TELKOMNIKA Telecommunication, Computing, Electronics and Control
Vol. 18, No. 6, December 2020, pp. 3080~3087
ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018
DOI: 10.12928/TELKOMNIKA.v18i6.16384

Improved anti-noise attack ability of image encryption algorithm using de-noising technique

Mohanad Najm Abdulwahed, Ali kamil Ahmed
Department of Materials, University of Technology, Iraq

Article Info

Article history:

Received Apr 4, 2020
Revised May 18, 2020
Accepted Jun 25, 2020

Keywords:

DCT
DWT
Gaussian noise
Image encryption
Image processing
SVD

ABSTRACT

Information security is considered as one of the important issues in the information age used to preserve the secret information throughout transmissions in practical applications. With regard to image encryption, a lot of schemes related to information security were applied. Such approaches might be categorized into 2 domains; domain frequency and domain spatial. The presented work develops an encryption technique on the basis of conventional watermarking system with the use of singular value decomposition (SVD), discrete cosine transform (DCT), and discrete wavelet transform (DWT) together, the suggested DWT-DCT-SVD method has high robustness in comparison to the other conventional approaches and enhanced approach for having high robustness against Gaussian noise attacks with using denoising approach according to DWT. Mean square error (MSE) in addition to the peak signal-to-noise ratio (PSNR) specified the performance measures which are the base of this study's results, as they are showing that the algorithm utilized in this study has high robustness against Gaussian noise attacks.

Corresponding Author:

Mohanad Najm Abdulwahed
Department of Materials,
University of Technology,
Baghdad, Iraq.
Email: mohanad.najm@yahoo.com

1. INTRODUCTION

Image processing is defined as certain mathematical operations with the use of signal processing, where the input might be image, picture, image collection, video or photo frame, while image processing's output might be image or set of image-associated parameters or features [1-3]. A lot of image processing approaches involves view the images as two-dimesional (2D) signal as well as utilizing standard approaches for signal processing. The image encryption methods might be categorized into 2 groups on the basis of frequency domain and spatial domain operations [4]. The latter work in spatial domain, encrypted artifacts have been the intensity and position of pixels, whereas the former is in frequency domain is frequency coefficients. The earlier encryption approaches are operating in spatial domain. The techniques related to spatial domain image-encryption are requiring a lot of computations [5].

Generally, some transformation approaches including discrete wavelet transform (DWT) and discrete cosine transform (DCT) have been utilized in the approaches of image encryption on the basis of transform domain. In comparison to conventional discrete Fourier transform (DFT), the DCT is avoiding complex computations, also the DWT might be obtaining strong input image localization features in frequency and spatial domain. The drawbacks of double random phase encryption (DRPE) are recognized, also it is indicated that the digital watermarking has increased robustness in frequency domain, also it might be exploiting the benefits of transform approaches [4]. The major workflow regarding digital watermarking has been close to decryption and encryption of image in which it is hiding original (secret) image to the host image. Specifying the efficiency of image encryption approaches has been of high important with the use of digital watermarking methods [6]. It has been indicated that the strategies of image denoising might be filtering out the image noises throughout image's pre-processing; in the case when such approach might be utilized in developing approaches of image encryption, anti-attack capability of such approach against the noise attacks is going to be enhanced; furthermore, robustness regarding such approach is going to be enhanced [7, 8].

The presented study develops DWT-DCT-SVD (singular value decomposition) based approach of the image encryption according to digital watermarking approaches; the results are showing that the developed approach has the ability for resisting the majority of attacks; the effectiveness of the suggested scheme has been however inacceptable in terms of Gaussian noise attacks. Therefore, the study will specify utilizing the image denoising for boosting anti-attack ability against the noise attacks.

