International Journal of Engineering & Technology, 7 (3) (2018) 1332-1336

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i3.12707
Research paper

A singular value decomposition based approach for the compression of encrypted images

Hiyam Hatem [1] *, Raed Majeed [2], Jumana Waleed [3]

[1] Department of Computer Science, Collage of Computer Science and Information Technology, University of Sumer, Iraq
[2] Department of Computer Information Technology, Collage of Computer Science and Information Technology, University of Sumer, Iraq
[3] Department of Computer Science, College of Science, University of Diyala, Iraq
**Corresponding author E-mail: h.hatim@uos.edu.iq*

Abstract

Image compression is a process which supplies a good solution to the current problems of data storage by reducing redundancy, and irrelevance within images. This paper provides effective encryption then compression technique applied for compressing images within the entire domain of encryption. The Singular Value Decomposition (SVD) application has been described for the results of compression from an image encrypted based on Discrete wavelet transforms (DWT). Initially, the original image has been decomposed into a pyramid of wavelet by utilizing DWT. The DWT subbands are enciphered via a pseudo random number and pseudo random permutation. Then, encrypted images are compressed evaluated by the SVD method which encompasses the corresponding singular values and singular vectors. The performance evaluated on several images and the experimental results and security evaluation is given to validate the explained goals of high security and good compression performance.

Keywords: *Discrete Wavelet Transform (Dwt); Image Encryption; Singular Value Decomposition (SVD); Image Compression.*

1. Introduction

The minds progression of humans has extremely changed the purpose and techniques of images preserving. Images are important parts and comprise the large volume of data. Nowadays, the process of saving and sharing a large number of images can be done on PCs. An increasing need to store many images causes an unreasonable cost, like the growing images availability. The cost needed for saving images is very necessary for reducing the images size before being sent.

The security of information transmission requires an integrated work of images encryption and compression processes. Encryption is employed for getting a secure indication of information, and the compression is employed for reducing the entire bits numbers needed for the data of an image that gives a faster transmission with reduced cost of storage space [1].

Recently, lots of techniques with the tools of images compression has been utilized for increasing the efficiency and performance. Medical institutions, Federal Government Agencies, astronomy, the industry of entertainment, multimedia, and the education section are among a great group of organizations that work based on images [2].

The conventional manner of protecting and reducing the data is done by firstly applying the data compression, and secondly encrypted it via privet key, as shown in Figure 1 (a). The process of images compression based on transform domains has obtained a massive popularity owing to the property of energy compaction. The integrated compression-encryption techniques accomplish the requirement of different scenarios of the security. Nevertheless, in other techniques, the regular manner needs to revisit as demonstrated in Figure 1 (b).

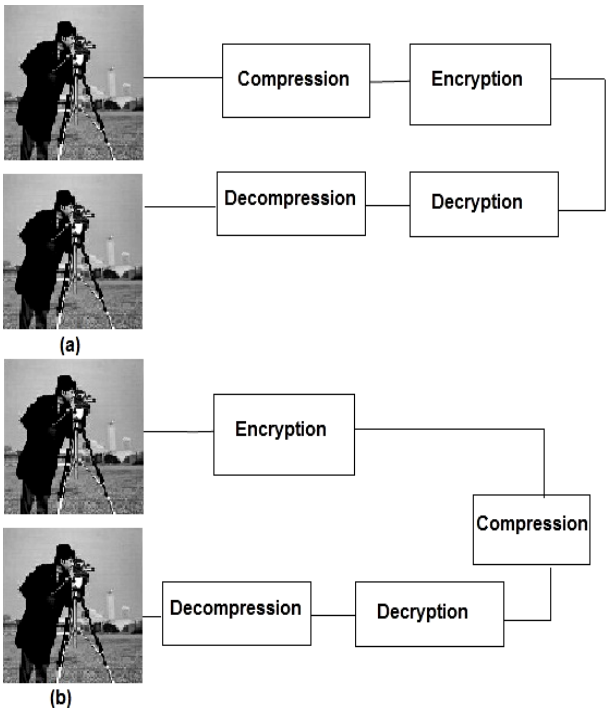


Fig. 1: Illustrates image compression and encryption techniques in (a) and Image encryption and compression techniques in (b).

