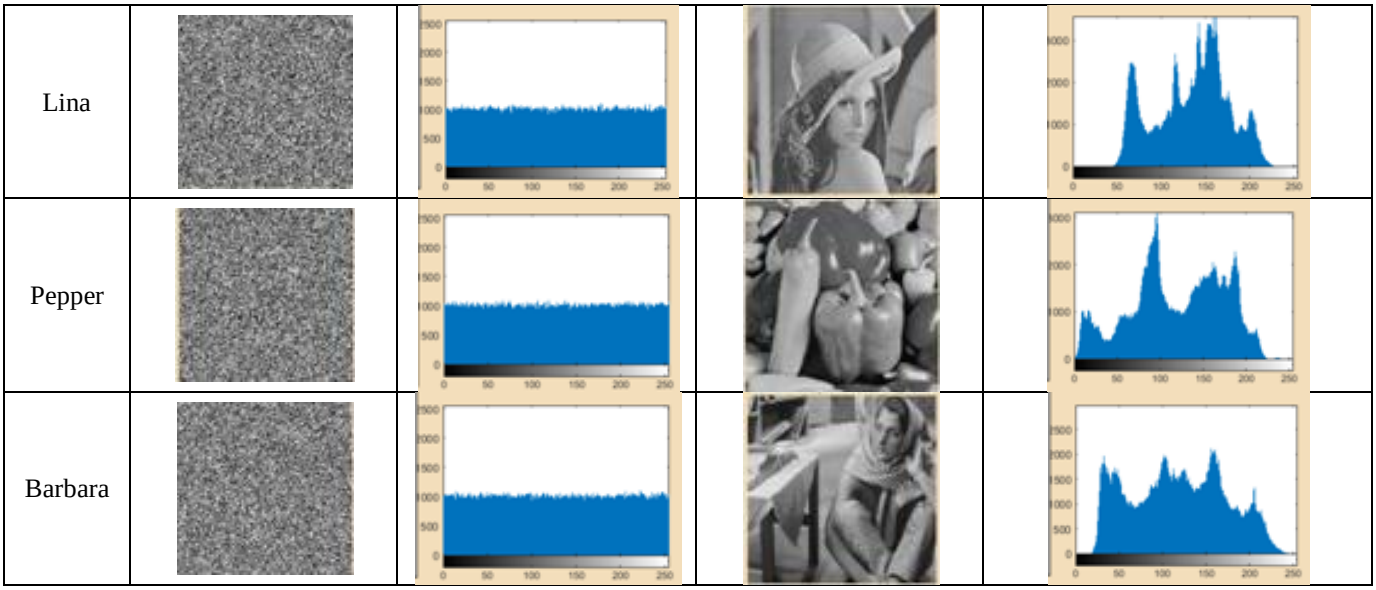


Figure 8. Column 2 and column 3 are DWT-DES compressed-encrypted image and corresponding histograms with respect to images as in column 1; Column 4 and Column 5 are decrypted-decompressed image and its corresponding histograms with respect to images as in column 1

(ii) Correlation of adjacent pixels

The correlation between adjacent pixels can be calculated with the help of correlation analysis. The correlation coefficient is calculated for, two vertically adjacent pixels, two horizontal pixels and two diagonally adjacent pixels in original image and encrypted image. The correlation coefficient is given as:

$$C = \frac{\sum_{i=1}^{N}(x_i-\overline{x})(y_i-\overline{y})}{\sum_{i=1}^{N}(x_i-\overline{x})^2 \times \sqrt{\sum_{i=1}^{N}(y_i-\overline{y})^2}} \quad (4)$$

Where $\overline{x}$ and $\overline{y}$ are the expected values of x and y respectively which can be expressed as

$$\overline{x} = \frac{1}{N}\sum_{i=1}^{N} x_i \text{ and } \overline{y} = \frac{1}{N}\sum_{i=1}^{N} y_i \quad (5)$$

The correlation coefficients of the adjacent pixels of original images in vertical, horizontal and diagonal directions are in the range of 0.726 to 0.9866, which shows that adjacent pixels are strongly correlated with the original image in each direction. On the other side, encrypted images have very low value of correlation coefficient, which shows that adjacent pixels are weakly correlated with encrypted images.