2. SINGULAR VALUE DECOMPOSITION (SVD)

SVD can be defined as matrix transformation approach that depends on the eigenvalue. Each one of the images could be provided as matrix, SVD might be decomposing the matrix to sum of various matrices. Also, SVD isn't associated to transformation between frequency and spatial domain, yet image's singular value has excellent stability; also, it is typically combining with the transform algorithms in the field of image processing. In the case when disturbances are applied to an image, singular value won't be too much modified. Also, matrix's singular vector has invariance in terms of rotation, translation, and so on. Thus, singular value might efficiently reflect the matrix's properties. In the case when being utilized to image's matrix, singular value in addition to its spanned vector space regarding the image might be reflecting various features and components of image. Image's algebraic characteristics might be specified, also SVD has been majorly utilized in the image processing. Due to its rotation invariance and stability, the majority of present algorithms of image encryption have been on the basis of SVD that have elevated robustness [9-11]. An excellent approach for computing eigenvectors and eigenvalues of data matrix X (KxM) has been with the use of SVD specified as follows [12]:

$$X = \begin{bmatrix} x_1 & x_2 \dots\dots\dots\dots & x_M \\ x_{M+1} & x_{M+2} \dots\dots\dots & x_{2M} \\ x_{(K-1)M+1} & x_{(K-1)M+2 \dots\dots} & x_{KM} \end{bmatrix} \quad (1)$$

The theorem of SVD indicating that ^xM matrix X might be decomposed to the next matrices' product:

$$X = U \sum V^{*^T} \quad (2)$$

In which U representing K x K orthonormal matrix which contain left singular vectors that are arranged column wise

$$U = \begin{bmatrix} 1 & 1 \dots\dots & 1 \\ u_1 & u_2 \dots\dots & u_K \\ 1 & 1 \dots\dots & 1 \end{bmatrix} \quad (3)$$

V representing M x M orthonormal matrix related to the right singular vectors,

$$V = \begin{bmatrix} 1 & 1 \dots\dots & 1 \\ v_1 & v_2 \dots\dots & v_K \\ 1 & 1 \dots\dots & 1 \end{bmatrix} \quad (4)$$

while $\sum$ representing K xM matrix regarding the nonnegative real singular values:

$$\Sigma = \begin{bmatrix} \sigma_1 & 0 & & 0 \\ 0 & \sigma_2 & & 0 \\ . & . & . & . \\ . & . & . & . \\ . & . & . & . \\ 0 & 0 & & \sigma_M \\ 0 & 0 & & 0 \\ . & . & . & . \\ . & . & . & . \\ . & . & . & . \\ 0 & 0 & & 0 \end{bmatrix} \quad (5)$$

Due to such SVD's properties, in the past two years, some watermarking calculations were suggested with regard to such system. The major concept of such approach has been discovering the cover image's SVD and then changing its solitary qualities for installing watermark. A few of the SVD-based calculations have been specified as SVD-situated, it might be indicated that the lone SVD area has been applied for implanting watermark to picture. Recently, a few of half and half SVD-based calculations were suggested, in which the different types of changes space involving DCT, DWT, and fast Hadamard transform. were used for inserting the watermark to picture [13].

3. DCT TRANSFORM

This approach has solid energy concentration properties in the low frequency part following a transform. Also, signal's statistical characteristics has been close to the process of Markov, DCT's de-correlated performance has been close to the performance regarding K-L transform; the latter provided optimum de-correlated performance, thus DCT has been majorly utilized in the image processing like image encryption and image compression. In comparison to DFT, computations in the DCT have been in the real domain, eliminating the complex operations as well as enhancing speed. Also, DCT has rotation, translation, and scaling invariance related to Fourier transform that might be efficiently resisting the geometric attacks. Due to such benefits, DCT has excellent performance in image encryption field and was utilized recently in a lot of studies [13, 14].

