Journal of Engineering and Applied Sciences 14 (16): 5762-5768, 2019
ISSN: 1816-949X

A Digital Image Watermarking Scheme based on Discrete Cosine Transform

Ghazwan Jabbar Ahmed, Adel Jalal Yousif and Fadhil Kadhim Zaidan
Electronic Computing Center, University of Diyala, Diyala, Iraq

Abstract: In this research, a grayscale image watermarking scheme is proposed using a Discrete Cosine Transform (DCT) to embed a binary invisible watermark image. The DCT is applied to the entire host image instead of dividing the image into 8×8 non-overlapping blocks as usual in the conventional schemes and then some of the coefficients in the low-frequency DCT band are selected for the watermark embedding process. For obtaining an acceptable trade-off between the robustness and imperceptibility of the watermark, the watermarking strength is controlled by a robustness factor. The value of the robustness factor is not threshold and can be changed by the user based on the required robustness level and the characteristics of the host image. Peak Signal to Noise Ratio (PSNR) and Normalized Correlation (NC) are calculated to evaluate the images quality. The simulations and results demonstrate that the proposed scheme still holds its validity under various attacks such as JPEG compression, low-pass filtering and noise attacks.

Key words: Discrete cosine transform, digital watermarking, copyright protection, JPEG compression, watermarking techniques, normalized correlation, robustness and imperceptibility

INTRODUCTION

With the growing development of computers and network technologies, digital multimedia such as image, audio and video can now be created and distributed through the internet simply and quickly. Copyright protection has become a challenging issue due to the possibility of illegal alteration and unlimited copying. One of the most effective solutions is the use of digital watermarking techniques. Digital watermarking refers to the process of embedding some information (which is known as watermark) into the digital multimedia content in some way, so that, it can be extracted or identified later for various purposes such as content authentication, copyright protection, data integrity detection, ownership verification, etc. (Abdullatif *et al*., 2013).

Depending on human perception, the digital watermarking can be classified into two main categories namely, visible watermarking and invisible watermarking, the second category is considered in this research. In case of visible watermarking, the inserted watermark is intentionally visible to the human eye in the host image to show some important information such as TV channel logo or company logo. Whereas the invisible watermark is embedded in a secret location and can be extracted only by authorized persons in such a way preserving the perceptual content of the watermarked image similar to the original image (Yusnita and Khalifa, 2007; Giri *et al*., 2015).

The essential parameters that determine the efficiency of the invisible watermarking scheme are robustness and imperceptibility. The robustness of a watermark can be defined as its ability to resist any unintentional attacks such as signal processing operations or intentional attacks. While the imperceptibility of a watermark means that the difference between the watermarked and the original images should be unnoticeable by human eyes (Huynh-The *et al*., 2016). The digital watermarking can be implemented by spatial domain or transform domain. The principle of spatial domain algorithms is to embed a watermark into an image by directly altering the values of certain pixels in the cover image (Islam and Chong, 2014). Whereas in the transform domain, the watermark is embedded into the transformed coefficients of the host image by using the transformed algorithms such as Discrete Cosine Transform (DCT) (Kumar and Anuradha, 2014), Discrete Wavelet Transform (DWT) (Gunjal and Mali, 2011) or other transform domain algorithm. The transform domain techniques have several advantages over the spatial domain techniques. It has more robust watermarking and more control of imperceptibility which make it an attractive choice as demonstrated by various surveys (Sinha *et al*., 2014; Parashar and Singh, 2014; Malshe *et al*., 2012). In this research, the transform domain is employed in the design of the proposed watermarking technique by using the DCT algorithm.

