A New Watermarking Scheme For Colour Images Captured By Mobile Phone Cameras

A.Al-Gindy [a], H.Al-Ahmad [b], R.Qahwaji [a] and A.Tawfik [c]
[a] School of Informatics, University of Bradford, UK
[b] Department of Electronic Engineering, Khalifa University of Science, Technology and Research, UAE
[a] Faculty of Engineering, Ajman University of Science and Technology, UAE

Summary

A new frequency domain based watermarking scheme for colour images captured by mobile phone cameras is proposed. The proposed technique embeds personal mobile phone numbers inside the image. The aim of the scheme is to protect the copy right ownership of the image. Each bit of the decimal digits is inserted onto one low frequency coefficient of one of the DCT blocks of the host image. A DCT coefficient selection (DCS) process has been applied to increase the invisibility qualities, this process managed to find the coefficient with the maximum magnitude. Different embedding location depending on the spatial frequencies of the host image will be selected. The proposed algorithm achieves a high PSNR values and is found to be robust against JPEG compression and different image manipulation algorithms.

Key words:
Watermarking, DCT, Blind, Error detection, colour image.

1. Introduction

Many mobile phones are equipped with high resolution digital cameras. Their users are capturing images and sharing them with others by sending them as email attachments, multimedia messages or via Bluetooth. Digital watermarking provides the security of knowing that no matter how or where images appear they carry the notice of ownership. This can be done by embedding the phone number including the international calling code onto the images. To achieve this objective two main goals should be considered, firstly to make use of the RGB colour model, and secondly to utilize the DCT. The main advantage of using the RGB colour model and DCT comes from the fact that JPEG compression which utilises the 8 × 8 DCT blocks are applied to captured images.

There are many digital image watermarking techniques reported in the literature. Reviews on image watermarking techniques can be found in [1, 2]. These techniques can be classified according to a number of different criteria. One such criterion is the domain in which the watermark is embedded. In this context, there are two main categories: spatial domain techniques [3, 4], and frequency domain techniques, [5, 6]. Another classification of digital image watermarking techniques is based on whether the original host image is needed in the watermark extraction process or not. Blind watermarking techniques, such as the one used in this work, can extract the watermark without the need for the original image.

In the past few years, several watermarking schemes have been proposed, but digital watermarking schemes on mobile devices are scarce. In addition, watermark insertion is needed in devices with various features such as Digital cameras, PDAs and mobile phone as multimedia services on those devices are heavily used. Some researchers [7-11] proposed watermarking algorithm that can be applied to mobile phones.

In [7] a method was proposed for detecting the cause of destroying or changing hidden data in an MMS (Multimedia Messaging Service) message. The authors in [7] embedded the copyright notes in an audio file that was sent along with the image. So while extracting the hidden information from the MMS message, if copyright notes which were extracted from both image and audio file are different, it was concluded that the hidden data are damaged or changed. A watermarking scheme for colour images using the Y channel was proposed in [8]. A spatial domain watermarking algorithm was used in [9]. The image was decomposed into blocks and the pixels were classified into different zones. A study in [10] evaluated the visual quality of watermarked images displayed on mobile devices. The results showed that for high-end displays the strength of the watermarking is a critical factor in image quality. In mobile devices the magnitude used for watermarking had little visual effect. A blind watermarking scheme was proposed in [11] using wavelet decomposition.

A new frequency domain based watermarking scheme for colour images is proposed here. Each bit from the phone digits is embedded in one of the low frequency DCT coefficients of the host image. This process allows the watermark to be embedded many times in the host image which increases the robustness against many attacks. Checksum error detection encoder is used in the technique where a numerical value representing the sum of the phone digits is added to the embedded numbers.

This paper consists of 4 sections. The new algorithm is discussed in Section 2. Results and comparison with other algorithms are presented in Section 3. Finally, the concluding remarks are introduced in Section 4.