Table 6. Comparison of correlation coefficient for different compression encryption techniques

Image	Our Proposed Methods						Comparative data from other research schemes Ref. [33]		
	Compression-encryption by DWT-AES			Compression-encryption by DWT-DES					
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lina (plain)	.9710	.9847	.9588	.9710	.9847	.9588	.9845	.9766	.9536
Lina(CE)	.00177	.0021	-.0022	.0017	.0018	-.0015	-.0094	.0240	-.0411
Pepper (plain)	.9844	.9866	.9724	.9844	.9866	.9724	.9777	.8839	.7494
Pepper (CE)	.0025	.0021	-.0016	-.00406	.0014	-.0014	-.0225	.0093	-.0251
Baboon (plain)	.8665	.7586	.726	.8665	.7586	.726	.7808	.8839	.7494
Baboon (CE)	-.0018	1.399	-.0023	.0016	.0012	.0013	-.0225	.0093	-.0251
							Comparative data from other research schemes Ref. [13]		
Boat (plain)	.9381	.9713	.9222	.9381	.9713	.9222	.9300	.9420	.8770
Boat (CE)	.0025	.0021	-.0016	-.0025	.0041	-.0058	.010	-.0064	.00007
Barbara (plain)	.8954	.9589	.8830	.8954	.9589	.8830	.8612	.9595	.8468
Barbara (CE)	.0016	.0013	.0014	-.0011	.0050	.0080	.0122	.0079	.0200

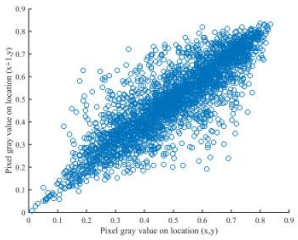
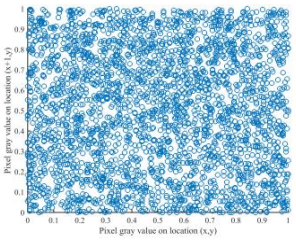
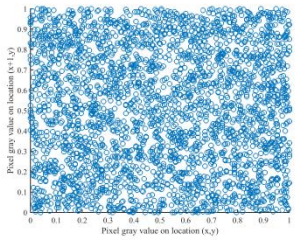
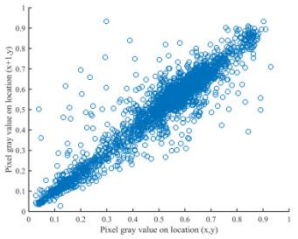
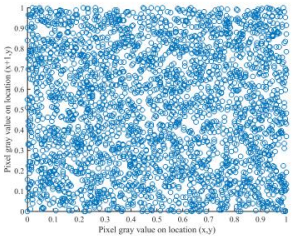
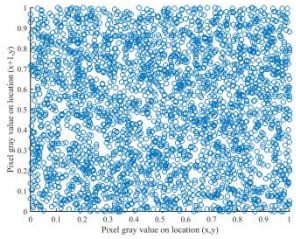
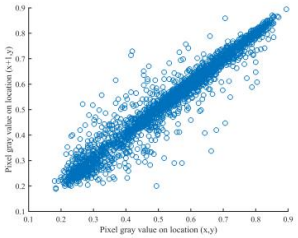
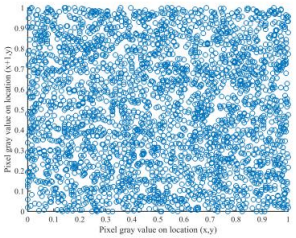
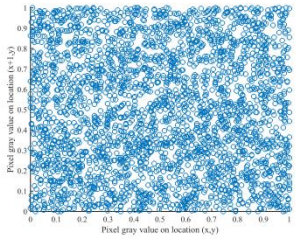
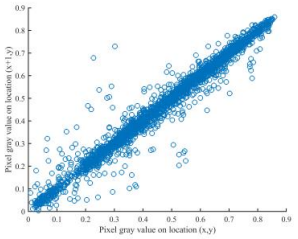
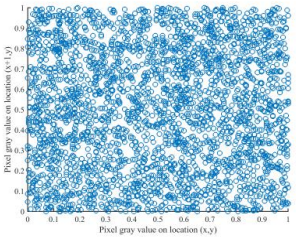
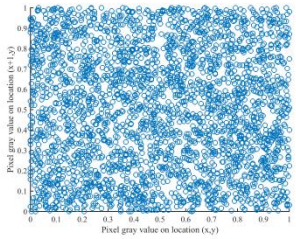
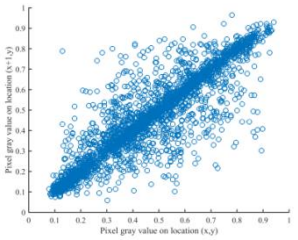
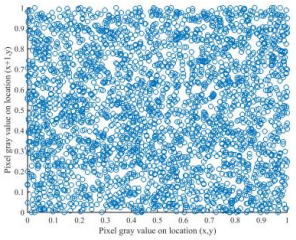
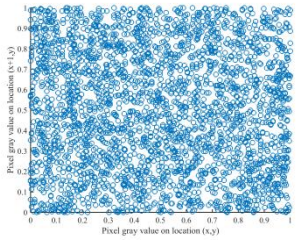
Image	Correlation Distribution of original images	Correlation distribution of DWT-DES encrypted images	Correlation distribution of DWT-AES encrypted images
Baboon			
Boat			
Lina			
Pepper			
Barbara			