MATERIALS AND METHODS

Discrete cosine transform: Discrete Cosine Transform (DCT) is basically an orthogonal transformation which is

Corresponding Author: Ghazwan Jabbar Ahmed, Electronic Computing Center, University of Diyala, Diyala, Iraq

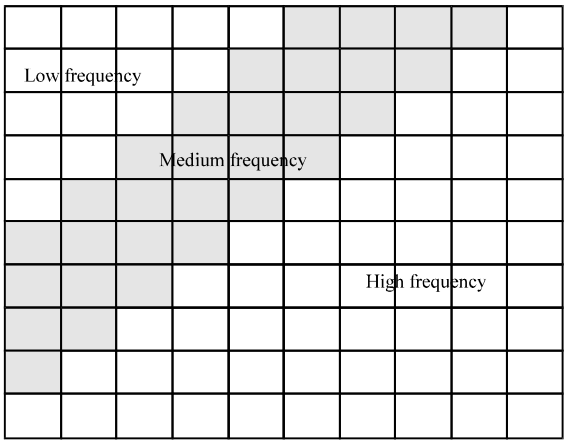

Fig. 1: DCT bands regions

used to transform a signal from the spatial domain to the frequency domain. The essential feature of the DCT is to collect the vast majority of the signal information in a few low-frequency components and ignoring the part that the human eye is least sensitive to. Additionally, DCT has a number of good features that make it one of the most commonly used tools in transformation domain such as strong energy compaction, moderate of complexity, less bit error rate and others (Ram, 2013; Eswaraiah *et al*., 2012). Thus, DCT tends to reduce the signal information by removing the redundant data of the transformed signal. Generally, the DCT divide the image into three different bands of frequencies namely low, medium and high-frequency band as shown in Fig. 1. The coefficient in the top-left represents the DC component and the others stand for AC components (Santhi and Thangavelu, 2011; Singh *et al*., 2013). In this research, the watermark is inserted in the low-frequency band to increase the robustness of the watermarking scheme (Mishra *et al*., 2015; Chen and Huang, 2008). For an image of size (M×N), the 2-Dimensional Discrete Cosine Transform (2D-DCT) and Inverse Discrete Cosine Transform (2D-IDCT) are defined as follows (Chen and Huang, 2008):

$$F(u,v) = c(u)c(v)\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)\cos\frac{\pi(2x+1)}{2M}\cos\frac{\pi(2y+1)}{2N} \quad (1)$$

$$c(u) = \begin{cases} \sqrt{1/M} & u=0 \\ \sqrt{2/M} & u=1,2,3,\ldots,M \end{cases} \quad (2)$$

$$v = 0$$

$$c(v) = \begin{cases} \sqrt{1/N} \\ \sqrt{2/N} \end{cases} v = 1, 2, 3, \ldots, N \quad (3)$$

$$f(x,y) = \sum_{u=0}^{M-1}\sum_{v=0}^{N-1} c(u)c(v)F(u,v)\cos\frac{\pi(2x+1)u}{2M}\cos\frac{\pi(2y+1)v}{2N} \quad (4)$$

Proposed scheme: In this research, a watermarking scheme is proposed to insert a binary watermark image into a grayscale image in transform domain by using the DCT algorithm. The DCT is performed to the entire image and the low-frequency band is employed for embedding the binary bits of the watermark by choosing the most significant coefficients excluding the DC term which is located at the position (0, 0) in the coefficients matrix. The algorithms of watermark embedding and extraction are presented below.

Watermark embedding algorithm: The procedure of the watermarking embedding process is summarized by the following steps:

- Reading the original grayscale image f with the size M×N and the binary watermark image with the size q×r
- Performing the DCT to the entire M×N image f to obtain the coefficients matrix denoted by F
- Choosing the (n) maximum coefficients $C_{max} = \{c_1, c_2, \ldots, c_n\}$ from the matrix F excluding the DC term where: $n = q \times r$, $C_{max} \in F$
- Embedding an element W (i, j) of the watermark using the chosen coefficients of C_{max} by applying the following Eq. 5:

$$c'_k = c_k * (1+t*\delta) \quad (5)$$

where, c'_k and c_k represent the watermarked and the original coefficients, respectively. K = 1, 2, 3, ..., n:

$$t = \begin{cases} 1, & W(i,j) = 0 \\ -1, & W(i,j) = 1 \end{cases} \quad (6)$$

where, $1 \le i \le q$, $1 \le j \le r$, δ represents the watermarking strength which is discussed. Performing the inverse DCT to the modified matrix coefficients to obtain the watermarked image. Figure 2 illustrates the watermark embedding algorithm.