Changes in discrete cosine has been a process to change flag to rudimentary recurrence parts. Also, it is dealing with the picture as entirety of sinusoids related to frequencies and fluctuating extents. With regard to the information picture, x, the DCT coefficients for changed yield picture, y, have been processed as shown in (5). Furthermore, x, representing info imagehaving N x M pixels, x(m,n) has been pixel's power in push m, also segment n related to picture, y(u,v) representing DCT coefficient in the push u, while the section v of DCT network [15, 16].

$$y(u,v) = \sqrt{\frac{2}{M}}\sqrt{\frac{2}{N}}\,\alpha_u\alpha_v \sum_{u=0}^{M-1}\sum_{v=0}^{N-1} x(m,n)\,\cos\frac{(2m+1)u\pi}{2M}\cos\frac{(2n+1)v\pi}{2N} \quad (6)$$

An image has been re-constructed via using the inverse DCT operation as show in (6):

$$x(m,n) = \sqrt{\frac{2}{M}}\sqrt{\frac{2}{N}} \sum_{u=0}^{M-1}\sum_{v=0}^{N-1} \alpha_u\alpha_v\; y(u,v)\,\cos\frac{(2m+1)u\pi}{2M}\cos\frac{(2n+1)v\pi}{2N} \quad (7)$$

4. DISCRETE WAVELET TRANSFORM (DWT)

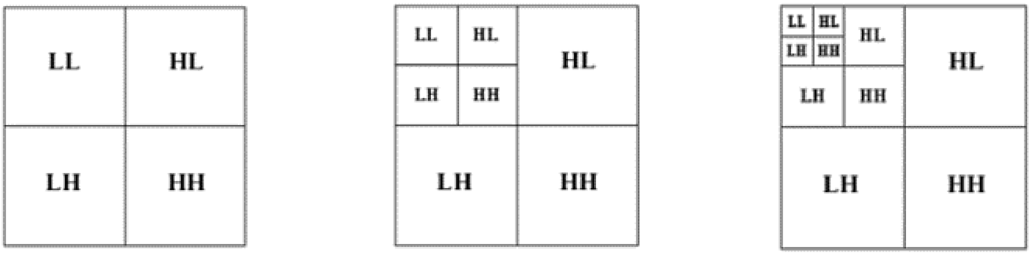
The wavelets have been utilized in image processing for compression, watermarking, sample edge detection, coding and denoising of the interesting features with regard to subsequent classification. The next sub-sections are discussing the denoising of image through thresholding DWT coefficients [17-20].

4.1. DWT of image data

Images are provided as 2D coefficients' array. Each one of the coefficients are representing that point's brightness degree. The majority of the herbal photographs are showing the smooth coloration variations with optimum details representing sharp edges from simple versions. The clean variations in coloration might be labelled as low-frequency versions, in which the pointy variations might be labelled as excessive-frequency versions. Also, low-frequency components (for instance, smooth versions) are showing the photographs' base, in which excessive-frequency components (for instance edges providing the details) have been uploaded upon low-frequency components for refining the image, thus creating in-depth images. Also, the easy versions have been significant in comparison to details. A lot of approaches might be utilized for differentiating between the photograph information and easy variations. An example of such approaches has been picture decomposition through DWT re-modeling. Various levels of de-composition related to DWT can be seen in the Figure 1.

4.2. Image's inverse DWT

Various data classes have been collected to re-constructed image with the use of reverse wavelet transform. Also, pair of the low and high-pass filters have been utilized throughout the process of re-construction. The filters have been indicated to as synthesis filter pair. The process of filtering has been the opposite of transformation; the process is starting from highest level. Furthermore, filters have been initially utilized column-wise, after that row-wise level by level till reaching lowest level.



