TELKOMNIKA Telecommunication, Computing, Electronics and Control
Vol. 18, No. 1, February 2020, pp. 511~518
ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018
DOI: 10.12928/TELKOMNIKA.v18i1.13092

Optimization of image compression and ciphering based on EZW techniques

Majid S. Naghmash, Nazar J. Alhyani, Ali M. Kadhim
Iraqi Ministry of Higher Education and Scientific Research, Computer Engineering Techniques Department, Dijlah University College, Iraq

Article Info

Article history:

Received May 10, 2019
Revised July 2, 2019
Accepted July 18, 2019

Keywords:

DCT
Embedded zero tree of wavelet
LFST
Vector quantization

ABSTRACT

This paper presents the design and optimization of image compression and ciphering depend on optimized embedded zero tree of wavelet (EZW) techniques. Nowadays, the compression and ciphering of image have become particularly important in a protected image storage and communication. The challenge is put in application for both compression and encryption where the parameters of images such as quality and size are critical in secure image transmission. A new technique for secure image storage and transmission is proposed in this work. The compression is achieved by remodel the EZW scheme combine with discrete cosine transform (DCT). Encrypted the XOR ten bits by initial threshold of EZW with random bits produced from linear-feedback shift register (LFSR). The obtained result shows that the suggested techniques provide acceptable compression ratio, reduced the computational time for both compression and encryption, immunity against the statistical and the frequency attacks.

Corresponding Author:

Majid S. Naghmash,
Iraqi Ministry of Higher Education and Scientific Research, Computer Engineering Techniques Department,
Dijlah University College,
Baghdad 00964, Iraq.
Email: majid.salal@duc.edu.iq

1. INTRODUCTION

Numerous technological transformation in the communication system has been presented in last decade involved each growing internet and explosive improvements ever rapidly increasing of video transmission [1]. One of the most technologies used of every aspect in multimedia is the data compression [2]. Without these techniques, the cellular phones could not able to provide efficient communication with secure path [3]. Large image files distribution remains a vital task within any communication systems and the data compression is still an important component of available solution for image creating [4].

In recent years, the compression and encryption of image become marketable with the development of multimedia. The image conveyance over communication path is susceptible to spying. Consequently, the transmit image requires dependable, rapidly and safe scheme during establishing and spreading the image [5]. Generally, the image contents are large and will make their transmission through restricted capacity channels is challenging. Therefore, the image compression should be considerable prior storage or transmitted any image. Image compression depends on take out redundancies at image data. During the image data transmission, the image data exposed to spy on. Consequently, to keep the safety of image information from unlicensed entrée by encrypted image data become a major task in data transmission.

The image encryption processing is used a technique to preserve security image. Normally, the image contents are larger size and the traditional code such as DES, AES, RAS, etc. are not suitable real time request [6, 7]. This work introduces efficient approach for both ciphering and image compression depends on modified EZW and DCT. The offered algorithm is use as a basis to find the significant parts acquired by the compression technique and only these parts are encrypting.

2. RELATED WORK

In general, the standardized image and video move compression such as Motion Picture Experts Group and Joint Photographic Experts Group are based on DCT transform, which transforms the image contents from spatial domain to another domain (frequency domain) [8]. The image is subdivided into blocks and each block is DCT transforms, quantization, the insignificant coefficients are converting to zero. Finally, Huffman encoding and RLE are applying to every block. The improvement of coding rate with embedded DCT has been approved within 30% evaluated with JPEG coder by [9] and 5% in mathematics coder in case of looking at was changed by look at layer. The embedded zero tree wavelet (EZW) is wavelet transforms the input image to several image transformation schemes. To increase the compression efficiency, the Huffman encoder is applied on the data out putted from EZW. On other hand, this method causes increasing in the computational processing time [10].

The effect of chosen threshold value on quality, compression ratio and processing time is examined by Shingate and Sontakke [11]. Said and Pearlman shows that the quality and compression ratio of image has been improved by applied set partitioning in hierarchical trees (SPIHT) [12]. Jun and Wells suggested a new approach to encode the place of wavelet coefficients. This approach called wavelet difference reduction (WDR) [13]. For image compression ratio based on quantization strategy [14] has been proposed for enhance compression ratio. The proposal suggested reorganized the DCT coefficients in a hierarchical sub-band structure form, and generate compressed bit based on zero tree coding algorithms. The results obtained show that the approach strategy surpasses the JPEG and EZW in term of compression ratio. The image compression base on joint DCT and DWT has been proposed in [15-17].

