

An Improvement in Digital Image Watermarking Scheme Based on Singular Value Decomposition and Wavelet Transform

Manasha Saqib¹ and Sameena Naaz²

^{1&2}Department of Computer Science and Engineering,

School of Engineering Sciences and Technology, SEST, New Delhi, India

E-Mail: manashasqib@gmail.com, snaaz@jamiyahamdard.ac.in

(Received 21 January 2019; Revised 4 February 2019; Accepted 16 February 2019; Available online 22 February 2019)

Abstract - An enormous growth of multimedia information in the internet has given rise to varied unauthorized use and modification. This authenticity issue is equally a limitation both in the defense data transmission and secured transmission. Digital watermarking is one of the legitimate solutions to the above problem since it makes possible validation and secure transmission of secret data. This paper presents a robust and secure digital image watermarking scheme that can be used for copyright protection. The scheme involves Lifting Wavelet Transform (LWT) and Singular Value Decomposition (SVD). The latest approach to wavelet transform is the Lifting Wavelet Transform and the significant transform technique for robust digital image watermarking is Singular Value Decomposition. The results are cross-validated by using inverse LWT and SVD. The digital signature mechanism is used to generate and embed a digital signature after the watermark is embedded, then the ownership is authenticated before extracting watermarks. In order to check the robustness of the method against various common image processing attacks like Mean, Median, Gaussian, Shear, Rotation and Crop, certain performance metrics such as peak to signal noise ratio (PSNR) and mean square error (MSE) is computed. To check similarity, normal cross-correlation (NCC) is used.

Keywords: Watermarking, Lifting Wavelet Transform, Singular Value Decomposition, Peak to Signal Noise Ratio, Mean Square Error, Normal Cross-Correlation

I. INTRODUCTION

In the modern period, there is an immense rise in sharing of multimedia messages that include images, audios, and videos over the internet as a result of which it is a problem of concern to secure that digital information. In this way, technocrats are trying endeavors to make innovations for the security of information. Digital watermarking is one such method that is employed to communicate multimedia information in a protected manner over the network by giving proprietorship rights. Digital watermarking is much more secured and progressed when compared with effectively existing strategies to send the interactive media information safely. Watermarks are named so because they truly correspond the impact of water droplets spread over the sheet of paper. Digital image watermarking is basically a branch of applied science that reviews the digital images and their changes so as to enhance their quality or to extract data [1-2]. Watermarking is actually described as hiding secret information regarding the signal within the cover signal itself so as to protect that cover signal. The

interactive media objects, within which the watermark is inserted, are typically called the original image, cover image. The watermark must be inserted in such a way that the uniqueness of the cover image is not changed or later it can be extracted as a proof of authenticity owner. In contrast to encryption, that is beneficial for transmission, however, does not give an approach to analyze the original information in its secured form, the watermark remains within the content in its unique form and user is not prevented from viewing, analyzing, or controlling the content. Also, in contrast to steganography, where both the message and methods of concealing the message is secret. In watermarking, generally, the watermark insertion procedure is known and therefore it is not necessary for the message to be secret. The basic requirements associated with any watermarking system are:

A. Imperceptibility: One of the essential conditions for digital image watermarking is imperceptibility. Imperceptibility is also referred to as fidelity or perceptual transparency. Imperceptibility means that there should be a low deformation of the image so that the user cannot distinguish the difference between the original images and the watermarked image [3]. Transparency and fidelity characterize the similarities between the original and watermarked content. Once the watermark is inserted into the cover image, no distortion in the watermarked image suggests that the transparency is high.

B. Robustness: One of the foremost ordinarily measured properties for image watermarking is that watermark signals should be moderately resilient to various attacks. The robustness means that the inserted image must be recovered even if the watermarked image was manipulated by attacks. The examples of these attacks are image processing attacks such as removal attacks, geometric attacks such as cropping, rotation, translation etc. Watermarking method is said to be robust if removal of a watermark is difficult for various attacks.

C. Security: The most significant issue of watermarking system is the Security. A watermarking system is secure if the watermark cannot be removed by an unauthorized person without having full awareness of embedding procedure, extraction, and composition of a watermark. Only an authorized person can detect the watermark.

Security is mainly used to explain the resistance of a scheme against malicious attacks.

D. Data Payload: It refers to the number of bits inserted into the cover image. The highest amount of data that can be covered up without destroying image quality is called as a data payload. It is calculated by the quantity of hidden data within the original information. This property depicts what proportion information must be inserted as a watermark with the goal that it can be successfully identified during watermark extraction process.

