International Journal of Engineering Research and Technology.
ISSN 0974-3154 Volume 11, Number 6 (2018), pp. 897-908
© International Research Publication House
http://www.irphouse.com

Blind Colour Image Watermarking Scheme Based on Quaternion and SVD Techniques

Danube Kirt NGONGANG Wandji[1*], Elijah Mwangi[2] and Edward Ndungu [3]

[1]*Department of Electrical Engineering, Pan African University, Nairobi, Kenya*

[2]*University of Nairobi, Kenya*

[3]*Jomo Kenyatta university Agriculture and Technology, Kenya*

Abstract

In this paper a blind watermarking scheme for colour images using SVD and Arnold scrambling is proposed. The host image is initially divided into non-overlapping blocks and SVD is applied to each individual block. In order to address the issue of colour loss information, a matrix of the host image is formed to represent the RGB components. Then insertion of the watermark in the host image is demonstrated. The robustness of the scheme has been proved through a series of image processing attacks. The issue of watermark security is addressed by the use of the Arnold transform.

INTRODUCTION

The fast development of the World Wide Web within the past few years has increased the supply of digital products like audio, images, text and videos to the public. Presently, technology has made the transmission of data much more accessible than it was a few years ago. Despite a boon in digital data transmission due to high speed, low cost, easy editing of digital data, it has also become a bane due to illegal copies. Digital watermarking is an important and effective technique then can be employed to solve the problems caused by illegal operations [1]. There are three key requirements for the digital image watermarking in terms of copyright protection. The first one is robustness. This is the ability of a watermark to be extracted with some level of accuracy despite some attacks performed on the watermarked image. The second is the distortion introduced in the process of embedding. The main idea of the watermarking is to embed additional information into the media without affecting its visual quality. Lastly, is the security of the watermark detection and retrieval. This is achieved by the use of a secret key.

In the past 20 years, many watermarking methods have been developed [2],[3],[4]. The watermark information is found in various formats such as random numbers, recognizable binary pattern and images. Some of the recent techniques are reported in literature [5],[6],[7]. For example the work of Narula et al. (2015) [8], they proposed two watermarking approaches DWT and DWT–SVD which are applied to ensure image content security and watermark robustness. After that they applied both watermarking approaches and compared values of peak signal to noise ratio (PSNR). Experimental results showed that the hybrid DWT–SVD is much better than DWT approach alone. The quality of the watermarked image degraded significantly when using DWT approach watermark embedding in comparison to DWT–SVD. Vaishnavi and Subashini (2015) [9] proposed a scheme which is based on the embedding of the watermark on the blue colour channel elements. Then the watermark is embedded on the blue colour channel of the host image as a result of the application of SVD technique.

In this paper, a blind watermarking scheme for colour image using Singular Values Decomposition and Arnold scrambling is proposed. In this proposed method, the embedded watermark can be extracted in a blind manner. Further processes could be applied to the host image and watermark image without losing colour information to achieve better invisibility and stronger robustness against signal processing attacks.

The rest of the paper is organized as follow: A short review of the theory of SVD and the Arnold transform is given in section 2, section 3 explains in details the methodology of the scheme and then some experimental results, discussions and performance comparison are presented in section 4. The conclusion is drawn in section 5.

1 THEORETICAL CONCEPTS

1.1 SINGULAR VALUE DECOMPOSITION

Singular Value decomposition (SVD) is an effective method for extracting algebraic features that enable the extraction of image features by factorization of the image matrix.

Consider the image matrix A ε R^{mxn}, there exists an orthogonal matrix such that :

U = $[u_{1,}\, u_{2\,\ldots}\, u_m]$ ε R^{mxn},V = $[v_{1,}\, v_{2,,\ldots\ldots}\, v_n]$ ε R^{mxn}, such that :

$$A = Udiag(\sigma_1, \sigma_2, \ldots\ldots\ldots \sigma_P)V \qquad (1)$$

$$S = diag(\sigma_1, \sigma_2, \ldots\ldots\ldots \sigma_P) \qquad (2)$$

$\sigma_1 \geq \sigma_2 \geq \ldots\ldots\ldots \geq \sigma_P \geq 0$, σ_i is the singular value of A, u_i and v_i are the left and right singular vectors of $\sigma_{i.}$