In 2010, Shrestha and Wahid proposed an image compression scheme depends on combine DWT and DCT transforms. The scheme beginning by applied DWT to image block, and throw away/out the coefficients of high frequencies sub band and then the DCT applied on low frequencies of DWT blocks, in decoding, zeros values are applied in places of high frequencies sub band coefficients of DWT. Consequently, there is decay in image quality compared with original image. In [18], Singh and Kumar has been proposed image compression base on joint DCT and DWT. The approach beginning by applying. The DCT on elevated frequency sub-bands of stage 5 DWT of the image decomposition. There are various algorithms have been applied for video and image encryption to keep the contents of them. A joint compression and encryption for image and video has been demonstrated by [19]. The encryption algorithm utilized the piece-wise linear disordered charts and arithmetic coding for both compression and encryption. In [20], Horan and David suggested a nonlinear stream cipher of 5 LFSRs. For image encryption, BEL and RED suggested a LFSR to product 607 bit from resilient function and nonlinear function [21, 22]. For image encryption, SRINIVAS and CA have been proposed a cypher based on utilizing random pixel permutation. Moreover, for video compression and encryption, a demonstration scheme used a vector quantization and combine DCT and DWT in many researchers as in [23-34].

3. PROPOSED ALGORITHM

The proposal based on joint DCT and EZW algorithms. The suggestion will improve the compression efficiency and reduce computational cost of EZW. The encryption used selective encryption concepts to reduce time encryption. Therefore, in this proposal we used the initial threshold of the EZW algorithm as the significant part and cyphered by LFSR. The concepts of EZW based on chose initial threshold and comparing with coefficients of DWT decomposition by iterations Morton scan, this processing will effect on compression efficiency and computational times of encoding method. Our suggestion scheme using the DCT combines with EZW to reduce the iterated scanning and improve the compression efficiency. We called this approach improve EZW (IEZW)

3.1. Proposal to improve EZW technique for and encryption image compression

The IEZW compression approach beginning by dividing uncompressed image into blocks size (8x8) pixels. Then DWT, quantization and DCT are applied respectively. The DCT will rearrange the significant coefficients (low frequency) with high value are concentrated in the peak left of block and the elevated incidence with minimum value in the right base of the block that is regrets the progeny.

Accordingly, through EZW indoctrination dispensation the close relative is frequently bigger than offspring. This scheme IEZW will make better the compression ratio and computational time of encoding. Eventually the EZW is applied and for more compression we used lossless compression such as Huffman coding. Generally, there are two kinds of ciphers for image encryption, stream and block cipher. The block cipher is more efficient than steam cipher. On other hand, the stream cipher is effective for image encryption because the simplicity and less computational time. Furthermore, in this proposal we used the selective encryption concepts to reduce the encryption processing. In IEZW compression processing, the coding depends on the initial threshold to produce sequence data of IEZW. Therefore, we encrypted only the initial threshold by ciphering with ten bits outputted from LFSR as shown in Figure 1. The steps of suggested IEZW are illustrated in the following:

a. Subdivision the image into blocks size (8x8) pixels
b. Decompose each block by DWT, DCT and quantize respectively
c. Implement EZW
d. Outputted data of EZW encoding by entropy encoding (Huffman encoding)
e. Every block is ciphered by 10 bits of XOP produced from LFSR as initial threshold
f. The compressed information and ciphering will send to the transmitter.

The block diagram of IEZW is illustrated in Figure 1. The decompression picture is recovered by reversing the compression scheme.

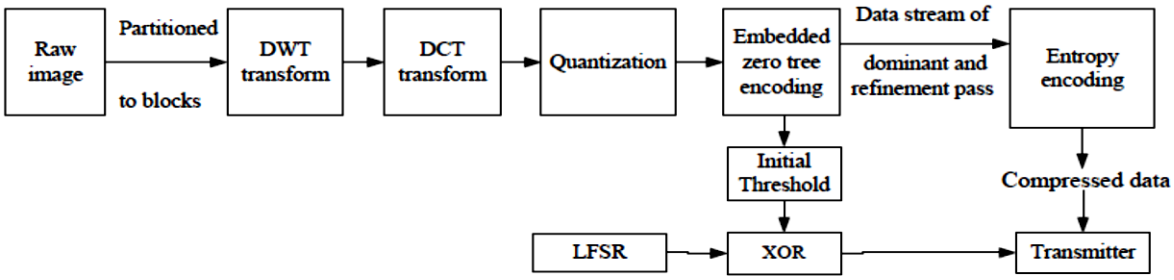

Figure 1. The scheme diagram of proposed IEZW

4. EXPERIMENTAL RESULTS

To assess the performance of our proposal IEZW scheme with original EZW algorithm, we shall compare the performance between them. We used 30 various images have size (258x320) pixels tested by means of quality, ratio of compression and the time of inspired processing. All tested pictures were changed to grey scale as illustrated in Figure 2. For IEZW implementation, the MATLAB environments have been used in this work.

