International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

Three Levels Dwt Watermarking Technique for Color Images and Watermarks

Ahmed Al-Gindy, Germin Ghaly

***Abstract:** This paper presents a three-levels Discrete Wavelet Transform (DWT) watermarking technique for color images and watermarks. The proposed technique utilizes embedding the RGB watermark information into the Y channel of the YCbCr cover image. A pre-processor is used to convert the color watermark from RGB to a binary sequence. The pre-processed output is, then, inserted several times into the Y channel of the YCbCr cover image by changing the LL3 DWT coefficients. The robustness of the proposed scheme is verified through the ability to resist several classical attacks such as scaling, cropping, JPEG compression, median filtering and low pass filtering. In addition, the proposed scheme does not need the original host image to recover the watermark; hence, the recovery method is blind. This paper also includes a qualitative comparison between the one-level and two-levels DWT.*

Keywords: Discrete wavelet Transform, watermarking.

I. INTRODUCTION

With the remarkable advancement of internet and communication technology along with the increasing availability of various advanced tools, digital information can be easily copied and exchanged from one place to another. As a consequence of the unauthorized replication, many copyright ownerships debates, concerning the originality of the digital information, arise.

Digital watermarking emerged as a tool for copyright protection against copyright infringement and authentication purposes. Digital watermarking techniques involve embedding information, known as the watermark, in digital media, known as the cover data, such as audio, video and images.

In General, watermarking algorithms involve embedding ownership information in digital contents through modifying the cover information. The watermark information can be represented in several ways; it can either contain small number of bits or several paragraphs of text depending on the total number of data required to be embedded [1].

Manuscript published on 30 September 2019
* Correspondence Author
Ahmed Al-Gindy*,Department of Electrical Engineering, Faculty of Engineering, Canadian University Dubai, Dubai, UAE
Germin Ghaly, Electronics and Communication Department, Faculty of Engineering, Ain Shams University, Cairo, Egypt
Email: agindy@cud.ac.ae, germin.saeed@eng.asu.edu.eg

Such changes have to be invisible to the human eye, in addition, it should be only recoverable by the control authorities. Secret keys are usually used to determine the locations at which the watermark is to be inserted; thus, they protect the watermark from being susceptible to removal by possible pirates.

Additionally, the watermarked image may undergo several alterations while being transmitted over the communication channel; these modifications are known as attacks. Possible attacks of watermarked images involve cropping, filtering and compression.

Digital watermarking techniques for copyright protection require the technique to be robust against attacks which enables the recovery of the watermark from the altered information. In contrast, digital watermarking algorithms for authentication purposes require the algorithm to be easily susceptible to attacks.

For digital images, several watermarking algorithms are utilized according to the required purpose and they can be categorized into frequency and spatial domains. Frequency domain schemes can resist several classical attacks; while, spatial domain algorithms are sensitive to such attacks. Hence, the robustness of frequency domain algorithms is better than that of spatial domain algorithms. Various frequency domain techniques are used in watermarking such as the DWT, Discrete Cosine Transform (DCT), Singular Value Decomposition (SVD) and Discrete Fourier Transform (DFT). This paper aims at watermarking for color images for copyright protection; thus, frequency domain scheme is more convenient to utilize than the spatial domain.

A DWT based watermarking algorithm is proposed in [2]. It utilizes uniform quantization of the direction of the most significant gradient vectors, acquired at several wavelet sub-bands, to insert the watermark. In this approach, enhanced Peak Signal to Noise Ratio (PSNR) is achieved; however, it lacks the verification against classical attacks.

A digital Image Watermarking with DWT-SVD hybridized approach is proposed in [3]. It involves applying SVD to the DWT decomposed 1-level frequency sub-bands. Gray scale images are used to test the robustness of this technique.

Authors in [4] proposed a 1-level DWT robust image watermarking algorithm. This algorithm utilizes the alpha blending technique in order to insert the watermark into the host image. The value of alpha is the only factor that affects the embedding and extraction of the watermark.

While, in [5], a DWT-DCT combined algorithm was proposed. This technique involves embedding watermark bits in the low frequency components of each DCT block of the specified DWT sub-band. 512×512 gray scale “Lena” image and 64×64 gray scale watermark are utilized.