Watermark extraction algorithm: The procedure of the watermarking extraction process is summarized by the following steps: Reading the watermarked f′ image and also the original image f. Performing the DCT to the entire watermarked image (f′) and the original image (f) to produce the coefficients matrices F′ and F, respectively. Selecting the (n) watermarked DCT coefficients $C'_w = \{c'_{w1}, c'_{w2}, \ldots, c'_{wn}\}$ from F′ that have the same position of the original DCT coefficients $C_{max} = \{c_1, c_2, \ldots, c_n\}$ in matrix:

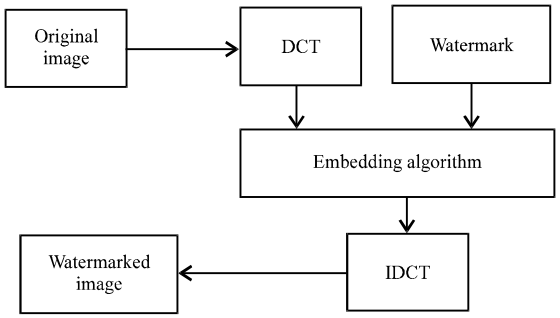

Fig. 2: Watermark embedding algorithm

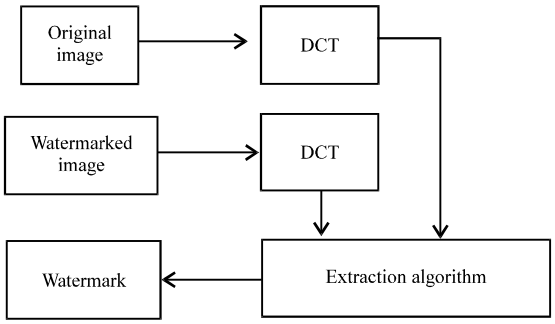

Fig. 3: Watermark extraction algorithm

$$\text{let } d_k = (c'_{wk} / c_k)\text{-}1 \tag{7}$$

where, k = 1, 2, 3, ..., n. Extracting the watermark W^e by making the judgment of d_k:

$$W^e(i, j) = \begin{cases} 0, d_k > 0 \\ 1, d_k \le 0 \end{cases} \tag{8}$$

where, $1 \le i \le q$, $1 \le j \le r$. Figure 3 illustrates the watermark extraction algorithm.

RESULTS AND DISCUSSION

The performance of the watermarking techniques is usually evaluated by measuring both properties of robustness and imperceptibility. In this study, 3 widely known grayscale images: Boats, Baboon and Goldhill with the size of (512×512) are taken to be the cover images for inserting binary watermark image with the size of (30×40) as shown in Fig. 4.

The robustness of the proposed watermarking scheme is evaluated by analyzing the watermarking strength under the commonly used signal processing operations such as JPEG compression with various Quality Factors (QF) and low-pass filtering in addition to the noise attacks. The Normalized Correlation (NC)

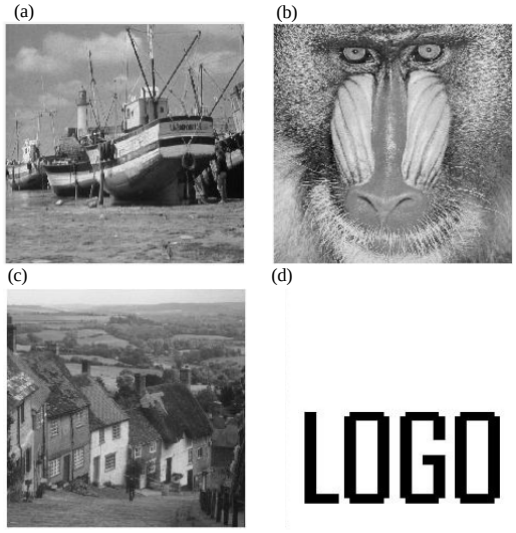

Fig. 4: Test images; a) Boats; b) Baboon; c) Goldhill and d) Watermark

criterion is used to estimate the watermark robustness by calculating the degree of similarity between the original watermark (W) and the extracted one W^e. When the value of the normalized correlation is 1, the extracted watermark is exactly like the original one. This value decreases as the difference between the two images increases as defined by the following Eq. 9, (Jawad *et al*., 2014):