Recently, the techniques of image compression and encryption have been simultaneously developed. There are several images enciphering and compression techniques that are appeared in the

Copyright © 2018 Hiyam Hatem et. al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

related works. A technique for optical image compressing and encrypting has been proposed by Alfalou and Brosseau [3] in order to provide an efficient and secure image transmission through the Internet. While, the presented technique in work [4], performed the compression and encryption in a simultaneous way. This technique is depending on the characteristics of Discrete Cosine Transformation (DCT). The encryption minimizing the space for storage gives good key syndication and helps to save large storage space. A technique of images encryption is presented in work [5] by incorporating compressive sensing and nonlinear fractional Mellin transform. However, this algorithm does not show better results at higher compression ratios and it compresses the energy in little low-frequency coefficients existing in the top left corner of the transformed image.

The challenge of compacting enciphered images has acquired a great deal of concern, at first sight, the performing of this kind of techniques seems to be unpractical since the secured data are not depending on the source data. Although the work in [6] compromised the data via swapping the order, and the process of compressing the encrypted images may lead to a good performance. [7] Analyzed the process of compressing the encrypted data from memory loss and hidden Markov resources via LDPC. A powerful strategy is proposed by [8]; Enciphering is accomplished by conjecture error clustering and unique permutation, and here the performance of the lossless and lossy compression process is analyzed. Recently, encryption then compression (ETC) technique has been proposed by [9] in which the prediction errors are computed via utilizing a sub-image. And to achieve an efficient compression, a quantization, and Huffman coding are used.

Many works have been reported singular value decomposition (SVD) method [10,11] was chosen as the inspiration of the compression formula in the literature on SVD for natural images compression, however, until now the compressing of enciphered images using SVD is not found, it is very computationally intensive. In the proposed work, we used (SVD) for compression the encrypted image by using the two-dimensional DWT, it demonstrates the images data into set of detail "high pass" and approximate "low pass" coefficients are obtained. Encrypted approximation subband is compressed nearly lossless, the LL subband, the detailed sub-bands (LH, HL, and HH) are enciphered by utilizing a pseudo random number series and pseudo random permutation, that leads the proposed technique to minimize the image size without extra losing of the reconstructed image quality, in addition, secure against any attack. After this, the encrypted images are compressed via a new technique, discussed in subsection 4.2.

The remainder of this paper is prepared as follows: An overview of DWT and SVD is briefly discussed in Section two and three respectively; Section four presents in details the proposed technique of image encryption and compression. In order to give the proof for the gotten results, the results of experiment are stated in section five; Finally, the conclusions for the proposed technique are drawn in the last section.

2. Background of DWT

DWT is utilizing extremely in the various digital image processing applications such as images encryption, images compression etcetera. Wavelet domain utilizes a multi-resolution approach through which various frequencies are analysed with various resolutions [12].

The DWT transform for images is done from the spatial domain to the frequency domain, in which wavelets are discretely sampled. DWT takes several merits over other digital image transformations domains like the image can be represented in multi-resolution form, the division of the image into non overlapping blocks, fulfil a raising compression ratio via avoiding blocking artifacts, better identification of data preferable for human perception, supplies best localization in space and frequency domains [13] [14] [15].

As the result of the DWT decomposition is achieved to decompose the input data into (LL) and (LH, HL, HH) coefficients as shown in Figure 2.

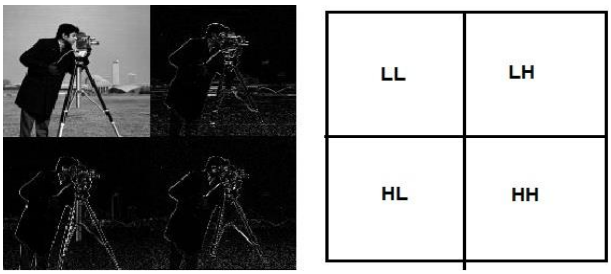


Fig. 2: One Level of DWT Decomposition.