Manuscript received July 5, 2009
Manuscript revised July 20, 2009

2. The Proposed Algorithm

The phone number plus the international country code is used as the watermark. The summation of the decimal digits is added to the number to make it 16 decimal digits. This is useful to check that the extracted number is correct or not. A special procedure is applied if the summation exceeds 99. Its worth mentioning that the maximum summation that can be achieved is 126 when a mobile phone with 14 digits all nines is entered, in such a case the check sum digits as shown in figure 1 will hold 12 and 6 instead of 6 and 3 respectively. Then each one of the 16 decimal digits is converted to a 4 bit binary number. Therefore, we will end up with 64 binary bits. Figure 1 shows an example for a UAE mobile number.

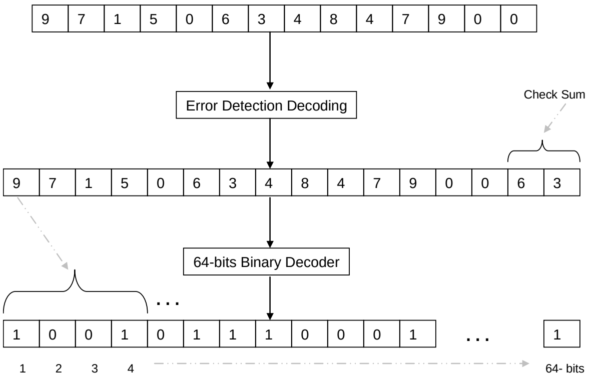


Figure 1 Phone number encoder

2.1 The DCT Selection Coefficients (DCS) Process

The DCT block consists of 8×8 coefficients. The 16 lower frequencies are screened to find the coefficient with the highest magnitude and register its location. This process is repeated for all DCT blocks. The location which is repeated more is selected. This location will vary from one image to another according to the spatial frequency contents of the image. One binary bit of the watermark will be embedded in this location. A flow graph of the DCT coefficients selection (DCS) process is shown in figure 2. Table I represents the registered location of some images. In order to test the security of the DCS process the images were screened again after embedding to verify that the method is secure and an attacker would not be able to use the DCS process again to detect the originally selected locations. Screening the DCT blocks again after embedding will result in totally different locations from the previously registered locations in the original unwatermarked images as shown in table II.

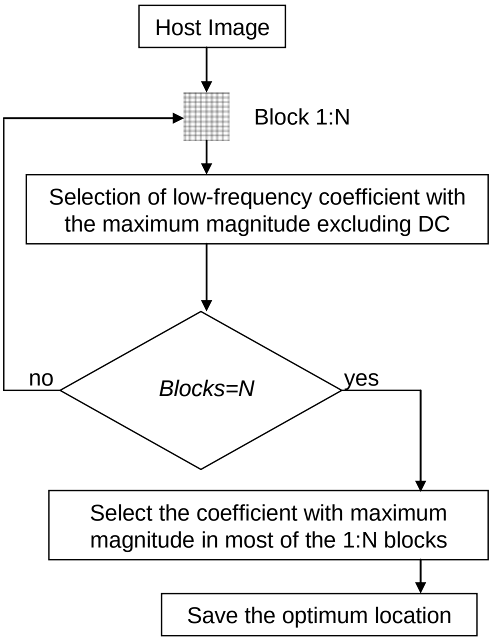

Host Image
Block 1:N
Selection of low-frequency coefficient with the maximum magnitude excluding DC
Blocks=N
no
yes
Select the coefficient with maximum magnitude in most of the 1:N blocks
Save the optimum location

Figure 2 A flow-graph of the DCS process

Table I The DCS locations for original images

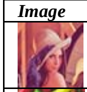
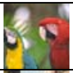
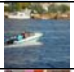
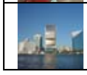
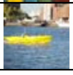
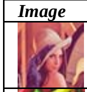
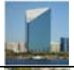
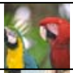
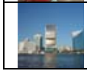
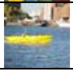
The DCS locations for some images					
Image	***Coefficient***	***Image***	***Coefficient***	***Image***	***Coefficient***
	*(1,2)*		*(1,2)*		*(2,1)*
	(1,2)		*(2,1)*		*(2,1)*
	(1,2)		*(2,1)*		*(2,1)*
	*(2,1)*		*(2,1)*		*(1,2)*