$$NC = \frac{\sum_{i=1}^{q}\sum_{j=1}^{r}\left(W(i, j) \times W^e(i, j)\right)}{\sum_{i=1}^{q}\sum_{j=1}^{r}\left(W(i, j)\right)^2} \tag{9}$$

The imperceptibility of the proposed watermarking scheme is evaluated by measuring the visual quality of the watermarked image by using the Peak Signal to Noise Ratio (PSNR) criterion. The high value of PSNR means high level of watermark imperceptibility in the cover image. The following equation describes the PSNR (Jawad *et al*., 2014):

$$PSNR = 10\log_{10}\left(\frac{225^2}{MSE}\right) \tag{10}$$

where, MSE is given by:

$$MSE = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N}\left(1(x,y)\text{-}1'(x,y)\right)}{M \times N} \tag{11}$$

In general, the robustness and imperceptibility requirements affect each other in reverse. In other words,

the high robustness watermarking can be achieved but the imperceptibility will be degraded due to the added signal and vice versa. Therefore, watermarking techniques should balance between the robustness and imperceptibility requirements. In this research, the watermarking strength is controlled by a factor (δ) which is represent the robustness factor to achieve the required balance between the robustness and imperceptibility. So, high level of robustness can be achieved by increasing the value of (δ) but at the same time the watermarked image quality will be decreased and vice versa. In addition, the value of (δ) can be changed by the user based on the desired robustness level and the characteristics of the host image. The effect of changing the robustness factor value on the watermarked boats image is shown visually in Fig. 5.

Table 1 and 2 show arithmetically the effect of changing the value of on the performance of the proposed

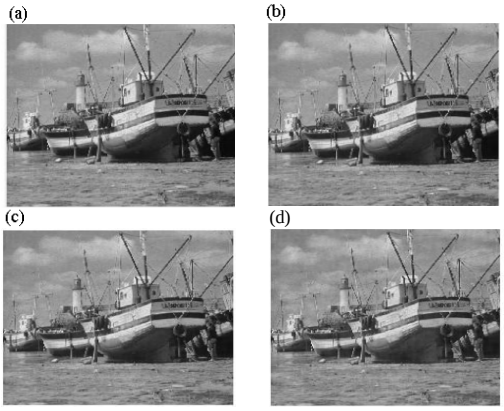

Fig. 5: a) Original boats image; b) δ = 0.05, PSNR = 41.53; c) δ = 0.1, PSNR = 35.51 and d) δ = 0.2, PSNR = 29.49 watermarked Boats image with different value of δ

Table 1: Performance analysis with low-pass filtering and JPEG compression attacks