E. Computational Complexity: Computation complexity is characterized as the measure of time taken by the watermarking procedure for embedding and extraction process. For the robust security and validity of the watermark, the more computational difficulty is required. On the other side, both speed and efficiency are required by real-time applications.

F. Inevitability: Inevitability is characterized as the likelihood to produce the original information during the watermark extraction process. The enhancement of the parameter is reciprocally competitive and cannot be evidently done at the same time. A reasonable transaction is dependably a prerequisite. On the other hand, if robustness to strong warp is a difficulty, the message that can be regularly covered up should not be too long.

These requirements must meet up to make a plan of a framework for watermarking images that can be described as watermark embedding and watermark extraction. Digital watermarking has numerous applications in the fields of ownership identification, copyright assurance, broadcast monitoring, tamper detection, various medical applications as well as secret communications etc. Depending upon the domain within which the watermark is inserted, these techniques are primarily classified into two classes that are spatial-domain and transform-domain methods. Spatial domain is the inserting of watermark by modifying the intensity values or pixel values of the image. The benefits of the spatial domain are low complexity and easy implementation. But the spatial-domain methods are typically fragile to image processing attacks. The frequency domain is the inserting of the watermark in frequency elements of the image. Frequency domain technique is simpler when compared to the spatial domain as a result of its robustness and imperceptibility [4]. The transform domain method is most popular over spatial domain method as they are much more resilient in presence of noise. In the frequency domain, the most popular techniques include Lifting Wavelet Transform (LWT), Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), and Singular Value Decomposition (SVD).

In this paper, LWT-SVD technique is introduced to insert watermark image into the main or cover image, thereby maintaining overall robustness property of the watermark, excellence of carrier media and security. Here is a brief

outline of the chapter, in Section I introduction regarding digital image watermarking is presented followed by brief literary in Section II. In Section III proposed approach is described. Here, watermark embedding and watermark extraction algorithms in Lifting Wavelet Transform domain with Singular Value decomposition are described. The Section IV describes the performance evaluation metrics followed by results in detail with graphical and tabular forms in Section V and finally in Section VI conclusion of the current research is presented.

II. LITERATURE REVIEW

Literature review survey was done on wavelet transformation and wavelet transformation in combination with singular value decomposition techniques to hide data in digital color images.

Kaur *et al.*, [4] proposed an improved method for inserting a watermark into a cover image that is based on the idea of 2-level discrete wavelet transform (DWT) in combination with the singular value decomposition (SVD). The algorithm proposed by them confirms that the method is secure enough to guard the multimedia objects. The proposed method is capable of achieving the various properties of digital image watermarking like imperceptibility, security and robustness of inserted watermark. Both the qualitative and quantitative results confirm that the watermark is imperceptible, robust under various attacks and is secure.

Radouane *et al.*, [5] proposed a robust watermarking method for copyright protection. The proposed method is primarily based on the combination of three transformations DWT, SVD and DCT using optimal block ensure the various properties of digital image watermarking like imperceptibility, capacity and robustness. The experimental results display the different results of PSNR for each coefficient of DWT and the method is robust against various attacks.

Shrinivas *et al.*, [6] proposed a unique watermarking method for color images using the combination of HL sub-band of Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD). The singular matrices achieved by applying SVD to the DWT applied watermark image, are added in proper proportion to the singular matrices achieved by applying SVD to the DWT applied cover image. The Peak Signal to Noise Ratio (PSNR) and correlation coefficients were used to estimate the quality of the watermarked image. The Experimental results applied to various test images display good performances for the proposed algorithm.

Bhuyan *et al.*, [7] proposed a hybrid singular value decomposition (SVD) and discrete wavelet transform (DWT) based watermarking scheme. In this scheme, a variant of the traditional SVD is used called as shuffled SVD (SSVD). By using DWT the host image is decomposed into four sub-bands (LL, LH, HL, and HH).

Further, the LL sub-band is decomposed into appropriate size blocks. In various blocks of LL sub-band, the components of the watermark image that are achieved by applying SSVD are inserted. The proposed method display good robustness against various attacks. The proposed technique exploits stability property of singular values and the localization and spatio frequency property of DWT. The correlation coefficient value close to 1 and PSNR value above 30 dB is achieved.