3. Background of SVD

Within the field of digital image processing, the SVD has several distinctive merits, it is a lossy compression technique, which it must keep the maximum number of characteristics of the image and maximize the gain with lower complexity [16].

It achieves compression by using a smaller ranking to approximate the original matrix representing an image [17]. SVD isn't only fixed for the square matrices, but it can also be performed to rectangular matrices. SVD is depending on a theorem of linear algebra in which the rectangular matrix A can be decomposed into U, S, and V matrices in a manner U and V are orthogonal matrices, and S is a diagonal matrix including descending order sorting to the singular values. To the input image with the size (I × j), U and V matrices are with the size (i × i, j × j), respectively, and S matrix is approximate with size (i × j).

$$A_{i\times j} = U_{i\times i}\, S_{ejm}\, (V_{j\times j})^{T} \quad (1)$$

The rank of the given matrix is determined by the no. of non-zero elements on the S matrix. the process of compression is done by minimizing the S rank for approximating the original matrix. In Mathematics, it is demonstrated as in equation (2):

$$S_{i\times j} = \begin{bmatrix} \overline{S}_{c\times d} & 0 \\ 0 & \ddots \end{bmatrix} c \le i, d \le j \quad (2)$$

According to $\overline{S}$, it has a minimal No. of rows & columns regarding S, thus, for making the matrix multiplication potential some of U columns & V rows require to be minimized as follows:

$$U_{i\times i} = [\overline{U}_{i\times c}\, \overline{U}_{i\times(i-c)}] \quad (3)$$

$$V_{j\times j} = [\overline{V}_{j\times d}\, \overline{V}_{j\times(j-d)}] \quad (4)$$

The SVD may be regarded as a technique to change the correlated variables into a set of interrelated variables. Simultaneously, the SVD domain is a technique for identifying and ordering the dimensions depending on the extremely important variation. If these dimensions are recognized, finding the preferable approximation of the original data items is possible for utilizing little dimensions. The technique of SVD supplied for arbitrary matrix results a decomposition which encompasses of related singular values and vectors. This kind of techniques is reversible in which depending on the multiplication operation for the decomposed portions, the original matrix is reconstructed. Nonetheless, the process of compression is dependent on the modifying the decomposition for producing matrix of low rank approximation. The reconstructed matrix a little bit differs from the original matrix, so the process does the lossy compression.

The description for the ratio formula of compression is well done through Figure 3. Mild colour refers to the decomposition part of the matrix which is to be stored in the output file as an input of a low rank estimation.

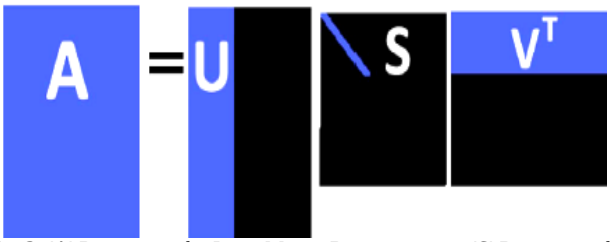


Fig. 3: 'A' Represents the Input-Matrix Decomposition; 'S' Represents the Diagonal Matrix; 'U' and 'V^{T}' Represent the Left & Right Singular Vectors Matrices Respectively. The Lighted Colour Illustrated the Low Rank of Approximation.

4. The proposed technique of encryption & compression

In this section, Figure 4 illustrates the details of the proposed technique 'encryption & compression'.