4.1. Compression analysis

Figure 3 illustrate the presentation of IEZW and EZW in term of CR, PSNR and consume time. Generally, it can observe that the quality (represented by PSNR) of IEZW is better than EZW. For example, the archived quality of second image of IEZW is less than in EZW, but the IEZW fulfilled CR better than EZW technique as illustrated in Table 1 and Figure 3. The encoding computational time of IEZW is less than default EZW for all tested images. In general, the results showed that DWT combine with DCT enhance quality, encoding time and compression ratio.

Furthermore, Figures 3 and Figure 4 show the performance of rate distortion and PSNR of all tested images. These figures illustrated that IEZW outperformance EZW in bit rate and PSNR. There was special case in image 28; it has limited texture and relatively smoother background compared with other tested images.

4.2. Encryption analysis

This part contain analyzed and examine the presentation of suggested encryption depend on two analyses: histogram and correlation analysis. The utilization of histogram is analysis to evaluate any statically attack. Figure 5 shows some images chosen from 30 images; the figure illustrates the histograms of the chosen images after encryption and decryption. It can be seen that the histograms of original images are completely different from encrypted images and does not given information used for statistical attack.

4.3. Correlation analysis

Between any two variables, the relationship between then is called a correlation. Accordingly, the association between two adjacent pixels becomes difficult in case of correlation among them approach is

zero and their relation becomes not easy. Therefore, to approximate the correlation among two neighboring pixels, in two directions inside image, we selected randomly 1000 pairs of two pixels vertically and horizontally contiguous from the raw and encrypted image. Then, the correlation between these pairs is calculated based on subsequent (1):

$$C_r = \frac{N\sum_{j=1}^{N}(x_j \times y_j) - \sum_{j=1}^{N} x_j \times \sum_{j=1}^{N} y_j}{\sqrt{(N\sum_{j=1}^{N} x_j{}^2 - (\sum_{j=1}^{N} x_j)^2 \times (N\sum_{j=1}^{N} y_j{}^2 - (\sum_{j=1}^{N} y_j)^2)}} \quad (1)$$

where y and x are the worth of 2 adjoining pixels and N represent the whole numeral of pixels within the picture. From Table 2, It can be seen that the correlation between two adjacent pixels of the raw image equal to one or near to one. On other hand, the correlation of the ciphered image is tending to zero.