(a) (b) (c)

Figure 1. DWT Decomposition levels; (a) single level decomposition, (b) two level decomposition, (c) three level decomposition

5. STRATEGIES OF IMAGE DENOISING UTILIZING DWT

With regard to digital image processing, images are sometimes attacked via different noises and the image's quality is going to be reduced; if the image noise might be efficiently filtered out or not, it is going to be affecting subsequent processing like image decryption, edge detection, object segmentation, and feature extraction [21, 22]. With regard to digital image processing, images are sometimes attacked via different noises and the image's quality is going to be reduced; if the image noise might be efficiently filtered out or not, it is going to be affecting subsequent processing like image decryption, edge detection, object segmentation, and feature extraction [21, 22]. The next phases are describing the process of image denoising.

- DWT related to a noisy image will be estimated.
- After the DWT representation done, de-noising is done using soft-thresholding by modified universal threshold estimation (MUTE). Providing ambient noise is a colored, a threshold dependent on level applied to each level of frequency was proposed in [7, 23]. The value of threshold applied to the coefficients of estimated time-frequency using MUTE [23] is expressed as:

$$\lambda_k = c.\sigma_{v,k}\sqrt{2\log(N)} \quad (8)$$

where N is length of signal, $\sigma_{v,k}$ is noise estimated standard deviation for level k, and c is the (modified universal threshold factor) $0<c<1$. The noise variance will be computed with the use of the next robust median estimator:

$$\sigma_v = \frac{median(|X_D(n,k)|)}{0.6745} \quad (9)$$

In which $X_D(n,k)$ representing all coefficients related to wavelet details in level k [24].

- Soft threshold will be utilized to sub-band coefficients with regard to each of the sub-bands, excluding low-pass or approximation sub-band [25].

$$X_{D,\gamma}(n,k) = \begin{cases} sgn(X_D(n,k))(|X_D(n,k)| - \gamma_k) & if|X_D(n,k)| > \gamma_k \\ 0 & if|X_D(n,k)| \le \gamma_k \end{cases} \quad (10)$$

In which γ_k representing threshold value in the level k, also $X_{D,\gamma}(n,k)$ representing wavelet detail coefficients following the process of thresholding in level k.

- Image has been re-constructed through using inverse DWT for obtaining denoised image. Figure 2 showing the data flow diagram related to the denoising process of an image.

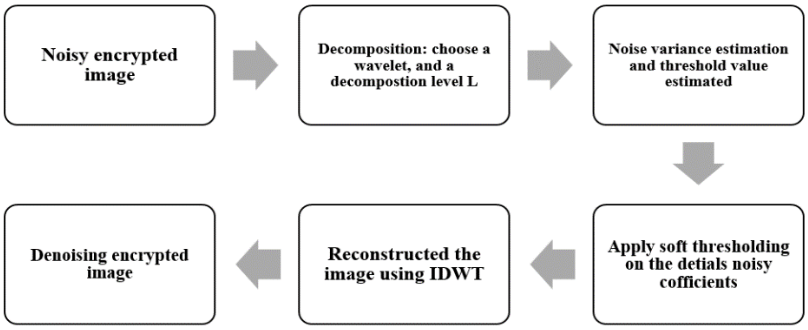


Figure 2. Data flow diagram of image denoising

6. ENCRYPTION TECHNIQUES ACCORDING TO DWT-DCT-SVD THROUGH UTILIZING DENOISING APPROACHES USING DWT

On the basis of the presented DWT-DCT-SVD encryption techniques with the use of normal image as host image, using the approaches of denoising prior to image decryption for enhancing the anti-attack capability related to such approach against noise attacks. Also, new workflow has been shown in the Figure 3. According to the Figure 3, the processes of encryption and decryption might be provided in the following way:

- Step 1: Selecting original and host images of same size;
- Step 2: Utilizing DWT to the two image, also getting 4 sub-bands for each one of the images; following utilizing DCT on the sub-bands, applying SVD for each one of the sub-bands and composed the coincident sub-bands towards original and host images; after that, applying the inverse-DWT as well as the inverse-DCT for getting encrypted image, such process might be treated as DWT-DCT-SVD encryption approach;
- Step 3: Through the encrypted image's transmission, it might be attacked through the noising attacks; using conventional denoising approaches or the linear CNN model-based approach for filtering attacked encrypted image;
- Step 4: Encrypted image is going to be decrypted, also the process of decryption is going to be handled as encryption's inverse procedure; after that, getting the decrypted image.