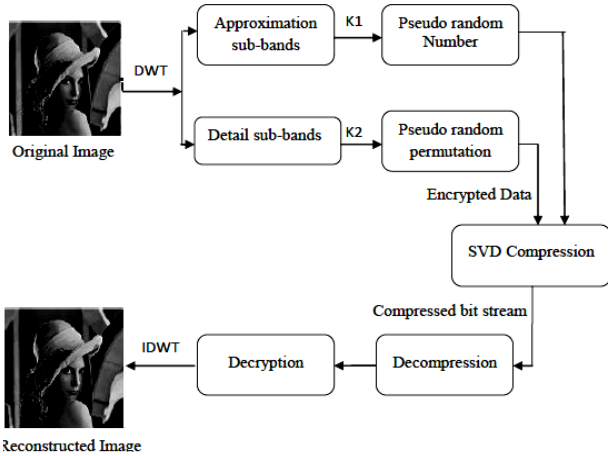


Fig. 4: Proposed Technique of Encryption, Then Compression (ETC).

4.1. Image encryption

As the result of the DWT (LL) and (LH, HL, HH) sub bands are acquired as demonstrated in Figure 2. The LL sub band appears extra similar to original image, so LL sub band coefficients are known as significant. While the (LH, HL, HH) sub bands coefficients are known as minimal significant. The amount of data for the (LH, HL, HH) sub bands should be hard to perform brute force search on these sub bands since it is three times of the LL sub band. Because of the high correlation among the pixels of neighbouring, almost all sub images values are nearly same, that produce to small values of errors, owing to that little portions can be assigned on quantization & coding. Meant for securing an effective transmission for the fused low-frequency coefficients, approximation sub band LL is encrypted by use pseudo-random number generator series PRNG, Mersenne Twister PRNG is utilized for generating pseudo-random numbers. The primary seed is utilized for generating the PRNG which is known as privet key k1 and the permutation for the coefficients is classified as another privet key k2. Suppose the size of LL sub band features is P/2 x Q/2, and the whole No. of LL sub band pixels is N (N=P/2 x Q/2). Firstly, LL sub band coefficients are quantized for reducing the area of coefficients.

$$QWC(i,j) = \left\lfloor \frac{WC(i,j) - WCmin}{WCmax - WCmin} \cdot R \right\rceil, \quad 1 \le i \le P/2, 1 \le j \le Q/2 \tag{5}$$

Where QWC (i, j) is the quantized wavelet coefficients, WC (i, j) refers to the LL sub band coefficient. WCmax & WCmin are the upper and lower coefficients values in the LL sub band, R represents a parameter utilized for bounding the LL sub band values between [0, R], here the R is equal to (28-1) and $\lfloor . \rceil$ is the round process.

Because of this quantization, the LL subband values will appear between [0, 255], therefore, it is appropriate for choosing a quantized of quality resolution "8 bits" to find the perfect reconstructed image quality. Following the stage of quantization, the content of owner creates N pseudo-random numbers that are consistently range between [0, 255] and implement one by one addition modulo 256 to get a secure image.

$$E(i,j) = mod[QWC(i,j) + S(i,j), 256], \quad 1 \le i \le P/2, 1 \le j \le Q/2 \tag{6}$$

Where S (I, j) represents pseudorandom numbers at the location (i, j) and the values encrypted pixel are E (i, j).

After encrypting the LL subband, we encrypt the detailed subbands (LH, HL and HH). Without taking many overhead the content owner just encrypts these sub-bands utilizing the permutation of coefficients. The coefficients permutation is used for hiding the structure of original image from. Lots of permutation methods reported in literary works [18] can be used here to permute the coefficients.

Our technique is proposed to be secure under any incredible force search. The manner of possible permutation for every single of the (LH, HL and HH) sub-bands are "N!" for considerable N values, it is hard to any attacker for performing brute force search.