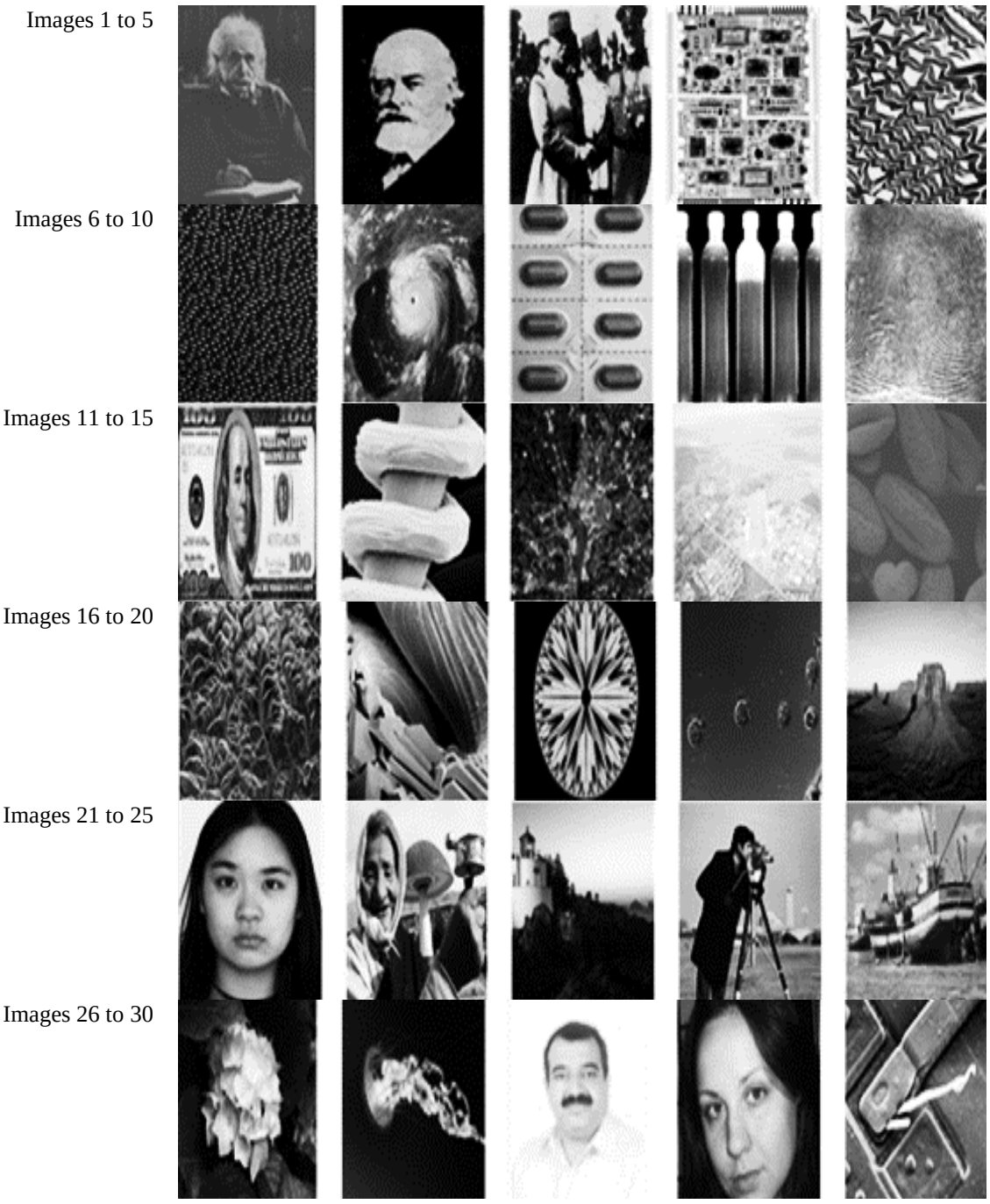

Figure 2. Shows raw test image

Table 1. Information results following programmed by IEZW and EZW

	MEZW method					EZW method				
Image	PSNR/dB	MSE	BPP	CR	Time/Sec	PSNR/dB	MSE	BPP	CR	Time/Sec
1	41.473	4.633	1.190	0.149	26.355	40.256	6.131	2.050	0.256	31.272
2	40.319	6.043	2.780	0.347	25.759	41.678	4.419	3.120	0.390	32.338
3	40.042	6.440	2.290	0.286	27.068	36.881	13.336	4.803	0.600	33.273
4	39.980	6.532	3.219	0.402	28.250	36.793	13.607	6.168	0.771	35.869
5	39.853	6.727	2.871	0.359	27.706	36.249	15.424	6.361	0.795	36.018
6	39.906	6.645	2.185	0.273	26.953	36.133	15.842	6.083	0.760	35.519
7	39.908	6.642	2.524	0.315	26.872	35.761	17.260	4.866	0.608	33.343
8	39.855	6.724	3.187	0.398	27.936	36.860	13.400	4.115	0.514	32.501
9	41.114	5.031	2.257	0.282	26.135	36.719	13.841	3.297	0.412	31.555
10	39.843	6.742	3.159	0.395	27.907	34.261	24.379	7.178	0.897	37.660
11	39.847	6.735	2.586	0.323	27.728	35.172	19.763	7.193	0.899	37.324
12	40.114	6.334	2.599	0.325	27.066	35.268	19.334	4.626	0.578	33.085
13	42.018	4.086	1.725	0.216	25.558	38.364	9.478	4.102	0.513	32.410
14	39.926	6.614	3.654	0.457	28.667	38.372	9.461	5.571	0.696	36.715
15	39.906	6.645	2.895	0.362	25.329	37.340	11.997	2.747	0.343	29.375
16	39.923	6.619	3.209	0.401	28.315	36.231	15.489	6.013	0.752	35.081
17	40.004	6.497	2.743	0.343	27.765	38.632	8.909	3.613	0.452	31.480
18	39.869	6.702	2.185	0.273	27.036	35.876	16.805	6.907	0.863	37.599
19	40.466	5.842	2.946	0.368	27.872	39.688	6.988	3.423	0.428	31.220
20	39.907	6.644	2.472	0.309	27.364	38.002	10.302	4.034	0.504	33.768
21	39.916	6.630	1.943	0.243	26.673	37.852	10.663	3.948	0.493	31.728
22	39.946	6.583	1.367	0.171	26.028	39.894	6.663	3.229	0.404	31.365
23	39.993	6.514	2.182	0.273	26.689	38.433	9.328	3.615	0.452	32.128
24	39.832	6.759	2.725	0.341	27.592	35.767	17.232	4.174	0.522	32.372
25	39.849	6.732	2.978	0.372	28.314	36.883	13.330	4.723	0.590	33.424
26	39.982	6.530	2.212	0.276	26.956	37.925	10.486	3.421	0.428	30.701
27	39.875	6.692	2.889	0.361	27.635	37.717	11.000	4.676	0.585	33.373
28	41.091	5.058	3.902	0.488	28.565	42.517	3.643	3.164	0.396	30.941
29	39.775	6.849	2.214	0.277	26.925	38.212	9.816	3.377	0.422	31.091
30	39.855	6.723	2.844	0.356	26.522	35.382	18.832	4.720	0.590	33.458
Mean	40.146	6.332	2.598	0.325	27.185	37.504	12.572	4.511	0.564	33.266
STD	0.547	0.697	0.605	0.076	0.894	1.920	4.878	1.373	0.172	2.243