Table II The DCS locations after embedding

The DCS locations for some images after embedding					
Image	***Coefficient***	***Image***	***Coefficient***	***Image***	***Coefficient***
	*(2,1)*		*(2,1)*		*(1,2)*
	(2,1)		*(1,2)*		*(1,2)*
	(2,1)		*(1,2)*		*(3,1)*
	*(3,1)*		*(3,1)*		*(2,1)*

2.2 The Embedding Process

The proposed watermarking scheme is based on the possibility of embedding multi copies of the binary watermark (i.e. 64 bits) in the host image. Let us assume that $f(i,j)$ is the host image of size Z_h pixels and let $w(i,j)$ be the binary phone digits of size Z_w bits which is usually much smaller in size compared to the size of the host image. For simplicity, let us assume that the host image size could accommodate integer copies of the watermark image. The watermark is converted to 1D vector and the host image is divided to N_{HB} non-overlapping 8×8 sub-blocks. The number of watermark copies n that can be embedded in the host image is given by,

$$n = N_{HB} / N_{wB} \tag{1}$$

where N_{wB} is the number of the watermark bits .

The embedding algorithm here is totally blind as the original host image is not required for watermark extraction. The watermark data is embedded in the very low-DCT frequency component obtained from the DCS process. This range of frequencies is chosen because the high frequency components may be discarded in some image processing operation such as JPEG compression. Placing the watermark using very low DCT coefficients maximizes the chances of reconstructing the watermark even after common signal distortions. Further, modification of these components results in severe image degradation long before the watermark itself is destroyed. An attacker would have to add more noise energy in order to sufficiently remove the watermark. However, this process would destroy the image fidelity.

In the technique presented here, the colour image is decomposed into three components R, G and B. The watermark information is embedded in the G plane [12] to produce G` after embedding. In [12] a library of different colour images and their associated gray level versions were used for testing and an analytical measurements have been carried out using some popular measurements metrics to demonstrate the validity of using the green channel of the RGB colour space for watermark embedding. The presented approach has proven to provide excellent invisibility qualities and stronger robustness compared to other watermarking techniques [12]. Inside each 8×8 sub-blocks, one DCT coefficient is identified and used throughout the embedding process. The predefined coefficient has been obtained form the adaptive process applied previously to the host image. It is worth mentioning that for each host image different predefined coefficient will be selected, with the advantage of studying the host image information; the invisibility qualities will be increased. The binary mobile number digits are randomly scrambled using a secret key. This scrambling process is essential to reduce the spatial correlation between the host image and the embedded watermark. After the scrambling process, the shuffle scheme presented in [13] is applied for each copy of the binary mobile number to shift the binary digits before the embedding process. The shift operation is carried out in a cyclic way. The number of shifted watermark bits depends on the host image size and the watermark size. It can be calculated as follows:

$$w_{SB} = Z_w / n \tag{2}$$

Where w_{SB} is the number of shifted watermark bits,

Finally individual insertion of the binary mobile phone digits is applied into the host image using the embedding equation as follows:

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

If w(i,j)=1 then

$$F_k(x,y) = \begin{cases} \Delta Q_e(\frac{F_k(x,y)}{\Delta}) & x,y \in H_k \quad 1 \le k \le N_{HB} \\ F_k(x,y) & x,y \notin H_k \quad 1 \le k \le N_{HB} \end{cases}$$

If w(i,j)=0 then

$$F_k(x,y) = \begin{cases} \Delta Q_o(\frac{F_k(x,y)}{\Delta}) & x,y \in H_k \quad 1 \le k \le N_{HB} \\ F_k(x,y) & x,y \notin H_k \quad 1 \le k \le N_{HB} \end{cases} \tag{3}$$

Where 1 ≤ *x*, *y* ≤ 1, and *Qe* is the quantization to the nearest even number and Q_o is the quantization to the nearest odd number, Δ is a scaling quantity and it is also the quantization step used to quantize either to an even or an odd number. All the previous watermarking steps are described graphically in the diagram as shown in Figure 3. It is important to note that the watermark is embedded several times in the host image depending on the sizes of the host image and the watermark image.