4.2. The compression for encrypted image

The process of image compression is to encode the image also to decrease the image size, image storage & transmission. Compression distributed as lossy & lossless compressions. In lossless compression scheme image reconstructed without any loss of information, after applying this process, is similar to the original image, some image file formats such as PNG or GIF use only lossless compression. In lossy compression, the approach supplies high compression percentage than lossless compression. In this process, we dot a higher ratio of compression; the decompressed image isn't similar to the original one, but near to it. In the process image compression, there are some conditions to compression algorithm that must consider:

a) Make sure that the information received so far as possible to restore the maximum global Information.
b) Obtain a larger compression ratio.
c) Keep the characteristics of smaller targets.
d) Should be applied in real time.
e) Will need to have a certain confidentiality.

Many methods for computing SVD. The strategy is dependent on diagonalization of the matrix that produces the complete decomposition at once. Another strategy is the utilization of the iterative algorithm, which produces one or several singular values at the same time and can be stopped after desired quantity of singular values and vectors has been computed.

The actually fundamental idea to the SVD domain: going for a high dimensional, highly variable group of data points and minimizing it to a less dimensional space that exposes the substructure of original data more evidently and orders it from the most significant variation to minimal. Making SVD practical to the applications of data compression is the fact that variation below a specific threshold can be simply dismissed to massively minimize data with assurance that the main relationships appealing have been conserved.

Essentially, the process of compression will be implemented on the encrypted (LH, HL and HH) sub-bands, channel provider uses a good technique for compressing these encrypted subbands individually, that lead for acquiring a better performance of compression these detail subbands independently. The encrypted approximation subband has been quantized by utilizing the "η step size" as:

$$Q(i,j) = \left\lfloor \frac{E(i,j)}{\eta} \right\rfloor, 1 \le i \le P/2, 1 \le j \le Q/2, \quad (7)$$

Where an operator $\lfloor \cdot \rfloor$ is an integer minus-infinity and η is equal to 256/α. Therefore, the quantization values Q (i, j) will be between [0, α]. An entropy coding known as binary coding is employed on quantized data. Entire bits needed for quantized approximation subband is B1:

$$B1 = N \log_2(\alpha) \quad (8)$$

There are several steps utilized in the process of compression which are as follows:

Step1 Compress Each one of the encrypted LH, HL and HH sub-bands individually by utilizing the same technique.

Step2 Select the LH sub band to demonstration, after that apply the SVD on the LH subband by utilizing equation (1), The SVD matrix is demonstrated via A.

$$A'_{ixj} = \overline{U}_{ixc}\,\overline{S}_{cxd}\,(\overline{V}_{jxd})^{T} \quad (9)$$

Step3 Finally, get the encrypted detail wavelet rapport utilizing Huffman decoding. Then, the minimized sub images via SVD are gotten for each single LH, HL and HH sub bands.

Because the singular matrix contains singular values "in descending order", then using the visual concept of psycho neglecting the minimum singular values will not significantly minimize the imperceptibility of the image. Because of the utilization of SVD.

In the proposed technique, although "it is lossy", the missing of information isn't clear for the human eye.

For every of the encrypted LH, HL and HH sub-bands, when obtaining the compressed bit streams, the receiver can acquire the encrypted details coefficients via Huffman decoding, then, sub images minimized by SVD are obtained for every wavelet subbands. Further, the actual position of comprehensive coefficients is established by using secret keys (K2). At last, for getting the reconstructed image, inverse of DWT is performed on determined "A" for reconstructing specified wavelet sub-bands.

5. Experimental results and discussion

This chapter clearly discusses about the performance of the developed methodology is evaluated by the common PC having 2.13GHz CPU with 16GB RAM, running on Windows 7 Ultimate 64 bits OS. The analysis presented here was tested on various grayscale images have been performed on a Matlab 2012b platform. The computation formulae of the proposed technique are analyzed utilizing the ratio of compression, mean squared error (MSE), and peak signal to noise ratio (PSNR). This section presents all the performance evaluation details of the security and compression of encrypted image.