This means:

$$\text{SVD (A) = [U S V]} \qquad (3)$$

1.2 ARNOLD SCRAMBLING

Arnold scrambling algorithm has the feature of simplicity and periodicity, so it is used widely in the digital watermarking technology [10]. In the proposed watermarking algorithm, the 2D Arnold scrambling transformation is used which shuffles the pixel positions of the watermark image as follows:

$$\begin{bmatrix} \tilde{x} \\ \tilde{y} \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} mod\ N \quad = A \begin{bmatrix} x \\ y \end{bmatrix} mod\ N \quad (4)$$

$$\begin{bmatrix} x \\ y \end{bmatrix} = A^{-1} \begin{bmatrix} \tilde{x} \\ \tilde{y} \end{bmatrix} mod\ N \quad = A^{-1} \begin{bmatrix} \tilde{x} \\ \tilde{y} \end{bmatrix} mod\ N \quad (5)$$

The digital image can be seen as a two-dimensional matrix. When the size of the image is N, with $N \times N$ elements, the subscript x, y stand for the position of pixel, $x, y \in \{0, 1, 2..., N\text{-}1\}$. Each pair (x, y) becomes $\tilde{x}$ and $\tilde{y}$ after Arnold scrambling. Which is equivalent to the original image of the point from (x, y) moving to $(\tilde{x}\ , \tilde{y})$. The movement of pixels in the image, traverses all the points to complete a picture of the Arnold scrambling.

According to the periodicity of Arnold scrambling, the original image can be restored after several iterations, which is presented in Figure 1. The recovery of the image is function of its size. From figure 1 the scrambling times 192 corresponds to the number of iterations required to unscramble an image whose size is 256 x 256. It is therefore evident to infer that the scrambling times strongly depends on the size of the image.

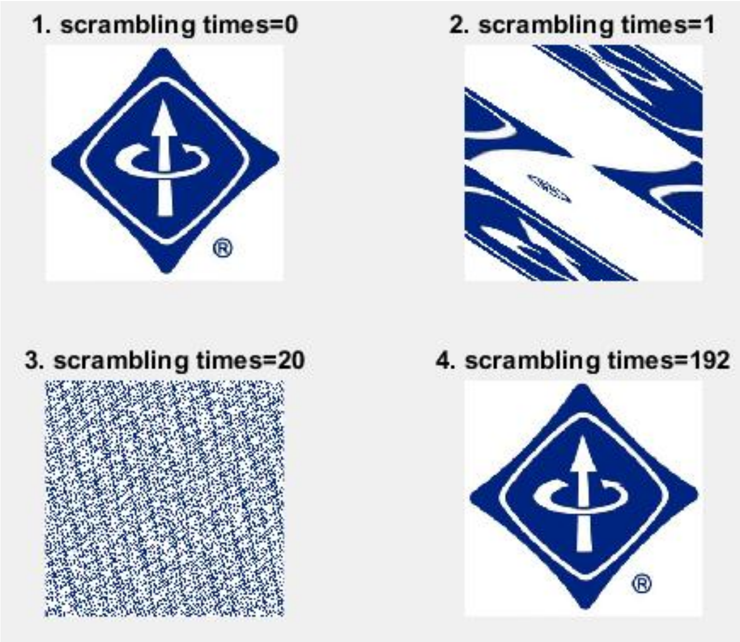


Figure 1. The scrambling technique applied to the watermark

2 THE PROPOSED METHOD

The proposed method is a two stage process: In the first stage the watermark embedding is performed and second stage the watermark extraction.

2.1 WATERMARK EMBEDDING

An original host image A is a RGB colour image of size *N*x*N* where N = 2^n and watermark image W is also a RGB colour image of size *M*x*M*, where M = 2^m and *N*≥ *3M; m* and *n* are the corresponding bit images of ~ the watermark and the host image respectively.

Step i Colour watermark preprocessing

In the process of applying the scrambling technique, the pixel position in an image is randomly changed to produce the meaningless image that is used for the embedding purpose on the host image. The scrambling factor used to generate the meaningless image is 5.

Step ii Partition

The original RGB host image is divided into non-overlapping blocks A_{ij} of size *dxd* pixels. Where $d = N/M$. The original image is partitioned in such a way to account for the size of the watermark image.

Step iii Pixel blocks rearranging

Components of the blocks A_{ij} are rearranged as rectangular matrices C_{ij} of *3dxd*.