Sheth and Nath [8] proposed a new secured digital Watermarking method for the validation of data based on the combination of discrete wavelet transform (DWT) and discrete cosine transform (DCT) methods along with cryptographic method known as Arnold Transform. The proposed method is efficient and secure. The proposed method has been implemented in MATLAB environment. The proposed method provides good robustness and perception transparency to the original and watermarked image against various types of attacks like noise, cropping and scaling. It is found that in terms of Peak Signal Noise Ratio (PSNR), Mean Square Error (MSE), and Similarity Factor (SF), the proposed method is DCT-superior to LSB and DCT methods.

Pardhu and Perli [9] proposed a secured algorithm for inserting digital watermarks into images. The proposed technique shows that the watermark is imperceptible in the domain. The watermark is inserted in a multi-resolution way in the DCT and DWT domain of an image. Once the watermark is extracted in the decoding phase from the watermarked image, various performance measures like correlation coefficient and peak signal to mean noise ratio (PSNR) are calculated. To check the robustness of the proposed technique various types of attacks have been applied to the watermarked image.

Furqan and Kumar [10] proposed a robust and blind digital image watermarking technique for copyright protection based on the combination of both DWT and SVD techniques. Initially, the original image is decomposed into 4 sub-bands using 2-D DWT, and then SVD is applied to each band by modifying their singular values. Different types of technologies have been developed so as to protect copyright material from illegal duplication, such as key-based cryptographic technique, digital watermarking etc. In digital image watermarking, by using an algorithm a signature or copyright message is embedded secretly in the image. The watermarked image is subjected to different attacks like rotation, cropping, adding noise, blurring, compression, the originally embedded watermark image is extracted from all the bands and are compared on the basis of their PSNR and PSNR values.

Makbol and EeKhoo [11] proposed a secure and robust digital image watermarking technique for copyright protection. The proposed method uses the integer wavelet transform (IWT) and singular value decomposition (SVD). In this scheme, the grey-image watermark pixels values are

inserted directly into the singular values of the 1-level IWT decomposed sub-bands. The experimental results show the effectiveness of the proposed technique in terms of imperceptibility, robustness, and capacity due to the IWT and SVD properties.

Dejun *et al.*, [12] proposed a robust digital image watermarking method based on discrete wavelet transform (DWT) and singular value decomposition (SVD). In this scheme, the singular values of small blocks of the low-frequency approximation sub-band (LL) of the DWT domain are modified to insert the watermark into the cover image. The experimental results show the robustness of image watermarking against various types of attacks.

Santhi and Thangavelu [13] proposed another Singular Value Decomposition and Discrete Wavelet Transform based procedure for concealing watermark in full frequency band of color images (DSFW). They measured the watermarked image quality and extracted watermark using various parameters like peak signal to noise ratio (PSNR) and normalized correlation respectively. The algorithm proposed by them shows the robustness of watermarked image against various attacks, for example, salt and pepper noise, Gaussian noise, JPEG compression and cropping. A good PSNR value of 36dB was found.

Tao *et al.*, [14] analysed and reviewed the different watermarking techniques in spatial and transform domains. In this scheme, different techniques using discrete wavelet transform and singular value decomposition in transform domain have been reviewed. Further, the analysis of the watermarking techniques has been represented in the form of tables taking into consideration various factors of image watermarking such as capacity, security, imperceptibility, robustness and false positive. In this scheme, various attack techniques were used in order to assess the digital watermarking system.

III. PROPOSED SYSTEMS

The proposed watermarking scheme is based on lifting wavelet transform (LWT) and singular value decomposition (SVD). The proposed work is focused on enhancing the robustness of watermark by working in the frequency domain and thereby improving the imperceptibility of the watermark. The image is decomposed first into four frequency bands: LL, LH, HL, and HH bands. LL depicts the low-frequency band and gives the approximate details, LH depicts the middle frequency band and gives the vertical details, HL band depicts the middle frequency band and gives the horizontal details, HH band depicts the high frequency and it gives the diagonal details of the image. In this scheme, HH band is selected to insert the watermark since this band contains the finer details and contributes inconsiderably to the image energy. The fundamental model of Digital Image Watermarking comprises of two sections:

1. Watermark embedding
2. Watermark extraction.

$$W=U_w * S_w * V_w^T$$

6. Extract the digital signature from the LL4 band. The procedure is as follows:
 - a) With the help of a secret key, select N random coefficients from LL4 and HH4 band. Now the integer part is converted into the binary code of L bits.
 - b) The digital signature is reconstructed by extracting the nth bit from the coefficients.
7. An audio key decryption is used for the validation of the signature.