This proposed technique is secure under different kinds of attack, as in circumstance of natural image, the neighbouring pixels have strong correlation. also the LL subband and (LH; HL, and HH) subbands are protected through pseudo random number series. Despite the errors and fine detail wavelet coefficients including little significant information that are pseudo-randomly permutated, as the detail sub-bands include the horizontal, vertical and diagonal details, it is appropriate to produce a pseudo-random permutation for hiding the structural information. because of the values of detail subbands aren't changed, that infect maintains the empirical syndication of coefficients in the detail wavelet subbands, at the same time, these will lead to increase the performance of compression.

Considering that the amount data of details wavelet sub bands are three times of that of the estimation subband, so it should be hard for using the search of brute force on the details subbands. Since every detail subbands have an N of coefficients thus, it should need an "N!" manners for predicting the actual location, such as, for an input image with size 512 x512, each one of the detail sub bands has (256 x 256) in other words "65536" of coefficients, Applying the brute force attack for each detail subbands are indeed efficient under permutation based encryption. After that, it should need (65536!) permutation manners, where, "!" is the factorial procedure. It might be hard for any opponent for implementing an effective brute force search on enciphered details wavelet subbands. Consequently, the proposal has gained a preferable point to be secure.

Also, the validity of the proposed technique has been evaluated via measuring the performance of compression, a various number of multisource images are simultaneously encrypted & compressed. And the reconstructed image quality based the minimized bit rate is also experimented, although the degradation in the standard of the reconstructed image isn't visually obvious for the eyes of human. Owing to this proposed technique, it is potential for reducing the images size with a good quality of the images. Figure 5 illustrates a comparison between the proposed technique and the existing technique [19].

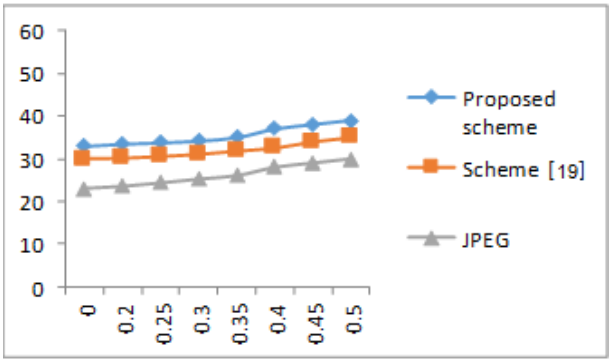


Fig. 5: A Comparison between the Proposed Technique and the Existing Technique [19], in the Values of Ratio of Compression and PSNR.

It could be discovered from Figure 6 that the performance of compression for the proposed technique is significantly much better than [19].

Because of proposed work, an illustration if the multifocus images are compressed utilizing suggested technique then we obtained PSNR equal to 42. 35 dB to 1.57 bpp, nevertheless, via maximizing the parameters of quantizing, a good achievement of compression performance is gotten with the little more destruction in the perceptual quality of reconstructed images.

Even more, for examining the performance of the proposed technique with the concept of compression for different images, the values for the ratio of compression and PSNR are computed with η equal to one. Because of the performance of compression to the images is highly dependent on the selection of wavelets.

Our proposed technique is implemented with different images. When the encrypted LL subband of Lena image is quantized by utilizing a η step size, as well as encrypted LH, HL, and HH subbands, singular values are being utilized for getting the reconstructed image. For example, the image "Lena" has been encrypted, compressed, and renovated, by utilizing Biorthogonal-wavelet on 256 SVs and η = 1, it yields 0.29 CR to PSNR equal to 45.17 dB. As techniques depending on permutation expose the statistical information, in general, the performance of compression is better than stream cipher based encryption & compression scheme. The reconstructed image of this scheme corresponding to the obvious is shown in figure 6 in which the suggested technique obtains a good field of security since until the decrypter won't have the true knowledge of the keys required for encryption and the arrangements manner, it will be difficult for guessing a glance at the original image.