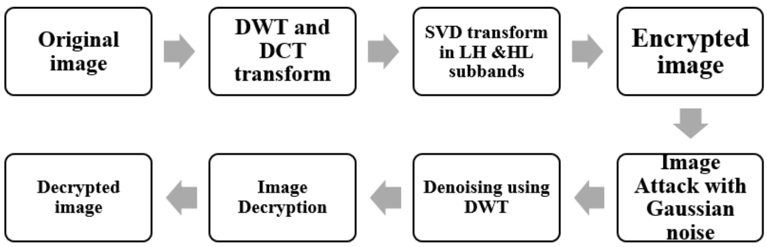


Figure 3. Suggested model

7. PERFORMANCE MEASURES

The common measurement parameters with regard to the reliability of image involves mean absolute error, normalized mean square error (NMSE), mean square error (MSE), and peak signal-to-noise ratio (PSNR). SNR over 40 dB offers optimum quality of the image which is close to original image; SNR with 30-40 dB generally producing excellent quality of the image with adequate distortions; SNR with 20-30 dB presenting bad quality of the image; SNR not more than 20 dB generating undesirable image [26]. Furthermore, the calculation approaches for NMSE and PSNR [27] have been provided in the following way:

$$PSNR = 10\ \log_{10}\frac{255^2}{MSE} \tag{11}$$

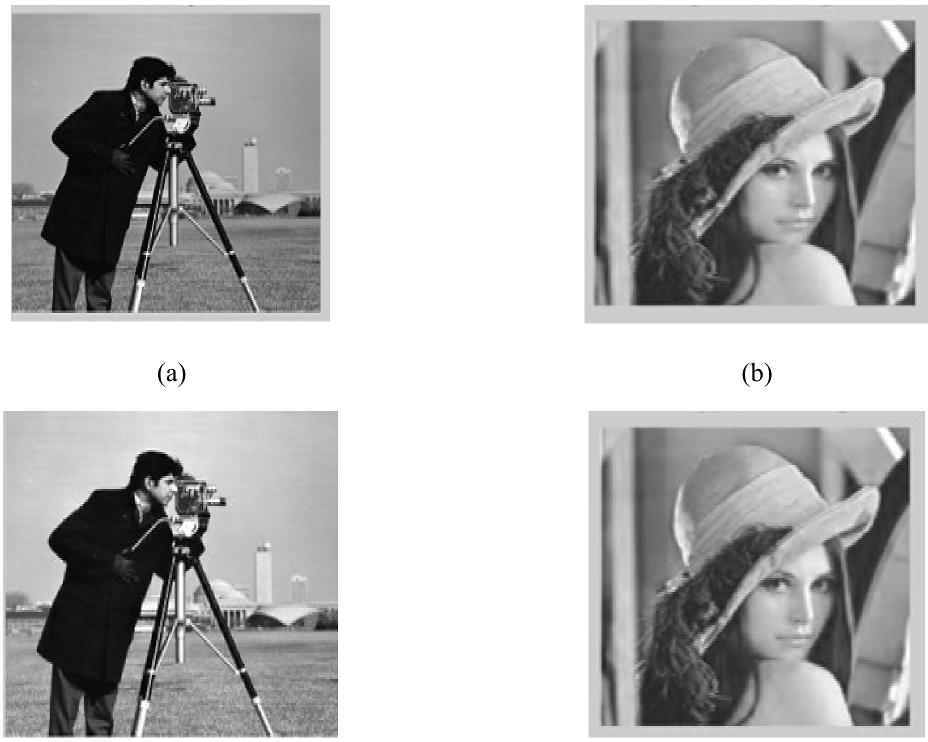
In which MSE representing MSE between original image (x) as well as denoised image ($\hat{x}$) with size M×N:

$$MSE = \frac{1}{M*N}\sum_{i=1}^{M}\sum_{j=1}^{N}[x(i,j)-\hat{x}(i,j)]^2 \tag{12}$$