8. Generate the digital signature using the orthogonal matrices of the original watermark and it is compared with reconstructed signature. If the signatures match, the orthogonal matrices are authenticated.
9. The watermark is constructed by using the singular values extracted from the HH band and orthogonal matrices U_w and V_w achieved after applying SVD to original watermark.

$$W = U_w * S_H * V_w^T$$

10. Thus, the watermark image is extracted.

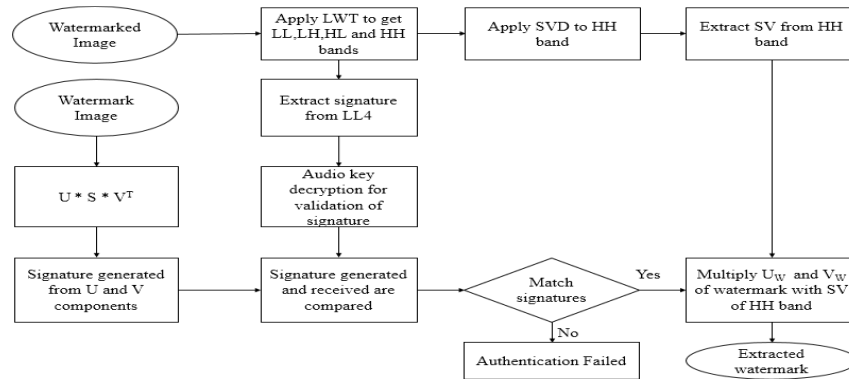


Fig. 2 Watermark Extraction Procedure

IV. PERFORMANCE EVALUATION METRICS

To evaluate the performance of the watermarked images, the various quality measures used in this scheme are PSNR (peak signal to noise ratio), MSE (mean square error) and NCC (normalized cross-correlation).

A. Peak Signal to Noise Ratio (PSNR): In this scheme, PSNR measures the imperceptibility between the original host image and the watermarked image. The watermark should not be noticeable to the user, nor should it corrupt the quality of the original image. For a gray scale image, PSNR is defined as:

$$PSNR = 10 \log_{10} \left[\frac{255^2}{MSE} \right]$$

B. Mean Square Error (MSE): MSE is defined as the Mean square error between the cover image and watermarked image. The MSE can be expressed as:

$$MSE = \frac{1}{M \times N} \sum_i \sum_j [I(i, j) - I_w(i, j)]^2$$

In the above equation $I(i, j)$ is the original host image and contains $M \times N$ pixels and $I_w(i, j)$ is the watermarked image.

C. Normalized Cross Correlation (NCC): The correlation coefficient is used to check the similarity between the two images of the same size. The value of Correlation coefficient varies between 0 and 1. The value of 1 for CC is considered to be the idle value.

$$\rho(W, W^*) = \frac{\sum_{i=1}^N \sum_{j=1}^N (w_{ij} - \mu_w)(w^*_{ij} - \mu_w^*)}{\sqrt{\sum_{i=1}^N \sum_{j=1}^N (w_{ij} - \mu_w)^2} \sqrt{\sum_{i=1}^N \sum_{j=1}^N (w^*_{ij} - \mu_w^*)^2}}$$

The above equation measures the correlation coefficient between the watermark inserted and the watermark extracted. Here W is the inserted watermark and W^* is the extracted watermark. μ_w is the mean value of the inserted watermark and μ_w^* is the mean value of the extracted watermark.

V. EXPERIMENTAL RESULTS

The proposed LWT–SVD scheme simulation was implemented in MATLAB. The experiment is performed for cover image “Lena” of dimension 512×512 . Image “Cherry” of dimension 512×512 is used as the watermark image. The images are given below in Fig.3 and Fig.4. Fig.5 and Fig. 6 shows the 1-step and 4-step LWT decomposition of the cover image.



Fig. 3 Cover Image



Fig. 4 Watermark Image

A. Test for Imperceptibility

Imperceptibility is the measure of transparency and is measured through performance measures like a peak signal to noise ratio (PSNR) and Mean Square Error (MSE). Imperceptibility is good when the watermarked image looks nearly identical to the original image. Thus, the watermark embedding process barely affects the cover image. Fig.7

shows the watermarked image obtained for cover image “Lena” keeping “Cherry” as the watermark. Fig.8 shows the watermarked images after applying various attacks. Table I gives the PSNR and MSE values of the watermarked image with respect to the original cover image before and after the attack. Fig.9 shows the PSNR values for cover and watermarked image. Fig.10 shows the MSE values for the cover and watermarked image.