Although, this technique shows robustness against several attacks, the achieved PSNR is not enhanced.

Authors in [6] proposed a dual watermarking technique. This technique uses one-dimensional (1D) watermark of size 1024 and two-dimensional (2D) gray scale watermark.

This algorithm involves embedding the 1D watermark into the second-level vertical and horizontal DWT of the 2D watermark. Several gray scale and color cover images are used. Although, the best achieved PSNR reached 68.8 in case of gray scale images and 54.8 in case of color images, the processing of this algorithm is too complex.

While, in [7], A digital watermarking algorithm that inserts a 2D watermark image into color image. It employed Multi-resolution DWT of the 200×200 Lena color cover image; while, the watermark utilized was 50×50 fishing boat gray scale image. This paper fails to evaluate the quality of the watermarked images. Moreover, it lacks the verification against the classical attacks.

In [8], a blind watermarking technique that utilizes three-dimensional (3D) watermark images is proposed. This technique converts RGB model of both the cover images and the watermark image into YCbCr model. Afterwards, the low and middle DCT frequency components of the YCbCr are modified by the watermark information. The cover image used was 512×512 Lena color images and two 64×64 watermarks were employed. This technique achieved an average PSNR 41 at watermarking strength α=3. However, this technique was not verified in case of JPEG compression attack.

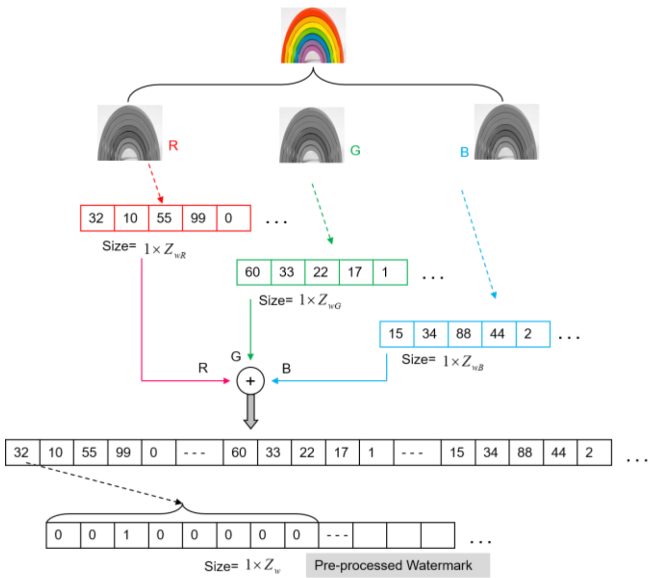
Commonly, authors use 1D and 2D digital watermarks for testing their proposed algorithms. However, these watermarks carry less information about the copyright ownership when compared with 3D watermarks. 3D watermark images are of larger size and capacity than 1D and 2D watermarks. Watermark capacity represents the maximum amount of data which can be inserted and extracted from a tampered watermarked image with low probability of bit error. Thus, the greater the watermark capacity, the more robust is the watermarking technique. Hence, the watermark capacity is an evaluation metric that indicate the robustness of the watermarking technique [9].

Throughout this paper, a digital watermarking technique is proposed that is implemented in the frequency domain. It involves applying the DWT block-based perspective to the Y channel of the YCbCr model. Shuffling process is used to embed a 3D RGB watermark image several times in the cover image [10]. The proposed algorithm is characterized by its robustness and high PSNR along with reduced processing complexity.

This paper is sorted as follows: Section II explains the pre-processing steps of the color watermark. The proposed watermarking technique is presented in section III. the achieved simulations and results are demonstrated in section IV. Finally, some conclusions are summarized in section V.

II. Pre-processing of Color Watermarks

Assuming that $m(i, j)$ is the color watermark image of size Z_w pixels; such that, each pixel is indicated by 24 bits. The RGB color watermark is divided into three different parts *R*, *G* and *B*; which are considered as three different gray level images. Each gray level image is then reshaped into 1D vector



of size $1\times Z_{WR}$, $1\times Z_{WG}$ and $1\times Z_{WB}$, respectively. The resulted 1D R, G and B elements are then combined into

Figure 1. Pre-procesing steps of color watermark

binary vector of size $1\times Z_W$. This binary vector is to be inserted in the host image, which will be discussed in section III. Applying the reverse order of the pre-processing color to binary steps, the color watermark image can be recovered through extracting the binary bits. Figure 1 depicts the pre-processing steps of the color watermark.