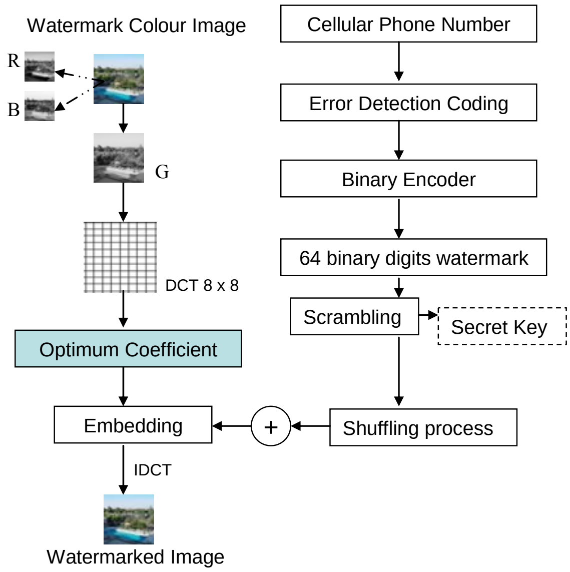


Figure 3 Graphical illustration of the embedding process

2.1 The Extraction process

The embedded watermarks information can be extracted by performing 8×8 DCT transform for the G channel of the watermarked host image and then indicating the same coefficient of the host image that carries the bits of the embedded watermarks using the required secret key. It is worth mentioning that although the proposed scheme is blind, it requires information such as the sizes of both the host and watermark images and the watermark embedding strength Δ. The extraction formula defined in equation 4 is used to produce the scrambled watermark. According to the key in the initial scrambling operation, the scrambled watermark is descrambled to retrieve the original watermark. A reverse shuffling process is implemented for each reconstructed watermark. Simply, the recovery function is the inverse of all the watermarking embedding steps. Each predefined frequency coefficient is quantized by Δ and rounded to the nearest integer. The extracted formula is defined as follows:

$$\text{If } \; Q\left(\frac{F_k(x,y)}{\Delta}\right) \text{ is odd then } w(i,j)=0$$

$$\text{If } \; Q\left(\frac{F_k(x,y)}{\Delta}\right) \text{ is even then } w(i,j)=1 \qquad (4)$$

Where Q is rounded to the nearest integer. Δ has a value that is equal to the value used for the embedding process. Finally, the error detection has been used to discard the incorrect number before the averaging process. The averaging process has managed to reduce the error of the extracted watermarks. A visual representation for the extraction process is shown in Figure 4.