6 types of attacks: mean attack, median attack, Gaussian attack, rotation attack, shear attack and crop attack.

TABLE I VALUES OF PSNR AND MSE FOR COVER AND WATERMARKED IMAGE

Attacks	Performance Metrics	
	PSNR	MSE
No Attack	42.39	3.74
Mean	28.28	96.42
Median	35.21	19.56
Gaussian	39.28	7.67
Rotation	10.43	5.8851e+03
Shear	9.07	8.0404e+03
Crop	12.90	3.3299e+03

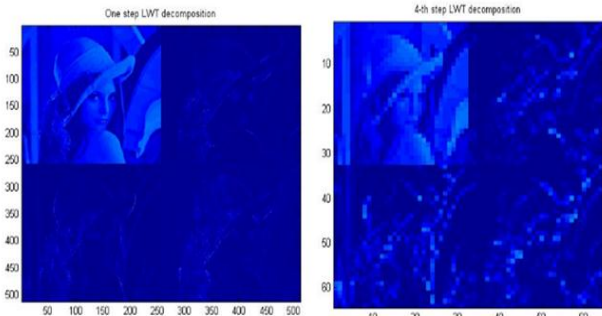


Fig. 5 1-step LWT decomposition

Fig. 6 4-step LWT decomposition



Fig. 7 (a).Cover Image (b).Watermarked Image signed with secret key (c).Watermark logo



Fig. 8 Attacked Watermarked Images

B. Test for Robustness

To check the robustness of the proposed method, various geometric attacks were performed on the watermarked image and watermark was extracted. Robustness of image was checked by comparing the similarity of watermark image extracted with the original watermark image. The robustness of the watermarking scheme against various types of attacks can be measured using normalized correlation coefficient values. The robustness is tested under

Fig. 11 shows the extracted watermark before the attack. Fig. 12 shows the extracted watermark after applying various attacks. For proposed scheme Table II gives values of the correlation coefficient between extracted watermark and original watermark for cover image “Lena” before and after the attack. Fig.13 shows the Normalized Cross Correlation values for the extracted watermark.

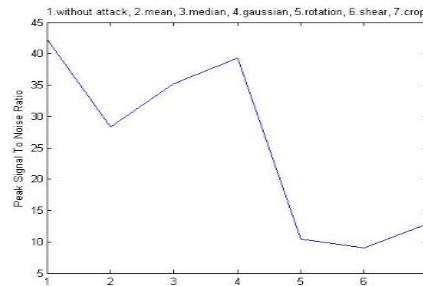


Fig. 9 PSNR values for cover and watermarked image

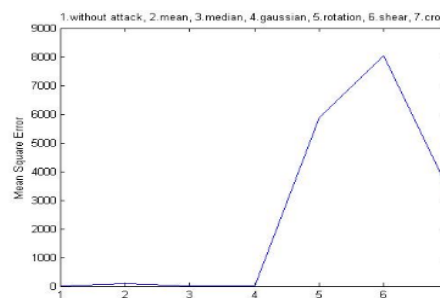


Fig. 10 MSE values for cover and watermarked image



Fig. 11 Extracted watermark without attack

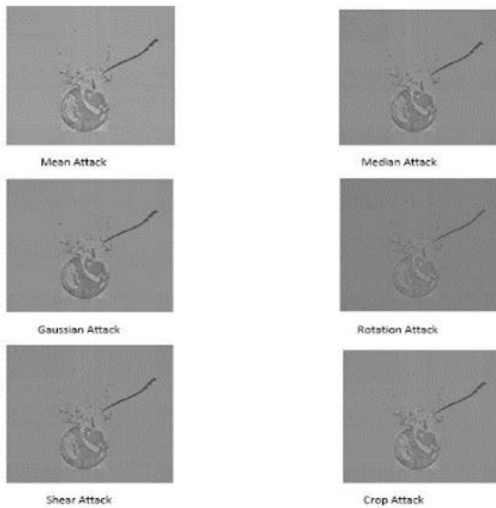


Fig. 12 Extracted Watermark Images after Applying Various Attacks

TABLE II VALUES OF NC FOR EXTRACTED WATERMARK IMAGE

Attacks	Performance Metric
	Normalized Cross Correlation
No Attack	1.00
Mean	0.6687
Median	0.6592
Gaussian	0.7354
Shear	0.6154
Crop	0.6289