III. The Proposed 3-Levels DWT Watermarking Algorithm

The proposed algorithm involves inserting the RGB color watermark into the YCbCr color cover image using a block-based DWT algorithm. The embedding process starts by converting the RGB color to the YCbCr plane; in which, the Y components indicate the brightness, whereas, both Cr and Cb elements indicate color information. Then, the pre-processed watermark information is inserted in the Y plane; the resulting Y' plane contains the watermark data. The inverse of the watermarked YCbCr planes is used to generate the RGB watermarked image. The general graphical presentation for the proposed algorithm is depicted in Figure 2.

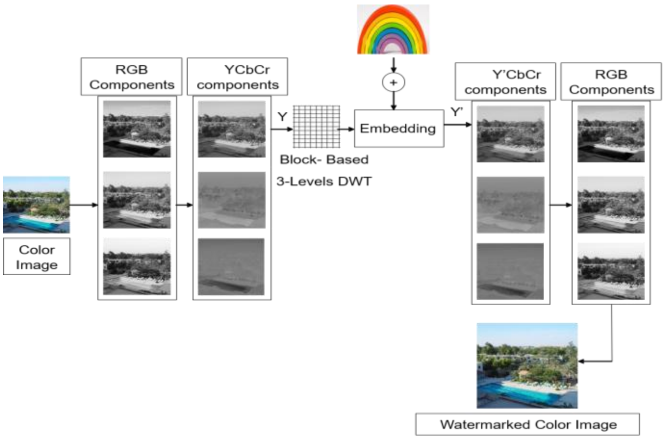


Figure 2. The proposed Three levels Technique

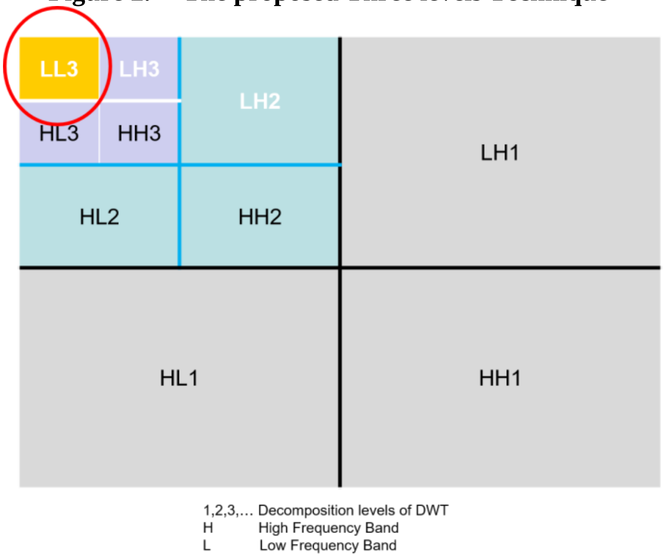


Figure 3. Three levels Block-Based DWT

As mentioned earlier, the proposed algorithm utilizes a block-based DWT technique in order to embed the binary watermark into the color cover image. Figure 3 shows the 3-levels DWT algorithm used. At first, the cover image is split into 32 × 32 blocks. Then, the DWT first level is applied on each block; which results in the division of the components of each block into four parts High-High frequencies (HH), High-Low frequencies (HL), Low-High frequency (LH) and Low-Low frequencies (LL). Hence, each block in the spatial domain will be divided into four parts in the DWT domain; HH1, HL1, LH1 and LL1 and each part has 16×16 pixels. The second level of DWT is applied to only the LL1 (16×16) parts in the first level. Each LL1 will be divided into four sub-parts; HH2, HL2, LH2 and LL2 and each part has 8×8 pixels. The process will be repeated for the LL2 (8×8) to generate the final LL3 (4×4). The embedding process will use only one coefficient in the LL3.