Step iv performing the SVD

Perform the SVD for $C_{ij:}$ $C_{ij} = U_{ij}\sum_{ij}V^T{}_{ij}$ where $\sum_{ij} = \mathrm{diag}\,(\sigma_1{}^{(ij)}, \sigma_2{}^{(ij)}, \sigma_3{}^{(ij)}, \ldots\ldots \sigma_d{}^{(ij)})$

Step v Embedding

The embedding of the watermark is carried out simply by replacing the last three values of the diagonal matrix by the component values of the three colour components of the watermark. The last three values correspond to the number of colour plane in the host image that need to be replaced by the colour component of the watermark.

$$\tilde{\sum}_{ij} = \mathrm{diag}\,(\sigma_1{}^{(ij)}, \sigma_2{}^{(ij)}, \sigma_3{}^{(ij)} \ldots \sigma_{d-3}{}^{(ij)}, \alpha\, \tilde{W}_{ij}{}^{R}, \alpha\, \tilde{W}_{ij}{}^{G}, \alpha\, \tilde{W}_{ij}{}^{B}) \qquad (6)$$

Where α is a scaling factor

$\alpha\tilde{W}_{ij}{}^{R} = \sigma_{d-2}{}^{(ij)}$

$\alpha\tilde{W}_{ij}{}^{G} = \sigma_{d-1}{}^{(ij)}$

$\alpha\tilde{W}_{ij}{}^{B} = \sigma_{d}{}^{(ij)}$

and where $\tilde{W}_{ij}{}^{R}$, $\tilde{W}_{ij}{}^{G}$, $\tilde{W}_{ij}{}^{B}$ are the red, green and blue component of the watermark W and α is the scaling factor

form $\tilde{C}_{ij} = U_{ij}\tilde{\sum}_{ij}V^T{}_{ij}$ and obtain $\tilde{A}_{ij}$ the watermarked image.

2.2 WATERMARK EXTRACTION

Extraction procedure

The watermark should be extracted and compared to the original in order to evaluate for the robustness and visual quality of the algorithm. The singular value decomposition is an effective method for extracting algebraic features that enable the extraction of images features by factorization of the image matrix.

Step i Division into blocks

Only the watermarked image $\tilde{A}_{ij}$ is divided into non-overlapping blocks of size d x d pixels respectively where $i,j = 1,2,3,\ldots\ldots M$. and d = N/M. This is achieved in order to highlight the blind property of the watermarking algorithm.

Step ii Re-arrangement of the matrices

The *R*, *G*, and *B* color components of $\tilde{A}_{ij}$ are rearranged as rectangular matrices $\tilde{C}_{ij}$ of $3d \times d$.

Step iii Perform the SVD for Cij :

$\tilde{C}_{ij} = U_{ij}\sum_{ij}V^{T}_{ij}$ and $\sum_{ij} =$ diag(diag $U^{T}ij\tilde{C}_{ij}V_{ij}$) = diag ($\sigma_1^{(ij)}$, $\sigma_2^{(ij)}$, $\sigma_3^{(ij)}$ … $\sigma_d^{(ij)}$).

Step iv Watermark extraction

$W_{ij}^{R} = (\tilde{\sigma}_{d-2}^{(ij)} / \alpha)$

$W_{ij}^{G} = (\tilde{\sigma}_{d-1}^{(ij)} / \alpha)$

$W_{ij}^{B} = (\tilde{\sigma}_{d}^{(ij)} / \alpha)$

Step v Arnold scrambling reversion

Once the watermark has been extracted, the security key has to be recognized in order to reconstruct the meaningless watermark image into a meaningful one by applying the inverse of the Arnold Scrambling technique. The inverse Arnold is applied to rearrange the pixels back into the original position.

3 EXPERIMENTAL RESULTS AND DISCUSSIONS

In this section the parameters used to evaluate the performance of the algorithm are presented. The second subsection introduces the visual results of the proposed algorithm. The third subsection presents a comparison to results obtained study with the existing results that were obtained by other techniques reported in the literature.

EVALUATION CRITERIA

The performance of our proposed scheme was evaluated using two main measures: PSNR (*peak signal-to-noise ratio*) and the NC (*Normalized correlation*). The visual fidelity can be measured using PSNR of the watermarked image. The PSNR is expressed in decibel (dB) and is defined in equation (7) as:

$$\text{PSNR} = \frac{3N^2[maxA(x,y,k)]^2}{\sum_{x=1}^{N}\ \sum_{y=1}^{N}\sum_{k=1}^{3}[A(x,y,k)-\tilde{A}(x,y,k)]^2} \qquad (7)$$

Where $maxA(x,y,k)$ represents the maximum pixel value of the colour image, and here it is 255. $A(x,y,k)\ and\ \tilde{A}(x,y,k)$ are the pixel values location at position (x, y, and k) in the original host image and the watermarked image, respectively. A higher PSNR generally indicates that the reconstruction of the watermarked image is of higher quality.