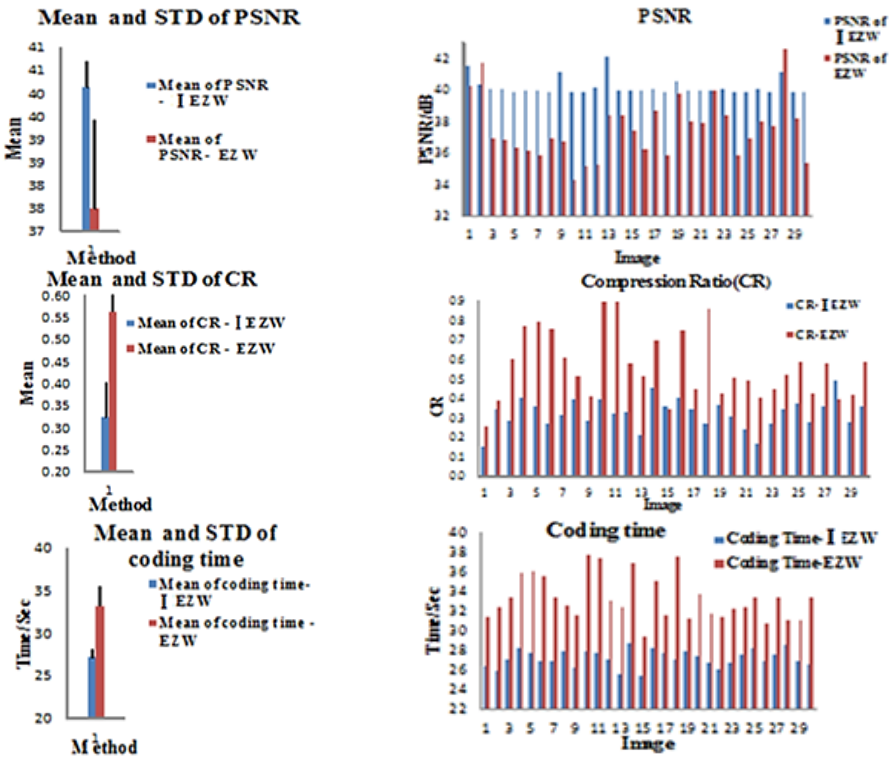

Figure 3. Results comparison between IEZW and EZW

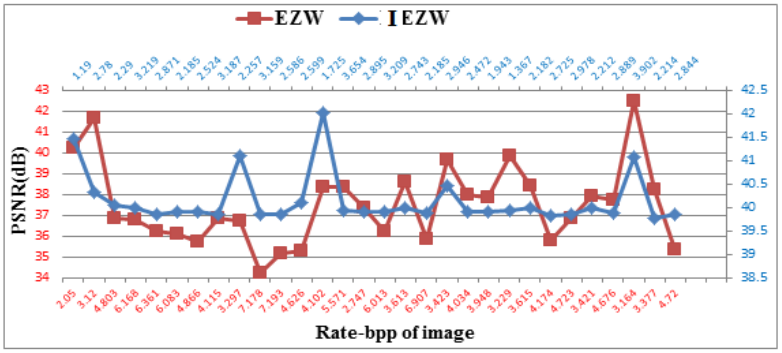

Figure 4. Comparison between rate-distortion curves achieved with IEZW and EZW

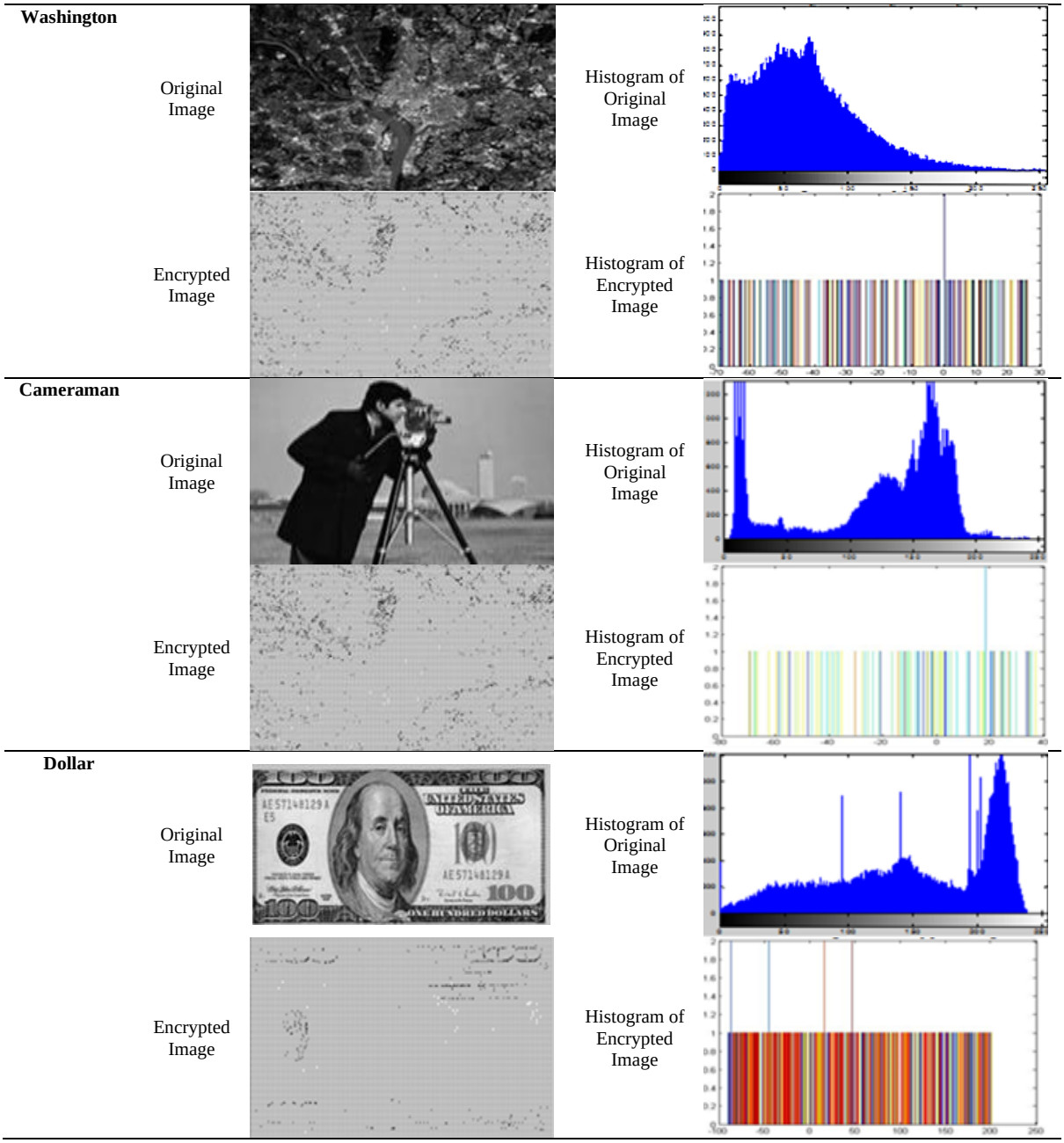

Figure 5. Shows the diffrence between histogram of original and encrypted image

Table 2. The correlation coefficient of original and ciphered image

Image	Original image		Encrypted image	
	Correlation coefficients Horizontal	Correlation coefficients Vertical	Correlation coefficients Horizontal	Correlation coefficients Vertical
Images-1	0.578911	0.9309	-0.00552	-0.0037
Images-2	-1	-1	-0.00242	-0.0026
Images-3	-1	-1	-0.00063	-0.0011
Images-4	-0.9503	-1	-0.00199	-0.0016
Images-5	-1	-1	-0.00122	-0.0015
Images-6	-1	-0.9997	-0.01235	-0.0139
Images-7	0.7646	1	-0.00389	-0.0017
Images-8	-1	-1	-0.00230	-0.0036
Images-9	-1	-1	-0.00602	-0.0011
Images-10	-1	-1	-0.00315	-0.0016
Images-11	-1	-0.9998	-0.00262	-0.0023
Images-12	-1	-1	-0.00283	-0.0027
Images-13	0.800438	0.9826	-0.00663	-0.0022
Images-14	-1	-1	-0.00134	-0.0013
Images-15	-1	-1	-0.00275	-0.0018
Images-16	0.74123	1	-0.00216	-0.0012
Images-17	-1	0.9083	-0.00341	-0.0009
Images-18	-0.99924	-0.9990	-0.00533	-0.0017
Images-19	-0.9990	-1	-0.00266	-0.0009
Images-20	0.6175	0.7398	-0.00334	-0.0011
Images-21	-0.9206	-0.9985	-0.00151	-0.0014
Images-22	-1	-1	-0.00247	-0.0008