	No attack		Average filter (3×3)		Median filter (3×3)		JPEG (QF = 20) compression		JPEG (QF = 40) compression		JPEG (QF = 60) compression	
Images/δ	PSNR	NC	PSNR	NC	PSNR	NC	PSNR	NC	PSNR	NC	PSNR	NC
Boats												
0.01	55.51	1.0000	28.84	0.9137	30.95	0.7108	30.47	0.6155	32.72	0.7152	34.16	0.7522
0.05	41.53	1.0000	28.59	0.9742	30.64	0.9507	30.15	0.8890	32.20	0.9798	33.46	1.0000
0.1	35.51	1.0000	27.95	0.9798	29.73	0.9966	29.29	0.9776	30.91	1.0000	31.79	1.0000
0.15	31.99	1.0000	27.07	0.9798	28.53	1.0000	28.15	0.9978	29.34	1.0000	29.96	1.0000
0.2	29.49	1.0000	26.09	0.9854	27.25	1.0000	26.95	1.0000	27.82	1.0000	28.23	1.0000
Baboon												
0.01	56.71	1.0000	22.36	0.9070	22.85	0.4888	24.64	0.6031	26.85	0.6883	28.70	0.7175
0.05	42.73	1.0000	22.32	0.9552	22.84	0.7231	24.58	0.8722	26.74	0.9854	28.54	0.9955
0.1	36.71	1.0000	22.20	0.9664	22.75	0.8890	24.39	0.9776	26.43	0.9989	28.07	1.0000
0.15	33.18	1.0000	22.01	0.9709	22.58	0.9496	24.08	0.9966	25.95	1.0000	27.38	1.0000
0.2	30.69	1.0000	21.76	0.9753	22.34	0.9753	23.68	1.0000	25.36	1.0000	26.58	1.0000
Goldhill												
0.01	53.91	1.0000	29.76	0.9316	31.62	0.6323	30.74	0.5975	32.83	0.6771	34.19	0.7007
0.05	39.93	1.0000	29.37	0.9563	31.18	0.9395	30.36	0.8475	32.21	0.9630	33.35	0.9933
0.1	33.91	1.0000	28.45	0.9675	29.97	0.9865	29.27	0.9686	30.69	0.9989	31.46	1.0000
0.15	30.39	1.0000	27.29	0.9742	28.48	0.9966	27.94	0.9955	28.93	1.0000	29.43	1.0000
0.2	27.89	1.0000	26.07	0.9776	26.98	0.9989	26.60	1.0000	27.28	1.0000	27.61	1.0000

Table 2: Performance analysis with different noise attacks

	Gaussian noise (μ = 0, ν = 0.001)		Gaussian noise (μ = 0, ν = 0.005)		Salt and pepper (0.5%)		Salt and pepper (1%)		Speckle noise (0.5%)		Speckle noise (1%)	
Images/δ	PSNR	NC	PSNR	NC	PSNR	NC	PSNR	NC	PSNR	NC	PSNR	NC
Boats												
0.01	29.98	0.6771	23.03	0.5964	28.41	0.6962	25.21	0.6984	28.34	0.6300	25.35	0.6087
0.05	29.71	0.9383	23.00	0.8038	28.16	0.9383	25.23	0.8778	28.19	0.8845	25.28	0.8509
0.1	28.90	0.9966	22.77	0.9249	27.83	0.9865	24.99	0.9776	27.65	0.9899	25.01	0.9619
0.15	27.87	1.0000	22.51	0.9720	26.77	1.0000	24.69	0.9955	26.86	1.0000	24.58	0.9877
0.2	26.73	1.0000	22.11	0.9944	25.99	1.0000	24.16	0.9978	25.93	1.0000	24.01	1.0000
Baboon												
0.01	29.96	0.6626	23.03	0.6020	28.59	0.7063	25.48	0.6525	27.60	0.6312	24.61	0.6143
0.05	29.77	0.9339	22.96	0.7836	28.33	0.9159	25.27	0.8587	27.50	0.8812	24.57	0.8173
0.1	29.15	0.9955	22.82	0.9249	27.75	0.9933	25.05	0.9619	27.16	0.9854	24.39	0.9417
0.15	28.29	1.0000	22.60	0.9630	27.09	1.0000	24.72	0.9966	26.59	0.9966	24.09	0.9843
0.2	27.31	1.0000	22.32	0.9966	26.34	1.0000	24.34	1.0000	25.93	1.0000	23.70	0.9966
Goldhill												
0.01	29.98	0.6558	23.04	0.5684	28.22	0.6704	25.49	0.6513	29.39	0.6435	26.45	0.5953
0.05	29.66	0.9182	22.95	0.7769	28.08	0.9193	25.29	0.8442	29.12	0.9025	26.29	0.8229
0.1	28.72	0.9922	22.73	0.9025	27.62	0.9731	25.00	0.9596	28.35	0.9865	25.86	0.9518
0.15	27.53	1.0000	22.40	0.9742	26.78	0.9955	24.36	0.9776	27.26	0.9989	25.22	0.9944
0.2	26.27	1.0000	21.94	0.9854	25.55	1.0000	23.75	0.9978	26.09	1.0000	24.50	0.9944