In order to perform an objective evaluation of the extracted watermark, the normalized correlation measure is employed. A higher NC simply means that there is close resemblance between both images. The measurement of the quality of the extracted watermark will carried out using the normalized correlation which is defined in equation (6):

$$\text{NC}= \frac{\sum_{x=1}^{N}\ \sum_{y=1}^{N}\sum_{k=1}^{3} W(x,y,k)*\widetilde{W}(x,y,k)]}{\sqrt{\sum_{x=1}^{N}\ \sum_{y=1}^{N}\sum_{k=1}^{3} W^2(x,y,k)}\sqrt{\sum_{x=1}^{N}\ \sum_{y=1}^{N}\sum_{k=1}^{3} \widetilde{W}^2(x,y,k)}} \qquad (8)$$

3.1 SIMULATION RESULTS IN THE ABSENCE OF ATTACKS

The results achieved using the proposed watermark embedding algorithm in the absence of attacks are shown in Table 1. Using the first experiment, the three sample images of size *1024* x *1024* were taken as host image and the watermark logo of size *128* x *128* with a watermarking scaling factor *α = 0.05* which had achieved the highest PSNR values with different benchmark images.. From Table 1, it is clearly observed that the watermark is imperceptible and by a subjective approach there is no visible differences between the original host image and the watermarked image after the embedding of the watermark.

Table 1. The experiment results in the absence of attacks

1024X1024	Lena	Mandrill	Barbara
PSNR(dB)	41.41	41.59	41.69
NC	99.98%	99.99%	99.99%

In the second experiment, Barbara colour image of size *1024* x *1024* was considered as host image, with the scrambled watermark of size *128* x *128* after 10 fold Arnold transformation. The detail of the implementation is highlighted in figure 2. The figure (2) highlights the embedding and extraction results of the watermark logo and watermarked image. The figure (2-c) shows the meaningless watermark achieved using 10 fold pixels iterations and the recovery in order to ensure a similarity with the original logo.

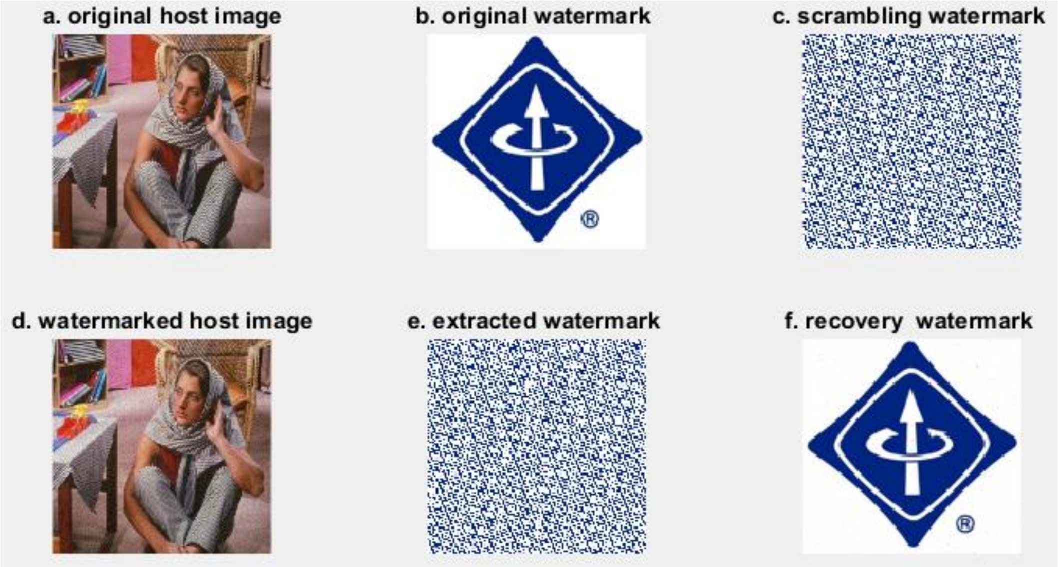


Figure 2: 1024 x 1024 Barbara host image with scale factor 0.05

3.2 SIMULATION RESULTS WITH VARIOUS ATTACKS

Some sets of experiments were carried out in order to evaluate the robustness of the proposed algorithm. The simulation of the attacks for signal processing, were done under various conditions. These are:

i. Salt and Pepper
ii. Histogram modification
iii. Gaussian filtering
iv. Speckle noise

The results obtained with each of these attacks are presented in this section.