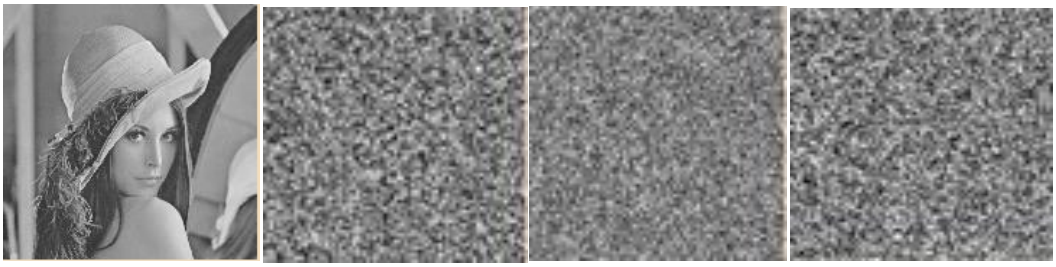
Figure 9. Correlation distributions of two horizontally adjacent pixels for five test images

B. Key sensitive analysis

A cipher key is used to encrypt and decrypt the image data. The encryption algorithm must be highly sensitive to cipher key. The size of the cipher key must be sufficiently large to make unauthorized attacks infeasible.

- The standard test image is encrypt using "9871236540123457" cipher key.
- The same test image is encrypted using slightly modified key "9871236540123456".
- Both encrypted images are analyzed pixel by pixel.

This key sensitive analysis is performed on five test images and both encrypted images are having 99.71% difference with each other. The test results on one test image are shown in Fig. 10.



(a) (b) (c) (d)

Figure 10. (a) Original plain image (b) Encrypted image using correct key (c) Encrypted using slightly different key (d) Decrypted image using slightly different key

C. Entropy analysis

Usually information source transmit long sequences of symbols that's why average information or Entropy is an important parameter.

The mean value or entropy of I(Xi) with m different symbols is given by

$$H(X) = \sum_{i=1}^{m} P(X_i)\, I(X_i) \quad (6)$$

$$H(X) = \sum_{i=1}^{m} P(X_i) \log_2 P(X_i) \quad (7)$$

The entropy H(X) satisfies the following relationship

$$0 \leq H(X) \leq \log_2 m \quad (8)$$

If a source is emitting 256 symbols then entropy of the source will be 8. The entropy analysis is also performed on five test images and results are shown in Table 7.

Table 7. Comparison of entropy analysis for different compression encryption techniques

Image	Our Proposed Methods		Comparative data from other research schemes	
	Compression-encryption by DWT-AES	Compression-encryption by DWT-DES	Ref. [13]	Ref. [18]
Baboon	7.8776	7.9993	7.9987	7.9993
Boat	7.8764	7.9993	7.9989	X
Lina	7.8749	7.9993	7.9989	7.9994
Pepper	7.8744	7.9994	7.9988	7.9992
Barbara	7.8752	7.9993	7.9901	7.9990

D. Differential analysis

The strength of the encryption methodology against external attacks can be analyzed through differential analysis. In differential analysis, the effects of variation in cipher image are observed if the input image is changed by a single bit. The effects on cipher image reflect the linkage between the input image and cipher image. If the variations in cipher image are significant with respect to small changes in original image, then the cipher image is secure from differential attacks.In this paper, Differential analysis is carried out to determine the efficiency of AES and DES encryption algorithms from unauthenticated differential attacks. NPCR and UACI are the two parameters used to find the differential analysis of DWT-DES and DWT-AES compression-encryption algorithms.

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 of NPCR and UACI must be greater than 99% and 33% respectively during transmission [5].

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

$$NPCR\,(C^1, C^2) = \sum_{i,j} \frac{D(i,j)}{M \times N} \times 100\,\% \quad (9)$$

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

$$D(i,j) = \begin{cases} 0, & if\ C^1\ i,j\ = C^2(i,j) \\ 1, & if\ C^1(i,j) \neq C^2(i,j) \end{cases} \quad (10)$$

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

$$UACI\,(C^1, C^2) = \sum_{i,j} \frac{C^1(i,j) - C^2(i,j}{M \times N} \times 100\% \quad (11)$$

Table 8 and Table 9 are showing the comparison of NPCR and UACI respectively under DWT-DES and DWT-AES combination of cryptanalysis. 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 DWT-DES compression-encryption algorithms are higher than the DWT-AES compression-encryption algorithms.