8. RESULTS AND DISCUSSIONS

This study utilized 2 distinctive algorithms with regard to digital image's watermarking, also for each one of the schemes, there are 3 types of results as follows:
- The image watermarking/dewater marking with no image attack.
- The image watermarking/dewater marking with the Gaussian noise image attack.

With regard to all the sets of images, there have been 3 results related to each algorithm. The recover image's quality has been estimated via MSE and PSNR. High PSNR values representing higher quality related to the recover image because of small errors in the algorithm of image extraction. Also, the MSE near zeros is the similarity measure between 2 images. The study selected image camerman for showing the results. Decrypted and encrypted images can be seen in Figure 4. According to the results, it can be seen that the encrypted image has been comparable to host image. Put differently, secret image's information was successfully hidden in encrypted image. With regard to the decrypted image, it can be indicated that the secret image's details are visible, also specifying that all the 4 results are meeting the expectations, also the encryption approach on the basis of DWT-DCT-SVD system is of adequate performance.



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

Figure 4. Results for algorithm one image encryption with no noise attack;
(a) host image, (b) original image, (c) encrypted image, (d) decrypted image

The study utilized the DCT-DWT-SVD noise algorithm on the host image for watermarking original image. After that, the Gaussian image with the variance attacks has been applied to the watermark image, also it has been dewater marked and the extracted watermarked image can be seen in the Figure 5. Table 1, showing the suggested method's performance on the noise power with variance 0.1 on the basis of Daubechies wavelet biases in comparison to the case with no noise attack. The values of MSE and PSNR have been estimated according to noise power value.

Table 1. Performance on the noise power with variance 0.1 on the basis of Daubechies wavelet biases in comparison to the case with no noise attack