Images-23	0.8081	1	-0.00231	-0.0011
Images-24	0.89205	0.6231	-0.00213	-0.0012
Images-25	-1	-1	-0.00209	-0.0011
Images-26	-0.99995	0.9999	-0.00223	-0.0015
Images-27	-1	-0.8775	-0.00267	-0.0013
Images-28	0.6411	0.5487	-0.00359	-0.0012
Images-29	-0.99965	-1.0001	-0.00214	-0.0015
Images-30	0.84279	-1.0000	-0.00096	-0.0018

5. CONCLUSION

This paper introduces combined algorithms of DCT and EZW to improve the image encryption and compression. The repeated numbers of scan loop has been reduced by DCT to improve the EWZ algorithms which will reduce the computational time of compression compared with EWZ algorithms. The encryption algorithms implemented the selective encryption concepts by exploit initial threshold of IEZW as significant part and encrypted by XOR with bits formed by LFSR. Results show that the encryption approach is resistance to the arithmetical and the frequency bothers.

REFERENCES

[1] D. Ravichandran, P. Praveenkumar, J. B. B. Rayappan, and R. Amirtharajan, "Chaos based crossover and mutation for securing DICOM image," *Computers in Biology and Medicine*, vol. 72, pp. 170-184, 2016.
[2] Zhang, M.; Tong, X., "Joint image encryption and compression scheme based on IWT and SPIHT," *Optics and Lasers in Engineering*, vol. 90, pp. 254–274, 2017.
[3] Stoyanov B., Kordov K., "Novel secure pseudo-random number generation scheme based on two tinkerbell maps," *Advanced Studies in Theoretical Physics*, vol. 9, no. 4, pp. 411–421, 2015.