Table 8. Comparison of NPCR for different encryption techniques

DWT Compressed Image File	Our Proposed Methods		Comparative data from other research schemes	
	Encryption by DWT-AES	Encryption by DWT-DES		
Baboon	0.995991	0.99625	0.9960 Ref. [34]	0.9961 Ref. [33]
Boat	0.9952	0.996143	0.9960 Ref. [34]	X
Lina	0.99527	0.996082	0.9960 Ref. [34]	0.9960 Ref [33]
Pepper	0.99527	0.996021	0.9961 Ref. [34]	0.99608 Ref. [33]
Barbara	0.9953	0.9961	0.9960 Ref. [18]	0.9961 Ref. [19]

Table 9. Comparison of UACI for different encryption techniques

DWT Compressed Image File	Our Proposed Methods		Comparative data from other research schemes	
	Encryption by DWT-AES	Encryption by DWT-DES		
Baboon	0.33464	0.33466	0.33442 Ref. [34]	0.33464 Ref. [33]
Boat	0.33466	0.33467	0.33452 Ref. [34]	X
Lina	0.33468	0.33469	0.33456 Ref. [34]	0.33467 Ref. [33]
Pepper	0.33465	0.33467	0.33468 Ref. [34]	0.33468 Ref. [33]
Barbara	0.33467	0.33468	0.33569 Ref. [18]	0.2957 Ref. [19]

4.3 Computational Time

Time taken to execute the proposed compression encryption algorithm during compression encryption and decryption decompression process is shown in Table 10. Results are compared with other existing algorithm schemes. Results are simulated over 5 test images and 1000 rounds are taken to calculate the average execution time. A system having i-7 processor, window 10 as operating system, 8GB RAM, and MATLAB 2018 is used for simulation purpose.

Table 10. Comparison of Computation time for different encryption techniques

Image file	Computation time during compression–encryption(in seconds)		Computation time during decompression –decryption(in seconds)		Comparative data from other research scheme	
	DWT AES	DWT DES	DWT AES	DWT DES		
Baboon	11.9607	6.9170	10.8022	4.9543	X	X
Boat	10.5823	4.5240	09.7604	3.3587	X	X
Lina	10.0745	4.1556	09.3332	2.9110	7.3942 Ref. [35]	7.4436 Ref. [20]
Pepper	10.4793	3.7918	10.3832	2.6490	7.3906 Ref. [35]	7.4520 Ref. [20]
Barbara	11.0562	4.7026	10.0167	3.6054	X	X

5. Conclusion and future scope

From the results it is concluded that the PSNR of lossy compressed image approaches more than 50dB if it is followed by AES or DES symmetric encryption algorithms but the DWT-DES combination of CE algorithm provides better PSNR than DWT-AES CE combination. The MSE of compressed image is also reduces up to a level of 0.12 if symmetrical encryption algorithms applied on compressed images. By analysing the MSE results it is concluded that DWT-DES combination is having least values of MSE for all test images in comparison with DWT-AES CE methodology. SSIM of processed image versus original image is also improves significantly if encryption is performed after compression on image data. SSIM during DWT-DES CE algorithm provides 99.95% similarity index. From both the combinations of compression-encryption methodology, the value of NPCR and UACI is larger than 99% and 33% respectively but DWT-DES combination provides higher NPCR and UACI in comparison with DWT-AES combination. The encryption efficiency of proposed algorithm is represented by performing Key sensitive analysis, entropy analysis and correlation coefficient

analysis and found that proposed algorithm shows robustness against different attacks. It has been authenticated that the DWT-DES combination of compression-encryption algorithms capable of removing redundancy in image data effectively and also provides better security during transmission. The proposed work can be further extended by apply on colour images of different pixel sizes. Researchers can also implement and analyse the proposed work over a system where encryption performed before compression.

References

[1] 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.

[2] M. Xu, "A new chaos-based image encryption algorithm," *Int. Arab J. Inf. Technol.*, vol. 15, no. 3, pp. 493–498, May 2018.

[3] 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.

[4] Q. Guan, "Research of image compression based on embedded zero-tree wavelet transform," in *2011 International Conference on Computer Science and Service System, CSSS 2011 - Proceedings*, 2011, pp. 591–595.

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

[6] S. S. Maniccam and N. G. Bourbakis, "Lossless image compression and encryption using SCAN," vol. 34, pp. 1229–1245, 2001.