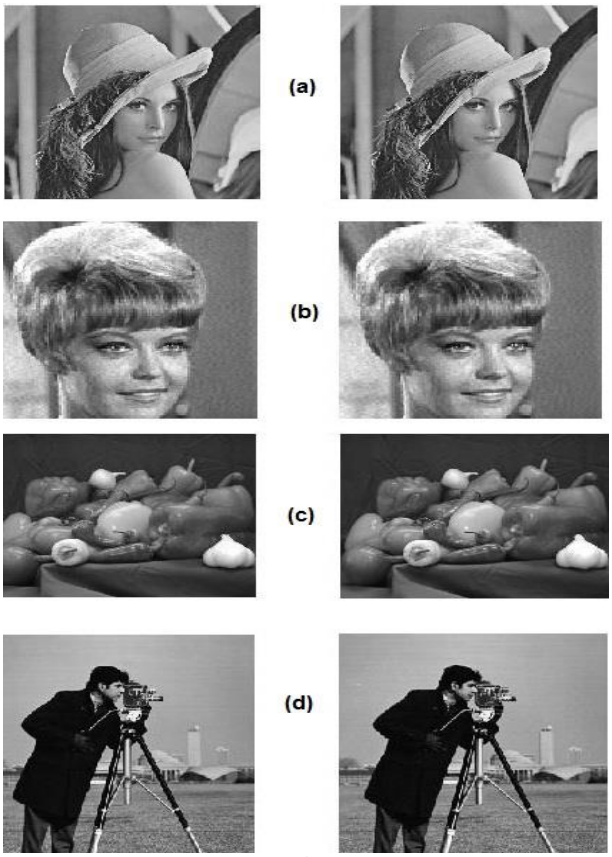


Fig. 6: The Reconstructed Images after the proposed scheme with PSNR equal to: (A) 45.17db, (B) 37.83 Db. (C) 42.29 Db, (D) 41.63 Db.

6. Conclusion

In The purpose of this paper is to provide effective technique of encryption and compression utilized the SVD in compression of results encrypted image by DWT. The encrypted approximation sub band is compressed approximately lossless, the LL coefficients were encrypted via pseudo-random number series with addition modulo 256. The detail coefficients have an information with minimal significant which enciphered via coefficients permutation, and this makes the proposed technique helpful for reducing the image size with a little quality degradation for the reconstructed image, also secure against any brute force search. The enciphered detail sub bands are compressed through SVD and Huffman coding method, a detail sub-bands have actually resulted good compression performance since it has previously less information and on selection of significant information from these sub-bands. The reconstructed image gets on for performing the decompression, decryption and inverse DWT. The performance of our technique is estimated by comparing it with a previous literature on compression of encrypted images and in a case of the task on compression of unencrypted images, the results shows the effectiveness of the proposal. Through the different tested filters of wavelet in the experiments, Biorthogonal wavelet resulted in slightly better results regarding PSNR and ratio of compression. Our proposed technique comes with a merit of utilizing SVD that make us to obtain a considerable performance of compression with keeping a desirable characteristics of the reconstructed image.

References

[1] Vaish, A., Gautam, S., & Kumar, M. (2017). 'A wavelet based approach for simultaneous compression and encryption of fused images'. *Journal of King Saud University-Computer and Information Sciences.* https://doi.org/10.1016/j.jksuci.2017.01.005.

[2] Satone, K. N., Deshmukh, A. S., & Ulhe, P. B. (2017, April). 'A review of image compression techniques'. *In Electronics, Communication and Aerospace Technology (ICECA), 2017 International conference of (Vol. 1, pp. 97-101). IEEE.* https://doi.org/10.1109/ICECA.2017.8203651.

[3] Alfalou, A., & Brosseau, C. (2009). 'Optical image compression and encryption methods'. Advances in Optics and Photonics, 1(3), 589-636. https://doi.org/10.1364/AOP.1.000589.

[4] Alfalou, A., Brosseau, C., Abdallah, N., & Jridi, M. (2013).' Assessing the performance of a method of simultaneous compression and encryption of multiple images and its resistance against various attacks'. Optics express, 21(7), 8025-8043. https://doi.org/10.1364/OE.21.008025.