Case	PSNR	MSE
No Attack	212	0.00
3	42.30	0.008

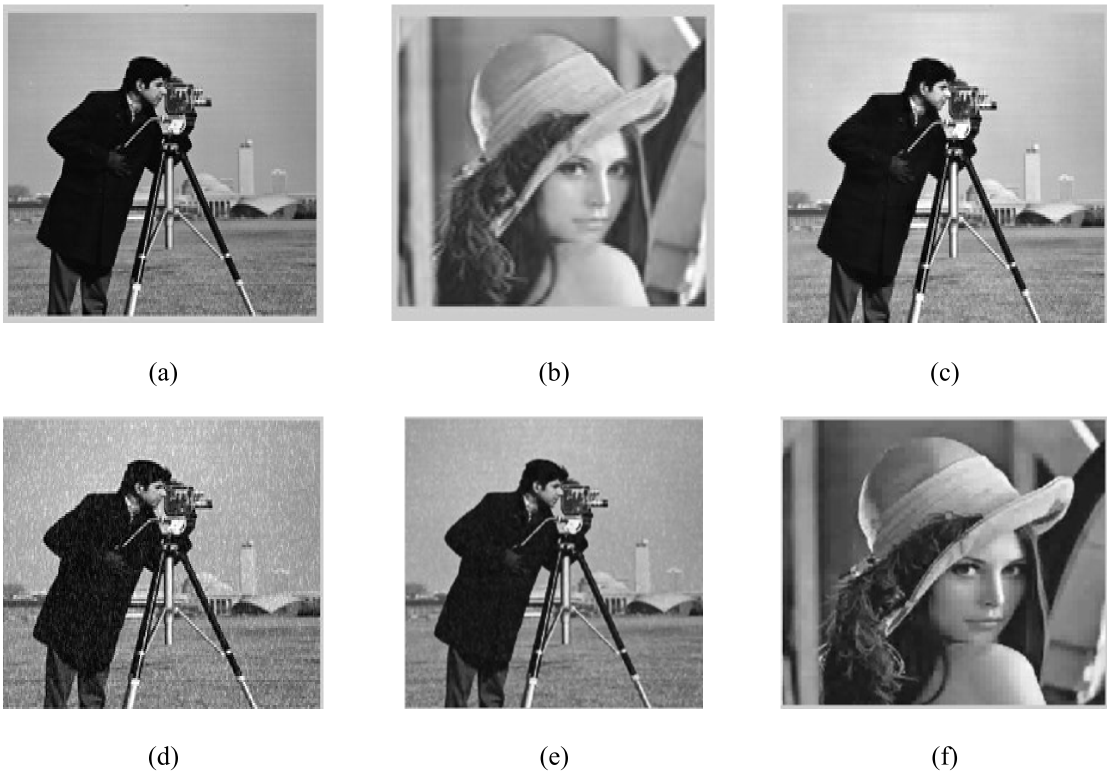


Figure 5. Image encryption results with the Gaussian noise attack;
(a) host image, (b) original image, (c) encrypted image, (d) gaussian noise encrypted image,
(e) encrypted image after denoising, (f) decrypted image denoising

9. CONCLUSIONS

The results of this study are suggesting that the DCT-DWT-SVD based watermarking approach as well as the denoising algorithm utilizing DWT has been providing optimum performance in the existence of watermark image's recovery that has been attacked via Gaussian noise. Results have been analytically verified with regard to MSE and PSNR, also the two have been high for new DCT-DWT-SVD watermarking system.

REFERENCES

[1] M. Sharkas, D. ElShafie, and N. Hamdy, "A Dual Digital-Image Watermarking Technique," *The Third World Enformatika Conference*, pp. 136-139, April 2005.

[2] O. Omoruyi, *et al*., "Evaluation of the quality of an image encrytion scheme," *TELKOMNIKA Telecommunication Computing Electronics and Control,* vol. 17, no. 6, pp. 2968-2974, December 2019.

[3] E. H. Rachmawanto, *et al*., "An improved security and message capacity using AES and Huffman coding on image steganography," *TELKOMNIKA Telecommunication Computing Electronics and Control,* vol. 17, no. 5, pp. 2400-2409, October 2019.

[4] Z. Liu, "Comparative evaluations of image encryption algorithms," Auckland University of Technology, 2018.

[5] Z. Liu, *et al.*, "Double image encryption by using Arnold transform and discrete fractional angular transform," *Optics and Lasers in Engineering,* vol. 50, no. 2, pp. 248-255, February 2012.

[6] N. Divecha and N. Jani, "Implementation and performance analysis of DCT-DWT-SVD based watermarking algorithms for color images," *2013 International Conference on Intelligent Systems and Signal Processing (ISSP)*, pp. 204-208, March 2013.

[7] Y. Y. Al-Aboosi, R. S. Issa, and A. khalid Jassim, "Image denosing in underwater acoustic noise using discrete wavelet transform with different noise level estimation," *TELKOMNIKA Telecommunication, Computing, Electronics and Control*, vol. 18, no. 3, pp. 1439-1446, June 2020.

[8] R. Thillainayagi and K. Senthil Kumar, "Combination of wavelet transform and singular value decomposition-based contrast enhancement technique for target detection in UAV reconnaissance thermal images," *Journal of Modern Optics,* vol. 66, no. 3, pp. 606-617, January 2019.

[9] N. M. Makbol, B. E. Khoo, and T. H. Rassem, "Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics," *IET Image processing,* vol. 10, no. 1, pp. 34-52, 2016.