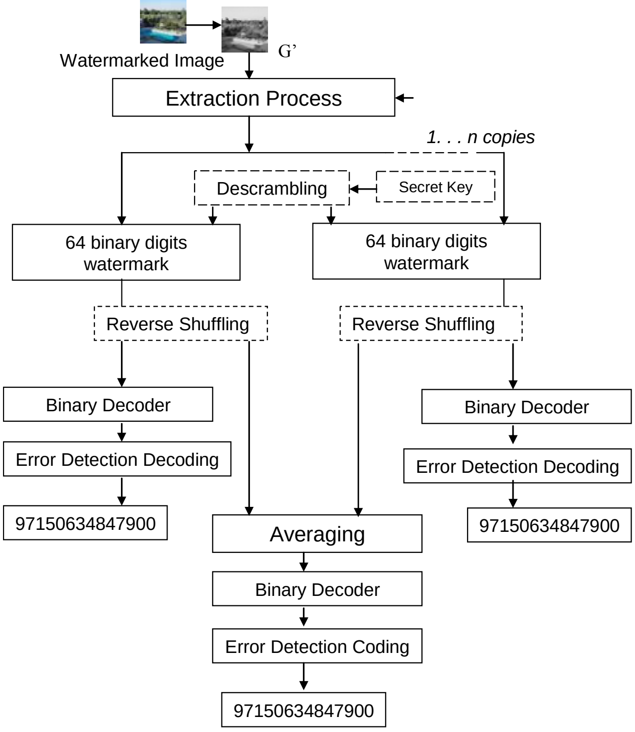


Figure 4 Graphical presentation for extraction steps

3. Results and Simulation

A library of several colour images depicted using digital camera plus some standard images were used to test and evaluate the proposed method, as shown in section 2.1 in tables I and II. Two evaluation techniques are used in our experiments with different watermarking strengths Δ as shown in Table III & IV. The first evaluation is carried out by calculating the peak signal to noise ratio (PSNR) between the host image and the watermarked colour image. The second evaluation is carried out using the structural similarity index measurement (SSIM) between the host image and the watermarked image [14]. The higher the SSIM percentage is, the larger the similarity between the compared images. The aim of the proposed algorithm is to embed digital watermarks that are both imperceptible to the human eye and robust against attacks. This can be a delicate balancing act, since the robustness and visibility of a digital watermark are directly related. An increase in the watermark embedding strength increases the visibility of the extracted watermarks.

As a part of our testing strategy, various embedding strengths have been investigated to determine which values provide best performance for the majority of the images. The experimental results show that the performance achieved by the proposed method for the extracted watermark after running through attacks is perceptually visible at Δ=24, which can be considered as the best value among the tested values as shown from table III. Higher embedding strength values such as Δ =34 will provide strong robustness and distinct perceptual visibility for the extracted watermark. However it will reduce the PSNR of the watermarked images as shown in table III, and vice versa if lower embedding strength values such as Δ =16 is chosen. In order to verify the better performance of the green channel over the Y channel of the YCrCb model a perceptual visibility comparison is shown in table V. The original "Lena" colour image is used to examine the perceptual quality at different embedding strengths as depicted in table VI. To verify the robustness of the proposed method, various common signal processing and geometric attacks are applied to the watermarked images. The normalized correlation (NC) is used to measure the similarity between the original and the extracted watermark. Table VII demonstrates the performance of the proposed method when using the country code and a mobile phone number from the United Arab Emirates (UAE), table VIII tests the performance when using the country code and a mobile phone number from Egypt and Finally the country code and a mobile number from United Kingdom (UK) shown in table IX.

Special requirements are needed when using mobile phone numbers as a method to authenticate digital images. From tables VII, VIII and IX normalized correlation values less than one means that the algorithm has failed to restore the embedded data.

Table III PSNR for the watermarked host image

Peak Signal to Noise Ratio			
Image	*Lena*	*Pepper*	*Baboon*
PSNR at Δ = 16	51.4395	50.6715	54.5712
PSNR at Δ = 24	47.8758	46.5765	49.1367
PSNR at Δ = 34	44.7981	43.1761	46.8171
PSNR at Δ = 40	43.2219	42.0291	45.7610

Table IV SSIM for the watermarked host image

Structural Similarity Index Measurements			
Image	*Lena*	*Pepper*	*Baboon*
SSIM at Δ = 16	0.9979	0.9963	0.9993
SSIM at Δ = 24	0.9950	0.9918	0.9985
SSIM at Δ = 34	0.9902	0.9829	0.9970
SSIM at Δ = 40	0.9865	0.9778	0.9957

Table V PSNR and SSIM for the watermarked host image using Y channel of the YCrCb colour model

PSNR and SSIM using Y channel of YCrCb model			
Image	*Lena*	*Pepper*	*Baboon*
PSNR at Δ = 16	44.0311	43.1115	48.3176
PSNR at Δ = 24	42.9778	41.5425	45.6677
SSIM at Δ = 16	0.9875	0.9813	0.9961
SSIM at Δ = 24	0.9758	0.9647	0.9925

Table VI Original and watermarked Lena image at different watermarking embedding strengths