Table 2. Shows the performance of the scheme in image under Salt and Pepper noise with different density (0.002, 0.005, and 0.01). It was clearly observed that despite the watermarked image attacked with Salt and Pepper noise with a factor of 0.01, the NC's of the extracted watermark is 95.48% which shows that the algorithm has an effective performance in resisting this type of attacks. For a factor greater than 0.01 it was very impossible to recover the watermark, the resulting image was completely blurred.

Table 2. Experiment results being attacked by Salt and pepper Noise.

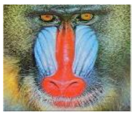
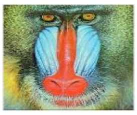
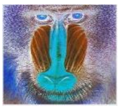
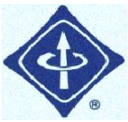
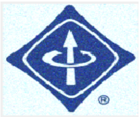
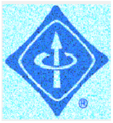
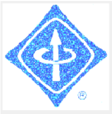
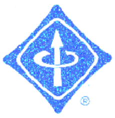
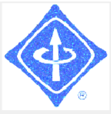
MANDRILL	GAUSSIAN FILTERING	HISTOGRAM MODIFICATION	SPECKLE NOISE
Original			
Watermarked under attack			
PSNR(dB)	23.79	22.46	3.20
Extracted logo			
NC	99.57%	99.60%	95.38%

Table 3. Experiments results being attacked by Gaussian filtering, Histogram modification and Speckle noise.

MANDRILL	Salt & pepper 0.01	Salt & Pepper 0.005	Salt & pepper 0.002
The watermarked colour image			
Watermarked attacked			
PSNR(dB)	19.80	22.03	25.88
The watermark extracted			
NC	95.48%	96.02%	96.54%

From Table 3, the proposed watermarking algorithm shows some good performance as a result of attacks on the watermarked image. The PSNR of the attacked image with speckle noise is as low as 3.2 dB, the algorithm was able to extract a watermark of 95.38%. It shows that despite the deep alteration of the watermarked image, the scheme was able to reconstruct a watermark close to the original one. The Gaussian filtering was also attacked to the watermarked image, an extraction of the watermark of 99.57% was achieved which shows a good performance of the watermarking algorithm. The method has the capability to resist histogram modification and Gaussian filtering attacks. In other words, the difference between the extracted watermark and the original watermark is 0.4% with a PSNR of 22.46 dB.

Table 4: PSNR watermarked image values after attacks

Image	Gaussian filtering	Salt and pepper(0.01)	Histogram	Rotation(180^0)
Foggysf1	29.88	19.69	29.88	0.91
pears	35.95	20.54	16.44	8.19
peppers	34.74	19.80	34.74	7.05
Onion	35.85	19.80	30.29	4.22
Toysflash	31.88	19.28	31.88	5.20
Office_4	32.87	20.01	32.87	4.9

Table 5: NC watermarked image values after attacks

Image	Gaussian filtering	Salt and pepper(0.01)	Histogram	Rotation(90^0)
Foggysf1	99.90	90.89	99.90	96.13
pears	99.91	90.77	99.49	96.15
peppers	99.69	90.80	99.69	95.95
Onion	99.39	90.39	99.25	95.59
Toysflash	99.61	91.03	99.61	95.91
Office_4	99.70	90.87	99.70	96.09

Table 4 gives the PSNR of watermarked images under attacks like Gaussian filtering, Histogram Modification, Salt and Peppers of density 0.01 and Rotation of angle 90^0. Table 5 gives the NC of the watermark. A larger sets of image was selected to prove the validity of the proposed algorithm like Foggysf1, pears, peppers, Onion, Toysflash and Office_4

Table 6. Performance Comparisons between the proposed algorithm and others

Performance comparisons	Yan et al.[11]	Tao Wang [12]	Yudit et al. [13]	Proposed scheme
processing domain	SVD domain and wavelet	SVD domain	2-level wavelet and SVD domain	SVD Domain
Blind watermarking method	NO	YES	NO	YES
Robustness	High	High	High	Very high
Embedding quality	High	Very high	good	excellent

The comparison of the proposed watermarking scheme with three similar watermark schemes in Table 6 highlights the fact that neither extra data nor the original host image is required during the extracted procedure, also the embedding procedure is achieved using the three colour bands of the watermark and host image to avoid loosing of colour information along the watermarking process.