[7] X. Zhang, "Lossy Compression and Iterative Reconstruction for," vol. 6, no. 1, pp. 53–58, 2011.

[8] A. Boucetta and K. E. Melkemi, "DWT based-approach for color image compression using genetic algorithm," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2012, vol. 7340 LNCS, pp. 476–484.

[9] T. M. P. Rajkumar and M. V. Latte, "Performance evolution of various wavelet families in SPIHT Image compression technique," *Eur. J. Sci. Res.*, vol. 59, no. 1, pp. 14–21, 2011.

[10] K. Ren and H. Li, "Large capacity digital audio watermarking algorithm based on DWT and DCT," in *Proceedings 2011 International Conference on Mechatronic Science, Electric Engineering and Computer, MEC 2011*, 2011.

[11] C. L. Hsu, Y. S. Huang, M. Da Chang, and H. Y. Huang, "Design of an error-tolerance scheme for discrete wavelet transform in JPEG 2000 encoder," *IEEE Trans. Comput.*, vol. 60, no. 5, pp. 628–638, 2011.

[12] C. Wang, J. Ni, and Q. Huang, "A new encryption-then-compression algorithm using the rate-distortion optimization," *Signal Process. Image Commun.*, vol. 39, pp. 141–150, 2015.

[13] X. J. Tong, P. Chen, and M. Zhang, "A joint image lossless compression and encryption method based on chaotic map," *Multimed. Tools Appl.*, vol. 76, no. 12, pp. 13995–14020, 2017.

[14] S. S. Gonge, V. M. Thakare, A. A. Ghatol, and S. A. Ladhake, "Combined DWT image watermarking and AES technique for digital 2-D image," in *2016 International Conference on Recent Advances and Innovations in Engineering, ICRAIE 2016*, 2017.

[15] J. Ahmad, M. A. Khan, S. O. Hwang, and J. S. Khan, "A compression sensing and noise-tolerant image encryption scheme based on chaotic maps and orthogonal matrices," *Neural Comput. Appl.*, vol. 28, pp. 953–967, Dec. 2017.

[16] M. Kumar and A. Vaish, "An efficient encryption-then-compression technique for encrypted images using SVD," *Digit. Signal Process. A Rev. J.*, vol. 60, pp. 81–89, Jan. 2017.

[17] S. P. Ambadekar, J. Jain, and J. Khanapuri, "Digital image watermarking through encryption and DWT for copyright protection," in *Advances in Intelligent Systems and Computing*, 2019, vol. 727, pp. 187–195.

[18] P. Ramasamy, V. Ranganathan, S. Kadry, R. Damaševičius, and T. Blažauskas, "An image encryption scheme based on block scrambling, modified zigzag transformation and key generation using Enhanced Logistic-Tent Map," *Entropy*, vol. 21, no. 7, 2019.

[19] A. Anand and A. K. Singh, "An improved DWT-SVD domain watermarking for medical information security," *Comput. Commun.*, vol. 152, no. November 2019, pp. 72–80, 2020.

[20] G. Ye, C. Pan, Y. Dong, Y. Shi, and X. Huang, "Image encryption and hiding algorithm based on compressive sensing and random numbers insertion," *Signal Processing*, vol. 172, p. 107563, 2020.

[21] O. Watanabe, A. Uchida, T. Fukuhara, and H. Kiya, "An Encryption-then-Compression system for JPEG 2000 standard," in *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings*, 2015.

[22] H. Agrawal, D. Kalot, A. Jain, and N. Kahtri, "Image encryption using various transforms-a brief comparative analysis," in *2014 Annual International Conference on Emerging Research Areas: Magnetics, Machines and Drives, AICERA/iCMMD 2014 - Proceedings*, 2014.

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

[24] 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.

[25] 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.

[26] 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.

[27] 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.

[28] 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.

[29] K. Gupta and S. Silakari, "Novel Approach for fast Compressed Hybrid color image Cryptosystem," *Adv. Eng. Softw.*, vol. 49, no. 1, pp. 29–42, 2012.

[30] R. K. Singh, B. Kumar, D. K. Shaw, and D. A. Khan, "Level by level image compression-encryption algorithm based on

quantum chaos map," *Journal of King Saud University - Computer and Information Sciences*, 2018.

[31] 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.

[32] 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.

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

[34] 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.

[35] R. Thanki, S. Borra, V. Dwivedi, and K. Borisagar, "A steganographic approach for secure communication of medical images based on the DCT-SVD and the compressed sensing (CS) theory," *Imaging Sci. J.*, vol. 65, no. 8, pp. 458–468, 2017.