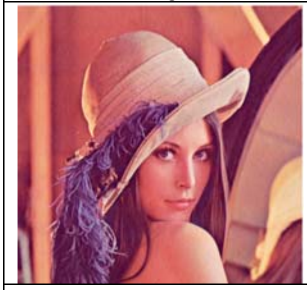
 Original Unwatermarked Lena image	
 Watermarked image at Δ = 16	 Watermarked image at Δ = 24
 Watermarked image at Δ = 34	 Watermarked image at Δ = 40

Table VII Extracted mobile numbers against some attacks

NC values at Δ =24 United Arab Emirates (UAE) mobile number = 97150634847900			
Attacks	**NC**	**Attacks**	**NC**
Cropping 50% V	0.739	Low pass 3×3	1
Cropping 48% V	1	Low pass 5×5	1
Cropping 75% H	1	Wiener 3×3	1
Cropping 50% H	1	Wiener 5×5	1
Gaussian noise m=0, v=0.002	0.80	Median 3×3	1
Gaussian noise m=0, v=0.001	1	Median 5×5	1
S&P noise, *d*=0.02+ Median 3×3	1	JPEG 50	1
S&P noise, *d*=0.05+ Median 3×3	1	JPEG 25	1
Contrast enhancements intensity=0.3, 0.9	1	JPEG 18	1
Scale 2	1	Scale 0.4	1

Table VIII Extracted mobile numbers against some attacks

NC values at Δ =24 Egypt mobile number =2012333603800			
Attacks	**NC**	**Attacks**	**NC**
Cropping 50% V	0.734	Low pass 3×3	1
Cropping 48% V	1	Low pass 5×5	1
Cropping 75% H	1	Wiener 3×3	1
Cropping 50% H	1	Wiener 5×5	1
Gaussian noise m=0, v=0.002	0.80	Median 3×3	1
Gaussian noise m=0, v=0.001	1	Median 5×5	1
S&P noise, *d*=0.02+ Median 3×3	1	JPEG 50	1
S&P noise, *d*=0.05+ Median 3×3	1	JPEG 25	1
Contrast enhancements intensity=0.3, 0.9	1	JPEG 18	1
Scale 2	1	Scale 0.4	1

Table IX Extracted mobile numbers against some attacks

NC values at Δ =24 United kingdom (UK) mobile number=44772070772400			
Attacks	**NC**	**Attacks**	**NC**
Cropping 75% V	0.745	Low pass 3×3	1
Cropping 48% V	1	Low pass 5×5	1
Cropping 75% H	1	Wiener 3×3	1
Cropping 50% H	1	Wiener 5×5	1
Gaussian noise m=0, v=0.002	0.82	Median 3×3	1
Gaussian noise m=0, v=0.001	1	Median 5×5	1
S&P noise, *d*=0.02+ Median 3×3	1	JPEG 50	1
S&P noise, *d*=0.05+ Median 3×3	1	JPEG 25	1
Contrast enhancements intensity=0.3, 0.9	1	JPEG 18	1
Scale 2	1	Scale 0.4	1

4. Conclusion

A secure blind watermarking algorithm of colour images using mobile numbers has been presented. A DCT coefficient selection (DCS) process has been applied to increase the invisibility qualities, this process managed to find the coefficient with the maximum magnitude. Different embedding location depending on the spatial frequencies of the host image was selected. The proposed algorithm is robust. Several watermarking strengths have been examined and the best watermarking strength is Δ =24. The algorithm has been tested with several mobile phone numbers from several countries. The new watermarking method has shown to be resistant to JPEG compression, additive noise, cropping, scaling, low-pass, and median filtering and removal attack.

References

[1] S. Katzenbeisser and F. Petitcolas, *Information Hiding Techniques for Steganography and Digital Watermarking*. London: Artech House, 2000.

[2] M. M. I. Cox and J. Bloom, *Digital Watermarking*. San Francisco: Morgan Kaufmann Publishers, 2001.

[3] P.S.Huang, C. S. Chiang, C. P. Chang, and T. M. Tu, "Robust spatial watermarking technique for colour images via direct saturation adjustment," in *Vision , Image and Signal Processing, IEE proceedings*, 2005, pp. 561-574.