Fig. 6: The watermarked boats images subjected to various attacks with the extracted logo watermark images for each: a) Average filter (3×3); b) Average filter (5×5); c) Median filter (3×3); d) Median filter (5×5); e) Gaussian noise ($\mu = 0$, $\nu = 0.002$), (f) salt and peppers noise (1%); g) Speckle noise (1%); h) JPEG compression QF = 30%; i) JPEG compression QF = 20%; j) JPEG compression QF = 10%; k) Mixed noise: salt and peppers noise (1%), Gaussian noise ($\mu = 0$, $\nu = 0.001$), Speckle noise (1%) and l) JPEG compression QF = 50% with salt and peppers noise (1%)

Table 3: Performance evaluation and comparison

		Images					
		Boats		Baboon		Gold-hill	
Attack	Parameters	PSNR	NC	PSNR	NC	PSNR	NC
No attack	-	35.51	1.0000	36.71	1.0000	33.91	1.0000
Median filter	(3×3)	29.73	0.9966	22.75	0.8890	29.97	0.9865
Median filter	(5×5)	26.70	0.9574	20.40	0.8094	27.89	0.9484
Average filter	(3×3)	27.95	0.9798	22.20	0.9664	28.45	0.9675
Average filter	(5×5)	25.05	0.9765	20.12	0.9608	26.13	0.9630
Gaussian noise	($\mu = 0, \nu = 0.003$)	24.84	0.9518	24.93	0.9596	24.76	0.9406

Table 3: Continue

		Images					
		Boats		Baboon		Gold-hill	
Attack	Parameters	PSNR	NC	PSNR	NC	PSNR	NC
Gaussian noise	($\mu = 0$, $\nu = 0.006$)	22.03	0.9182	22.08	0.9114	21.97	0.8868
Gaussian noise	($\mu = 0$, $\nu = 0.01$)	19.95	0.8565	19.96	0.8397	19.92	0.8587
Salt and peppers noise	(density = 0.01)	25.07	0.9720	25.10	0.9652	24.89	0.9518
Salt and peppers noise	(density = 0.02)	22.25	0.9372	22.26	0.9316	22.05	0.8957
Salt and peppers	(density = 0.03)	20.63	0.9036	20.49	0.9137	20.35	0.8991
Speckle noise	(density = 0.01)	24.99	0.9552	24.38	0.9395	25.86	0.9585
Speckle noise	(density = 0.02)	22.21	0.8935	21.51	0.8756	23.21	0.9025
Speckle noise	(density = 0.03)	20.55	0.8677	19.86	0.8475	21.61	0.8666
JPEG compression	(QF = 10)	27.40	0.8969	22.63	0.8823	27.61	0.8498
JPEG compression	(QF = 20)	29.29	0.9776	24.39	0.9776	29.27	0.9686
JPEG compression	(QF = 30)	30.29	1.0000	25.53	0.9978	30.14	0.9922
JPEG compression	(QF = 40)	30.91	1.0000	26.43	0.9989	30.69	0.9989
JPEG compression	(QF = 50)	31.37	1.0000	27.22	1.0000	31.07	1.0000

scheme with varied attacks. Depending on Table 1, 2 and Fig. 5, the value of the robustness factor should be carefully selected to maintain the cover image quality and the watermark strength. In this study, the selected value is ($\delta = 0.1$). Figure 5 and 6 show the extracted watermark after subjecting the watermarked boats image to various attacks including JPEG compression, low-pass filtering, and different types of noise. Performance analysis of the proposed scheme is presented in Table 3 using the test images.

CONCLUSION

An invisible watermarking scheme for grayscale images based on DCT is introduced in this study. The low-frequency region of DCT bands is utilized for embedding a binary watermark image. The watermarking strength is controlled by the user by changing the robustness factor (δ) value according the required robustness level and the characteristics of the host image. The performance of the proposed scheme is evaluated by subjecting the watermarked test images to varied attacks including average filter, median filter, speckle noise, salt and peppers noise, Gaussian noise and JPEG compression with various quality factor. The visual quality of the watermarked image is preserved and can be controlled by the robustness factor (δ) value. Additionally, the extracted watermark holds its high quality in terms of NC even under certain types of attacks. So, the employing of the low-frequency region of DCT bands improves the performance of the proposed scheme for achieving both the robustness and the imperceptibility even under different attacks.