A. The Embedding Process

As mentioned, the DWT is applied such that the cover image is decomposed into four separate multi-resolution sub-bands: HH, HL, LH and LL. The process will be repeated to apply three levels of DWT.

The watermark data is inserted into the LL3 sub-band where 8 bits are embedded in one 4×4 LL3 sub-block. Afterwards, the process is repeated until one whole watermark is embedded in a portion of the host image. Then, the complete operation is repeated such that the several copies of the same watermark are embedded. It is important to notice that the sizes of both the watermark and the cover image can limit the total number of embedded watermark copies. After selecting the desired sub-block of the cover image, each bit of the watermark *w* is inserted into it.

Assuming that *f(i,j)* indicates the pixel of the G element of the RGB characterization of the color cover image and *m(i,j)* corresponds to the binary pixel of the watermark.

$$F_k(u,v) = DWT\{ f_k(i,j)\},$$

If m(i,j)=0 then

$$F(x,y) = \begin{pmatrix} \Delta\, Q_o\left(\frac{F_k(x,y)}{\Delta}\right) & x,y \in H_k & 1 \le k \le N_{HB} \\ F_k(x,y) & x,y \notin H_k & 1 \le k \le N_{HB} \end{pmatrix} \quad .... \quad (1)$$

If m(i,j)=1 then

$$F(x,y) = \begin{pmatrix} \Delta\, Q_e\left(\frac{F_k(x,y)}{\Delta}\right) & x,y \in H_k & 1 \le k \le N_{HB} \\ F_k(x,y) & x,y \notin H_k & 1 \le k \le N_{HB} \end{pmatrix} \quad .... \quad (2)$$

Such that x ≥1, y ≤ 8, Δ is a scaling quantity which represents the step utilized to quantize either to the odd or even number, Qo represents the quantization to the nearest odd number, while, Qe depicts the quantization to the nearest even number. Afterwards, the 8x8 block is inversely transformed back to the spatial domain, then, this step is applied again to the remaining blocks. The watermarked Y' component is, then, merged to the Cr and Cb components to produce the watermarked color image.

In order to minimize the spatial correlation between the inserted watermark and the cover image, a secret key is used to randomly scramble the binary watermark digits; thus, enhancing the quality of the watermarked image. Subsequently, each binary watermark copy undergoes a shuffle scheme; this shuffling technique reshapes the watermark copy as a vector and then applies different shifts, which has to be applied in a cyclic way, to this vector before the embedding step. The sizes of both the cover image and watermark determine the number of shifted bits of each watermark, which can be computed as shown below:

$$T_{SB} = Z_w / n \quad ..... \quad (3)$$

Such that T_{SB} indicates the total shifted bits of the watermark. As depicted, this shift is important in order to decrease the spatial relation, as well as, reduce the sensitivity to vertical cropping attacks [8] . Figure 4 shows a graphical demonstration of the insertion step.

B. The Extraction Process

Extracting the inserted watermark data $m(i,j)$ is achieved through performing block-based level 3 DWT of the watermarked image. Along with, utilizing the same confidential key used in the initial scrambling technique to select the exact components of the cover image that carry the 8 bits of the inserted watermark, the watermark can be extracted. The Y component is classified into 32 × 32 blocks. Each block is transformed into the DWT domain at which the LL3 band is to be used in the recovery process. The watermark recovery steps are the inverse of the insertion steps where each pre-defined frequency component is quantized using the scaling quantity. The extraction equation is represented as shown:

If $Q\left(\frac{F_k(x,y)}{\Delta}\right)$ is even then m(i,j) = 1

If $Q\left(\frac{F_k(x,y)}{\Delta}\right)$ is odd then m(i,j) = 0 ….. (4)

Such that Δ is equivalent to the one used in the embedding step and Q is rounded to the nearest integer. Figure 5 shows a graphical demonstration of the extraction step.