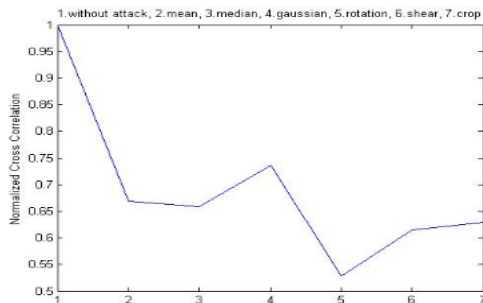


Fig. 13 Normalized Cross correlation Values for Extracted Watermarks

VI. CONCLUSION

The proposed method has been implemented in MATLAB environment. In this chapter, an improved, secure and robust image watermarking scheme using Lifting Wavelet Transform (LWT) and Singular Value Decomposition (SVD) is proposed. This scheme particularly presents the whole process of the research, which includes image processing, embedding of the watermark that is encoding, attacking of the watermarked images, extraction of the watermark that is decoding, and evaluation of the results achieved. This scheme utilizes the properties of both LWT and SVD transforms to achieve the watermarking requirements that is the watermark is imperceptible, robust under various attacks like mean, median, Gaussian, rotation, shear and crop and is

secure. The main objective of the research is to improve the efficiency of digital image watermarking under various circumstances that can be depicted by the type of the attack as well as by the motivation of the watermarking. Performance of the watermarked images has been analysed in terms of normalized cross-correlation, peak signal to noise ratio and mean square error. This watermarking scheme gives NCC value 1 for no attacks with good PSNR and MSE values. Parameter values achieved by this scheme are good for all most all common image processing attacks. The security is improved and guaranteed by using a digital signature authentication mechanism.

REFERENCES

- [1] V. Stuhl and N. N. Khalsa, "Digital watermarking of an image using wavelet transform", *International Journal of Pure and Applied Research in Engineering and Technology (IJPRET)*, Vol. 8, No. pp.365-378, 2013.
- [2] K.S. Rawat, S. Goyal, and R. Gupta, "Discrete wavelet based image watermarking: An idea leads to security", *Journal of Biometrics*, Vol.1, No. pp.06-10, 2010.
- [3] H.M. Yang, Y.Q. Liang, X.D. Wang, and S.J. Ji, "A DWT- based evaluation method of imperceptibility of watermark in watermarked color image", *International Conference on Wavelet Analysis and Pattern Recognition*, 2007.
- [4] J. Kaur, N. Singh, and C. Jain, "An improved image watermarking technique implementing 2-DWT and SVD", *IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, 2016.
- [5] M. Radouane, R. Messoussi, R. Touahni, and T. Boujiha, "Robust method of digital image watermarking using SVD transform on DWT coefficients with optimal block", *International Conference on Multimedia Computing and Systems (ICMCS)*, 2014.
- [6] N. S. Naik, N. Naveena, and K. Manikantan, "Robust digital image watermarking using DWT SVD approach", *IEEE International Conference on Computational Intelligence and Computing Research (ICIC)*, 2015.
- [7] T. Bhuyan, V. K. Srivastava, and F. Thakkar, "Shuffled SVD based robust and secure digital image watermarking", *International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, 2016.
- [8] R. K. Sheth and V. V. Nath, "Secured digital image watermarking with discrete cosine transform and discrete wavelet transform method", *International Conference on Advances in Computing, Communication, & Automation (ICACCA) (Spring)*, 2016.
- [9] T. Pardhu and B. R. Perli, "Digital image watermarking in frequency domain", *International Conference on Communication and Signal Processing (ICCSP)*, 2016.
- [10] A. Furqan and M. Kumar, "Study and Analysis of Robust DWT-SVD Domain Based Digital Image Watermarking Technique Using MATLAB", *IEEE International Conference on Computational Intelligence & Communication Technology*, 2015.
- [11] 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.
- [12] Y. Dejun, Y. Rijjing, L. Hongyan, and Z. Jiangchao, "A digital watermarking scheme based on singular value decomposition and discrete wavelet transform", *Proceedings of 2011 International Conference on Computer Science and Network Technology*, 2011.
- [13] V. Santhi and A. Thangavelu, "DWT-SVD Combined Full Band Robust Watermarking Technique for Color Images in YUV Color Space", *International Journal of Computer Theory and Engineering*, pp. 424–429, 2009.
- [14] H. Tao, L. Chongmin, J. Mohamad Zain and A. Abdalla, "Robust Image Watermarking Theories and Techniques: A Review", *Journal of Applied Research and Technology*, Vol. 12, No. 1, pp. 122-138, 2014.