[4] Stoyanov B., Kordov K., "A novel pseudorandom bit generator based on Chirikov standard map filtered with shrinking rule," *Mathematical Problem in Engineering*, vol. 2014, pp. 1-4, 2014.
[5] C. Wu and C. Kuo, "Design of integrated multimedia compression and encryption systems," *IEEE Transactions on Multimedia*, vol. 7, no. 5, pp. 828-839, 2005.
[6] A. Uhl, A. Pommer, "Image and video encryption: from digital rights management to secured personal communication, *Springer*, vol. 15, 2005.
[7] S. Li, X. Zheng, X. Mou and Y. Cai, "Chaotic encryption scheme for real-time digital video," Proc. SPIE 4666, Real-Time Imaging VI, 2002, https://doi.org/10.1117/12.458527.
[8] K. Cabeen, P. Gent, "Image compression and the discrete cosine transform," College of Redwoods, Department of Mathematics, The Chinese University of Hong Kong, 1998.
[9] J. Li, J. Li, C. Kuo, "Embedded DCT Still Image Compression," *Signal and Information Display*, 1996.
[10] R. Janaki, A. Tamilarasi and others, "Still Image Compression by Combining EZW Encoding with Huffman Encoder," *International Journal of Computer Applications*, vol. 13, no. 7, pp. 1-7, 2011.
[11] V. Shingate, T. Sontakke and S. Talbar, "Still Image Compression using Embedded Zerotree Wavelet Encoding," *International Journal of Computer Science & Communication*, vol. 1, no. 1, pp. 21-24, 2010.