[10] A. Mansouri, A. M. Aznaveh, and F. T. Azar, "SVD-based digital image watermarking using complex wavelet transform," *Sadhana,* vol. 34, no. 3, pp. 393-406, June 2009.
[11] L. Novamizanti, G. Budiman, and E. N. F. Astuti, "Robust audio watermarking based on transform domain and SVD with compressive sampling framework," *TELKOMNIKA Telecommunication, Computing, Electronics and Control,* vol. 18, no. 2, pp. 1079-1088, April 2020.
[12] Handito, Kurniawan Wira, *et al.*, "The comparison between SVD-DCT and SVD-DWT digital image watermarking," *International Conference on Data and Information Science. IOP Conf. Series: Journal of Physics: Conf. Series,* vol. 971. 2017.
[13] Zhang, Lina, and Deyun Wei, "Dual DCT-DWT-SVD digital watermarking algorithm based on particle swarm optimization," *Multimedia Tools and Applications,* vol. 78, pp. 28003-28023, 2019.
[14] L. Novamizanti, G. Budiman, and I. Safitri, "Modified DCT-based audio watermarking optimization using genetics algorithm," *TELKOMNIKA Telecommunication, Computing, Electronics and Control,* vol. 16, no. 6, pp. 2651-2660, December 2018.
[15] K. R. Rao and P. Yip, "Discrete cosine transform: algorithms, advantages, applications," *Academic Press Professional*, August 1990.
[16] G. Budiman, L. Novamizanti, and I. Iwut, "Genetics algorithm optimization of DWT-DCT based image Watermarking," *Journal of Physics: Conference Series*, vol. 795, no. 1, pp. 012039, February 2017.
[17] M. Misiti, *et al*., "Wavelet toolbox," *The MathWorks Inc., Natick, MA,* vol. 15, pp. 21, 1996.
[18] D. Gupta and S. Choubey, "Discrete wavelet transform for image processing," *International Journal of Emerging Technology and Advanced Engineering,* vol. 4, pp. 598-602, 2015.
[19] D. Baleanu, "Advances in wavelet theory and their applications in engineering, physics and technology," *BoD–Books on Demand*, 2012.
[20] W. S. Sari, E. H. Rachmawanto, and C. A. Sari, "A Good Performance OTP encryption image based on DCT-DWT steganography," *TELKOMNIKA Telecommunication Computing Electronics and Control,* vol. 15, no. 4, pp. 1987-1995, December 2017.
[21] M. N. Abdulwahed and A. kamil Ahmed, "Underwater image de-nosing using discrete wavelet transform and pre-whitening filter," *TELKOMNIKA Telecommunication, Computing, Electronics and Control,* vol. 16, no. 6, pp. 2622-2629, December 2018.
[22] C. Kumar, G. Sai, R. K. Kumar, G. A. Naidu, and J. Harikiran, "Noise removal in microarray images using variational mode decomposition technique," *TELKOMNIKA Telecommunication Computing Electronics and Control,* vol. 15, no. 4, pp. 1750-1756, December 2017.
[23] D. L. Donoho, "De-noising by soft-thresholding," *IEEE transactions on information theory,* vol. 41, pp. 613-627, 1995.
[24] I. M. Johnstone and B. W. Silverman, "Wavelet threshold estimators for data with correlated noise," *Journal of the royal statistical society: series B (statistical methodology),* vol. 59, pp. 319-351, 1997.
[25] R. Aggarwal, *et al*., "Noise reduction of speech signal using wavelet transform with modified universal threshold," *International Journal of Computer Applications,* vol. 20, no. 5, pp. 14-19, April 2011.
[26] C. Tan, G. Seet, A. Sluzek, and D. He, "A novel application of range-gated underwater laser imaging system (ULIS) in near-target turbid medium," *Optics and Lasers in Engineering,* vol. 43, no. 9, pp. 995-1009, September 2005.
[27] J. Ellinas, T. Mandadelis, A. Tzortzis, and L. Aslanoglou, "Image de-noising using wavelets," *TEI of Piraeus Applied Research Review,* vol. 9, pp. 97-109, 2004.