[5] Zhou, N., Li, H., Wang, D., Pan, S., & Zhou, Z. (2015). 'Image compression and encryption scheme based on 2D compressive sensing and fractional Mellin transform'. Optics Communications, 343, 10-21. https://doi.org/10.1016/j.optcom.2014.12.084.

[6] Johnson, M., Ishwar, P., Prabhakaran, V., Schonberg, D., & Ramchandran, K. (2004). 'On compressing encrypted data'. IEEE Transactions on Signal Processing, 52(10), 2992-3006. https://doi.org/10.1109/TSP.2004.833860.

[7] Schonberg, D., Draper, S. C., & Ramchandran, K. (2005, September). 'On blind compression of encrypted data approaching the source entropy rate'. In Signal Processing Conference, 2005 13th European (pp. 1-4). IEEE.

[8] Zhou, N., Zhang, A., Zheng, F., & Gong, L. (2014). 'Novel image compression–encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing'. Optics & Laser Technology, 62, 152-160. https://doi.org/10.1016/j.optlastec.2014.02.015.

[9] Vaish, A., & Kumar, M. (2015, September). 'Prediction error based compression of encrypted images'. In Proceedings of the Sixth International Conference on Computer and Communication Technology 2015 (pp. 228-232). ACM.

[10] Baker, K. (2005). 'Singular value decomposition tutorial'. The Ohio State University, 24.

[11] Ranade, A., Mahabalarao, S. S., & Kale, S. (2007). 'A variation on SVD based image compression'. Image and Vision computing, 25(6), 771-777. https://doi.org/10.1016/j.imavis.2006.07.004.

[12] Majeed, R., Beiji, B. Z., Hiyam, H., & Jumana, W. (2015). 'Ancient Cuneiform Text Extraction Based on Automatic Wavelet Selection'. International Journal of Multimedia and Ubiquitous Engineering, 10(6), 253-264. https://doi.org/10.14257/ijmue.2015.10.6.25.

[13] Padmavati, S., & Meshram, V. (2017, February). 'A hardware implementation of discrete wavelet transform for compression of a natural image'. In Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET), 2017 International Conference on (pp. 1-5). IEEE. https://doi.org/10.1109/ICAMMAET.2017.8186683.

[14] Singh, A. V., & Murthy, K. S. (2013). 'Vector quantization–based neuro–wavelet model with cumulative distribution function for efficient image compression'. International Journal of Computer Applications in Technology, 48(2), 106-119. https://doi.org/10.1504/IJCAT.2013.056017.

[15] Jumana Waleed, Huang Dong Jun, and Saad Hameed., (2015), "An optimized digital image watermarking technique based on cuckoo search (CS)", ICIC Express Letters, Part B: Applications, Vol. 6, No. 10, pp. 2629-2634.

[16] Jumana Waleed, Huang Dong Jun, Sarah Saadoon, Saad Hameed, Hiyam Hatem, (2015), "An Immune Secret QR-Code Sharing based on a Twofold Zero Watermarking Scheme", International Journal of Multimedia and Ubiquitous Engineering Vol.10, No.4, pp.399-412. https://doi.org/10.14257/ijmue.2015.10.4.38.

[17] Kalman, D. (1996). 'A singularly valuable decomposition: the SVD of a matrix'. The college mathematics journal, 27(1), 2-23. https://doi.org/10.1080/07468342.1996.11973744.

[18] Yen, J. C., & Guo, J. I. (2000). 'Efficient hierarchical chaotic image encryption algorithm and its VLSI realization'. IEE Proceedings-vision, image and signal processing, 147(2), 167-175. https://doi.org/10.1049/ip-vis:20000208.

[19] Zhang, X. (2011). 'Lossy compression and iterative reconstruction for encrypted image'. IEEE transactions on information forensics and security, 6(1), 53-58. https://doi.org/10.1109/TIFS.2010.2099114.