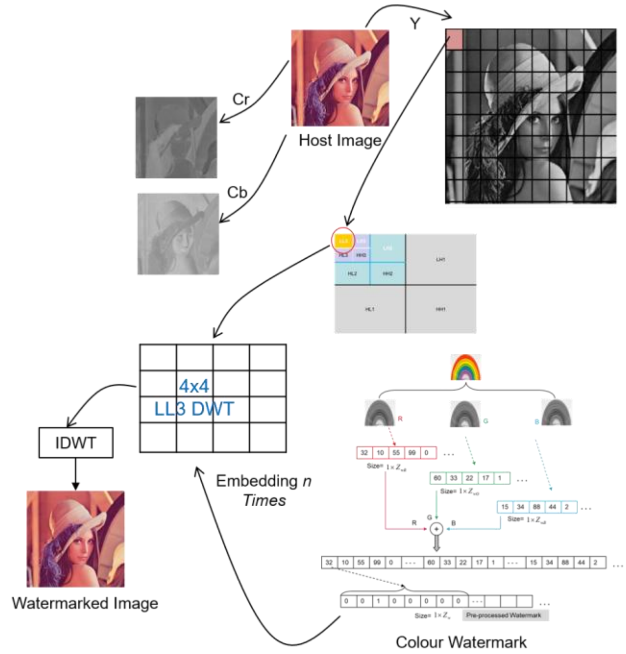


Figure 4. Embedding process of the watermark

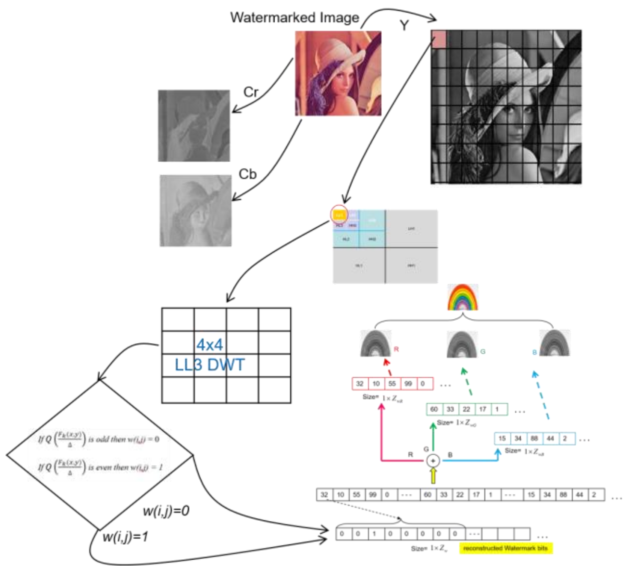


Figure 5. Extraction process of the watermark

IV. Results and Simulations

The proposed technique is tested using several 512×512 color cover images at which each pixel is denoted by 24 bits. The watermark used is a color image of size 32×32. The proposed technique is evaluated with various embedding strengths Δ. The PSNR is computed between the cover and the watermarked color images. Table I studies the imperceptibility of the proposed technique at several values of Δ. Taking Lena image as an example, it can be noticed that the PSNR values achieved range between 46.9 dB and 59.9 dB for Δ = 40 and Δ = 8, respectively. The Structural Similarity Index Measurement (SSIM) represents the second evaluation metric used. It is important to recognize that high SSIM percentage indicates large likeness among the compared images. The imperceptibility of the proposed technique is evaluated against level 1 DWT and Level 2 DWT through calculating SSIM at several values of Δ. Figure 6 shows the calculated SSIM for the different levels of the DWT at different values of Δ.

TABLE I. Calculated PSNR at several watermarking strengths

Image	Lena	Baboon	Pepper
Δ = 8	59.9	59.5	59.0
Δ = 12	54.4	54.2	53.9
Δ = 16	53.8	53.5	53.3
Δ = 20	51.9	51.4	51.2
Δ = 24	50.9	50.9	50.8
Δ = 30	49.1	49.2	49.5
Δ = 34	47.4	47.4	47.4
Δ = 40	46.9	46.8	46.7