[12] A. Said, W. Pearlman, "A new, fast, and efficient image codec based on set partitioning in hierarchical trees," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 6, no. 3, pp. 243-250, 1996.
[13] J. Tian, R. W. Jr, "A lossy image codec based on index coding," *Proceedings of Data Compression Conference - DCC '96*, 1996.
[14] D. Monro, G. Dickson, "Zerotree Coding of DCT coefficients," *Proceedings of International Conference on Image Processing*, vol. 2, pp. 625-628, 1997.
[15] S. Shrestha, K. Wahid, "Hybrid DWT-DCT algorithm for biomedical image and video compression applications," *10th International Conference on Information Science, Signal Processing and their Applications (ISSPA 2010)*, 2010.
[16] S. Benchikh, M. Corinthios, "A hybrid image compression technique based on DWT and DCT transforms," *International Conference on Advanced Infocom Technology 2011 (ICAIT 2011)*, 2011.
[17] S. Singh, V. Kumar and H. Verma, "DWT-DCT hybrid scheme for medical image compression," *Journal of Medical Engineering & Technology*, vol. 31, no. 2, pp. 109-122, 2007.
[18] A. Pande, P. Mohapatra and J. Zambreno, "Using chaotic maps for encrypting image and video content," 2011 *IEEE International Symposium on Multimedia*, 2011.
[19] D. Horan, R. Guinee, "A novel stream cipher for cryptographic applications," *MILCOM 2006 - 2006 IEEE Military Communications conference*, 2006.
[20] D. Nadir, R. Mohamed, F. Banhawi, N. M. Ali, H. M. Judi, S. Venkateswari, R. Muthaiah, B. Thamotharan, M. Menaka and others, "An image encryption approach using stream ciphers based on nonlinear filter generator," *Journal of Theoretical and Applied Information Technology*, vol. 41, no. 1, 2012.
[21] G. Sathishkumar, S. Ramachandran and K. B. Bagan, "Image encryption using random pixel permutation by chaotic mapping," *2012 IEEE Symposium on Computers & Informatics (ISCI)*, 2012.
[22] Nasrullah, et al., "Joint Image Compression and Encryption Using IWT with SPIHT, Kd-Tree and Chaotic Maps, *Applied Science*, vol. 8, no. 10, 2018, doi:10.3390/app8101963
[23] Padmavati S, Vaibhar M., "DCT combined with fractal quadtree decomposition and Huffman coding for image compression," *2015 International Conference on Condition Assessment Techniques in Electrical Systems (CATCON)*, pp. 28-33, 2015.
[24] Kamisli F., "Block-based spatial prediction and transforms based on 2D Markov processes for image and video compression," *IEEE Transactions on Image Processing*, vol. 24, no. 4, pp. 1247-1260, 2015.
[25] G. S. Chandel and P. Patel, "Image Encryption with RSA and RGB randomized Histograms," *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, vol. 3, no. 5, pp. 9750-9757, 2014.
[26] R. U. Ginting and R. Y. Dillak, "Digital color image encryption using RC4 stream cipher and chaotic logistic map," *2013 International Conference on Information Technology and Electrical Engineering (ICITEE)*, pp. 101-105, 2013.
[27] W. W. Zhang, et al., "A watermark strategy for quantum images based on quantum fourier transform," *Quantum Information Processing*, vol. 12, pp. 793-803, 2013.
[28] C. Sankara Narayanan and S. Annadurai, "A Critical Study on Encryption Based Compression Techniques," *Journal of Computers*, vol. 11, no. 5, pp. 380-389, 2016.
[29] P. Kumar, P. K. Pateriya, "RC4 Enrichment Algorithm Approach for Selective Image Encryption," *International Journal of Computer Science and Communication Networks*, 2012.
[30] P. Singh and K. Singh, "Image Encryption and Decryption Using Blowfish Algorithm in Matlab," *International Journal of Scientific & Engineering Research*, vol. 4, no. 7, pp. 150-154, 2013.
[31] Y.-G. Yang, et al., "Novel image encryption/decryption based on quantum Fourier transform and double phase encoding," *Quantum information processing*, vol. 12, pp. 3477-3493, 2013.
[32] X. Zhang, et al., "Compression of encrypted images with multi-layer decomposition," *Multimedia Tools and Applications*, vol. 72, pp. 489–502, 2014.
[33] T. Hoang and D. Tran, "Cryptanalysis and security improvement for selective image encryption," *The European Physical Journal Special Topics*, vol. 223, pp. 1635–1646, 2014.
[34] Abdul Jaleel.J and Jisha MaryThomas, "Guarding Images using a Symmetric key Cryptographic Technique: Blowfish Algorithm," *International Journal of Engineering and Innovative Technology (IJEIT)*, vol. 3, no. 2, pp. 196-201, 2013.