REFERENCES

Abdullatif, M., A.M. Zeki, J. Chebil and T.S. Gunawan, 2013. Properties of digital image watermarking. Proceedings of the 2013 IEEE 9th International Colloquium on Signal Processing and its Applications, March 8-10, 2013, IEEE, Kuala Lumpur, Malaysia, ISBN:978-1-4673-5608-4, pp: 207-210.

Chen, W.Y. and S.Y. Huang, 2008. Digital watermarking using DCT transformation. Electron. Eng., 1: 173-184.

Eswaraiah, R., S.A. Edara and E.S. Reddy, 2012. Color image watermarking scheme using DWT and DCT coefficients of R, G and B color components. Intl. J. Comput. Appl., 50: 38-41.

Giri, K.J., M.A. Peer and P. Nagabhushan, 2015. A robust color image watermarking scheme using discrete wavelet transformation. Intl. J. Image Graphics Signal Process., 1: 47-52.

Gunjal, B.L. and S.N. Mali, 2011. Comparative performance analysis of DWT-SVD based color image watermarking technique in YUV, RGB and YIQ color spaces. Intl. J. Comput. Theor. Eng., 3: 714-719.

Huynh-The, T., O. Banos, S. Lee, Y. Yoon and T. Le-Tien, 2016. Improving digital image watermarking by means of optimal channel selection. Expert Syst. Appl., 62: 177-189.

Islam, S. and U.P. Chong, 2014. A digital image watermarking algorithm based on DWT DCT and SVD. Intl. J. Comput. Commun. Eng., 3: 356-360.

Jawad, M.M., E.H. Ali and A.J. Yousif, 2014. A fuzzy random impulse noise detection and reduction method based on noise density estimation. Intl. J. Sci. Eng. Res., 5: 455-468.

Kumar, A. and Anuradha, 2014. A novel watermarking algorithm for color images based on discrete wavelet transform. Intl. J. Comput. Electr. Eng., 6: 303-306.

Malshe, S., H. Gupta and S. Mandloi, 2012. Survey of digital image watermarking techniques to achieve robustness. Intl. J. Comput. Appl., 45: 1-8.

Mishra, B.P., H.N. Pratihari and P. Das, 2015. DCT based grey scale still image watermarking using 1-D walsh code and biometric protection. Intl. J. Emerging Trends Technol. Comput. Sci., 4: 28-32.

Parashar, P. and R.K. Singh, 2014. A survey: Digital image watermarking techniques. Intl. J. Signal Image Process. Pattern Recognit., 7: 111-124.

Ram, B., 2013. Digital image watermarking technique using discrete wavelet transform and discrete cosine transform. Intl. J. Advancements Res. Technol., 2: 19-27.

Santhi, V. and A. Thangavelu, 2011. DC coefficients based watermarking technique for color images using singular value decomposition. Intl. J. Comput. Electr. Eng., 3: 8-16.

Singh, R., M. Mathuria, K. Rathore and S. Kumar, 2013. A robust color image watermarking using combination of DWT and DCT. Proceedings of the 4th International Conference on IT Summit Confluence 2013 and the Next Generation Information Technology Summit Confluence, September 26-27, 2013, Institute of Engineering & Technology Educational, Noida, India, pp: 11-14.

Sinha, M.K., R. Rai and G. Kumar, 2014. Literature survey on digital watermarking. Intl. J. Comput. Sci. Inf. Technol., 5: 6538-6542.

Yusnita, Y. and O.O. Khalifa, 2007. Digital watermarking for digital images using wavelet transform. Proceedings of the IEEE International Conference on Telecommunications and Malaysia International Conference on Communications, May 14-17, 2007, Penang, Malaysia, pp: 665-669.