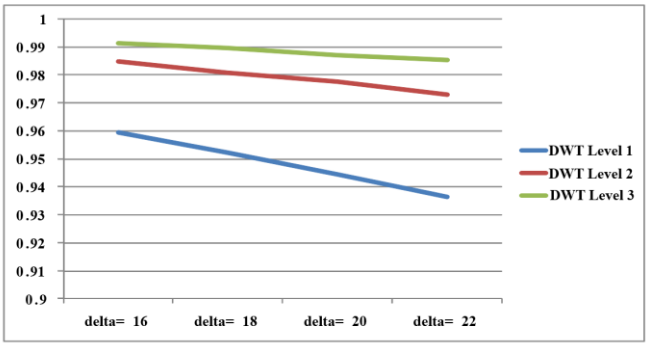


Figure 6. Comparison between DWT levels for the proposed technique using SSIM

To prove the robustness of the proposed technique, the watermarked images undergo several geometric and signal processing attacks. As an evaluation metric, the PSNR is computed to compare between the extracted and the original watermark. It can be noticed that as the total number of pixels present in the watermark image decreases, the watermark capacity increases; hence, enhanced robustness can be achieved. Table II summarizes the achieved results.

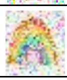
TABLE II. PSNR values of the extracted watermarks after attacks

PSNR evaluation for Color watermark size 32×32, at Δ =20	
Attacks	**PSNR**
Scale 0.75	42.19
Scale 0.5	39.50
Low pass 3×3	36.99
Wiener 3×3	38.40
Median 3×3	38.80
Median 3×3	36.67
JPEG 75	40.25
JPEG 50	37.70
JPEG 40	38.80
Salt & Pepper noise, *d* = 0.02	36.23
Scaling up (x2)	60.40

Contrast enhancements (intensity = 0.3, 0.9)	43.18
Gaussian noise (v = 0.002, m = 0)	34.80
Vertical Cropping 75%	39.20
Vertical Cropping 50%	38.67
Horizontal Cropping 75%	39.85
Vertical and Horizontal Cropping 75%	36.47

Using color watermarks as an information to be embedded is of interest in case where a visually meaningful detected watermark whose integrity can be verified by visual inspection is needed. It must be noted that the watermarks were scrambled to prevent statistical estimation of the original watermark by an attacker. Additionally, the watermarks were encrypted using a secret key. Table III represents visual recognition of the extracted color watermarks.

TABLE III.
sual inspection for the extracted watermarks after attacks

Extracted color watermarks after attacks, size 32×32, at Δ =20	
Attacks	**Visual Inspection Results**
Vertical Cropping 75%	
Vertical Cropping 50%	
Horizontal Cropping 75%	
Vertical and Horizontal Cropping 75%	
Contrast enhancements (intensity = 0.3, 0.9)	
Gaussian noise (v = 0.001, m = 0)	
Scaling down (x0.5)	
Scaling down (x0.75)	
Scaling up (x2)	
JPEG 40	
JPEG 50	
JPEG 75	
Wiener 3×3	
Median 3×3	
Median 5×5	
Low pass 3×3	
Salt & Pepper noise, *d* = 0.01	

The proposed technique targets the embedding of color watermarks into color host images, along with, producing watermarked color images that have both properties: imperceptibility to the human eye and robustness against attacks. As mentioned, both properties represent a trade-off, as there is a direct relation between both the visibility and robustness of a digital watermark.

To determine the optimum performance for most of the images, several insertion strengths are evaluated. The evaluation technique aims at finding the optimum balance between the imperceptibility, capacity and robustness. Table IV depicts a visual demonstration of the watermarked Lena images at several embedding strengths. After running through attacks and extracting the watermark, it was noticed that the implementation of the proposed technique is visible at Δ = 20. As the embedding strength value increases, such as Δ = 40, the proposed technique will achieve stronger robustness; however, the quality of the cover image will be reduced. Thus, embedding strength of value 20 can be considered as the optimum value in order to attain the balance of robustness and imperceptibility.

TABLE IV.
enuine and watermarked Lena images at several watermarking strenghts

	
Genuine Lena image and the used watermark	
	
watermarked Lena (Δ = 8)	watermarked Lena (Δ = 12)
	
watermarked Lena (Δ = 16)	watermarked Lena (Δ = 20)
	
watermarked Lena (Δ = 30)	watermarked Lena (Δ = 40)

V. CONCLUSION

A block-based 3-levels DWT for inserting a color watermark image into a cover color image is proposed. A pre-processing step, of the color watermark, is applied firstly before embedding; in order to convert it from RGB to binary sequence.