Yan et al. can provide high image quality but relatively high robustness. Under similar attacks (Salt &pepper, Gaussian filtering) the scheme has shown higher robustness due to the higher value of NC. Their scheme cannot be applied to colour image.

Tao Wang successfully used the blind property for the extraction of the gray scale image watermark. Under Gaussian filtering and Salt & pepper attacks the robustness was found to be NC = 85.43%, NC = 87.85 % which is lower than the values of the proposed scheme was able to achieve NC = 99.57% and NC = 95.48%.

Yudit et al. were able to optimize the trade-off between imperceptibility and robustness. Their method requires both the original image and original watermark image during extraction of the watermark colour image. But based on their recorded values of different attacks, the proposed algorithm shows better performance and higher robustness.

4 CONCLUSION

Based on the experimental results that have been tested on the proposed watermarking scheme, it was clearly established that indicators of the imperceptibility and the robustness demonstrate a good performance on the watermarked image. Also the value of NC without attack obtained is 99.99%, this shows the high efficiency of the extraction algorithm. The effectiveness of the scheme has been proved through a series of experiments to evaluate the robustness against several possible image attacks such as Gaussian filtering, Salt and Pepper noise, speckle noise and Histogram modification. The proposed algorithm has shown better results in achieving watermarked images with better PSNRs. High NC can be obtained despite the deep attack (Speckle noise) of the watermarked image, which shows that the proposed algorithm is robust. Specifically it has demonstrated effective robustness against Gaussian filtering, Salt and Pepper noise attack.

REFERENCES

1. Battiato, S., et al., *Multimedia in forensics, security, and intelligence.* IEEE MultiMedia, 2012. **19**(1): p. 17-19.
2. Bailey, K. and K. Curran, *An evaluation of image based steganography methods.* Multimedia Tools and Applications, 2006. **30**(1): p. 55-88.
3. Cheddad, A., et al., *Digital image steganography: Survey and analysis of current methods.* Signal processing, 2010. **90**(3): p. 727-752.
4. Langelaar, G.C., I. Setyawan, and R.L. Lagendijk, *Watermarking digital image and video data. A state-of-the-art overview.* IEEE Signal processing magazine, 2000. **17**(5): p. 20-46.
5. Su, Q., et al., *Color image blind watermarking scheme based on QR decomposition.* Signal Processing, 2014. **94**: p. 219-235.
6. Li, Y., et al., *A new double color image watermarking algorithm based on the SVD and Arnold scrambling.* Journal of Applied Mathematics, 2016. **2016**.
7. Rastegar, S., et al., *Hybrid watermarking algorithm based on singular value decomposition and radon transform.* AEU-International Journal of Electronics and Communications, 2011. **65**(7): p. 658-663.
8. Narula, N., D. Sethi, and P.P. Bhattacharya, *Comparative analysis of DWT and DWT-SVD watermarking techniques in RGB images.* International Journal of Signal Processing, Image Processing and Pattern Recognition, 2015. **8**(4): p. 339-348.
9. Vaishnavi, D. and T. Subashini, *Robust and invisible image watermarking in RGB color space using SVD.* procedia computer science, 2015. **46**: p. 1770-1777.
10. Al-Gindy, A., et al. *A high capacity digital watermarking technique for the authentication of colour images*. in Signal Processing and Information Technology (ISSPIT), 2009 IEEE International Symposium on Ajman, United Arab Emirates.December 2009. IEEE.
11. Y. Dejun, Y. Rijing, L. Hongyan, Z. Jiangchao, "*A digital watermarking scheme based on singular value decomposition and discrete wavelet transform*," international conference on computer science and network technology, pp.154-157, December 2011, Harbin, China.
12. T. Wang, "*Digital Image Watermarking Using Dual-Scrambling and Singular Value Decomposition*" in Computational Science and Engineering (CSE) and Embedded and Ubiquitous Computing (EUC), 2017 IEEE International Conference on july 2017 Guangzhou, China.

13. Y. Arum, D. Rosal, C. Atika, E. Hari, M. Muljono , "*Non-blind RGB image watermarking technique using 2-level discrete wavelet transform and singular value decomposition*," International conference on information and communications technology(ICOIACT), , pp.623 – 627, April 2018 Yogyakarta, Indonesia