The proposed algorithm was examined using several watermarking strengths; thus, an optimum watermarking strength was selected which is $\Delta = 20$. Several evaluation metrics were used to verify the robustness of the proposed technique against various image processing operations like contrast enhancements, additive noise, JPEG compression, scaling and cropping. The proposed algorithm of 3-level DWT has been compared with 1-level and 2-level DWT.
Comparison results indicated that the proposed technique has achieved the highest SSIM with various embedding strengths. In addition, the proposed technique uses blind extraction process.

REFERENCES

1. Ahmed Al-Gindy. "A graphical user interface watermarking technique for the copyright protection of colour images using colour watermarks", 2011 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT), 12/2011.
2. Kullayamma, I & Sathyanarayana, P. (2015). Satellite enhanced image watermarking using gradient direction quantization. 1-9. 10.1109/EESCO.2015.7253665.
3. Arora, Shaifali M. "A DWT-SVD based robust digital watermarking for digital images." Procedia computer science 132 (2018): 1441-1448.
4. Akhil Pratap Shing, Agya Mishra, 2011. Wavelet Based Watermarking on Digital Image, Indian Journal of computer Science and Engineering.
5. Deb, Kaushik, et al. "Combined DWT-DCT based digital image watermarking technique for copyright protection." 2012 7th International Conference on Electrical and Computer Engineering. IEEE, 2012.
6. J.-w. Gao and J.-g. Li, 2009. Digital Watermark Algorithm Based on Embedding Gray Image into Color Image, in International Conference on Computer Engineering and Technology, pp. 146 - 147.
7. Z. Yong, L. Li-Cai, L. Q. Shen, and J. Z. Tao, 2009. A Blind Watermarking Algorithm Based on Block DCT for Dual Color Images in Second International Symposium on Electronic Commerce and Security, ISECS Nanchang, China, pp. 213 - 217.
8. Y.J.Song, R.Z.Liu, and T.N.Tan, 2001. Digital Watermarking for Forgery Detection in Printed Materials in International Symposium on Multimedia Information Processing, Beijing, China, October 24-26.
9. S. Shefali and S. M. Deshapande, 2006. Mathematical Model for Improved Capacity Estimations for Data Hiding Techniques under Lossy Compression in Proceedings of the 2nd IMT-GT Regional Conference in Mathematics, Statictics and Applications, Malaysia, June.
10. A. Al-Gindy, H. Al-Ahmad, R. Qahwaji, and A. Tawfik, 2007. Enhanced DCT based technique with shuffle scheme for robust image watermarking of handwritten signatures. in proceeding of ICCCP'07 International conference for communication, Computer and Power, Muscat, Oman, pp. 450-455

AUTHOR PROFILE

Dr. Al-Gindy holds a Ph.D. in Electrical and Communication Engineering from Faculty of Engineering and Informatics, University of Bradford, United Kingdom. He also obtained his M.Phil Degree from Faculty of Engineering and Informatics University of Bradford United Kingdom, and a Bachelor of Engineering in Electrical and Computer Engineering from Faculty of Engineering & Technology, Maritime Academy for Science & Technology, Alexandria Egypt.
Dr. Al-Gindy is a certified academic program assessor in the association of Arab Universities, Department of quality Assurance and quality enhancement in higher education institute. He is certified in Business process Management and Improvements, from George Washington University, USA.
Dr. Al-Gindy has developed several curriculum and instruction Manuals in Engineering and Computing Technologies. His research interests cover design of various signal and image processing algorithms, RFID technologies and Artificial Intelligence.

Germin Ghaly holds an M.Sc. in Electronics and Communications Engineering from Faculty of Engineering, Ain Shams University, Egypt. She, also, obtained her B.Sc. in Electronics and Communications Engineering from Faculty of Engineering, Ain Shams University, Egypt. Germin is an assistant lecturer in the Electronics and Communications department, Ain Shams University, Egypt. In addition, she was a researcher in the "60 GHz Sensor Network Based Wireless ECG System" project funded by the National Telecommunications Regulatory Authority (NTRA), Egypt.