[4] B. Verma, S. Jain, D. P. Agarwal, and A. Phadikar, "A new colour image watermarking scheme," *Infocomp, Journal of computer Science,* vol. 5, pp. 37-42, 2006.

[5] X. Li and X. Xue, "Improved robust watermarking in DCT domain for colour images," in *18th International Conference on Advanced Information Networking Applications (AINA04)*, 2004.

[6] W. Lu, H. Lu, and F. L. Chung, " Robust digital image watermarking based on sub-sampling " in *applied mathematics and computation*, 2006, pp. 886-893.

[7] M. Shirali-Shahreza, "A simple method for detecting the possible changes of hidden information of watermarked image in an MMS message," in *International Symposium on Biometrics and Security Technologies*, Islamabad, Pakistan, 2008, pp. 1-4.

[8] J. H. Seo and H. B. Park, "Colour images watermarking of multi-level structure for multimedia services," in *International Conference on Convergence Information Technology*, Gyeongju, South Korea, 2007, pp. 854 - 860.

[9] K. Krasavin, J. Parkkinen, and T. Jaaskelainen, "Digital watermarking on mobile devices," in *International Conference on Information and Communication Technologies: From Theory to Applications*, Damascus, Syria, 2004, pp. 319-320.

[10] K. Krasavin, J. Parkkinen, and T. Jaaskelainen, "Visual quality of watermarking for mobile devices," in *Journal of the Society for Information Display* June 2006, pp. 575-580.

[11] J.-S. Sohn, S.-l. Lee, and D.-G. Kim, "Image adaptive watermarking technique for digital phone," in *International Conference on Computational Intelligence and Security*, Guangzhou, China, 2006, pp. 1190 - 1194.

[12] A. Al-Gindy, H. Al-Ahmad, R. Qahwaj, and A. Tawfik, "A novel blind Image watermarking technique for colour RGB images in the DCT domain using green channel " in *Mosharaka International Conference on Communications, Computers and Applications (MIC-CCA 2008).* , Amman, Jordan, 2008.

[13] A. Al-Gindy, H. Al-Ahmad, R. Qahwaji, and A. Tawfik, "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, 2007, pp. 450-455

[14] Z. Wang, A. Bovic, H. Sheikh, and E. Simoncelli, "Image Quality Assessment: From Error Visibility to Structural Similarity," in *IEEE Transactions on Image Processing*, 2004, pp. 600-612.

Ahmed Al-Gindy received his BEng degree from Maritime Academy for Science & Technology, Alexandria, Egypt in 1997, MPhil degree from School of Engineering, University of Bradford, Bradford, UK, in 2004 and currently a PhD student in the department of Electronic imaging and media communications, School of Informatics, University of Bradford, Bradford, UK. He is currently a lecturer in Faculty of Engineering, Ajman University of Science & Technology, Ajman, United Arab Emirates. His current research interest in digital image processing.

Hussain Al-Ahmad received his B.Sc degree in electrical engineering from the University of Basra, Iraq in 1976. MSc in microwave communications and PhD in signal processing from the University of Leeds, UK in 1979 and 1984 respectively. He is an expert in signal and image processing. He is currently a Professor of signal processing and Head of the electronic engineering department at Khalifa University, UAE. He worked before at University of Bradford, Kuwaiti Faculty of Technological Studies, Leeds Polytechnic and Portsmouth Polytechnic. He published more than 50 papers in international conferences and journals. He supervised successfully more than 20 PhD students. Prof. Al-Ahmad is a fellow of IET, C.Eng, senior member of IEEE, member of BCS, CITP, fellow of RPS, ASIS. He is the chairman of the UAE IEEE computer chapter and vice chairman of BCS-ME. He served on many organization and technical program committees of international conferences.

Dr Rami Qahwaji is a Senior Lecturer in the Department of Electronic Imaging and Media Communications (EIMC) at the University of Bradford. Dr Qahwaj received a first class BSc honors degree in Electrical Engineering followed by an MSc in Control and Computer Engineering and finally a PhD in Computer Vision Systems in 2002 from the University of Bradford. His research interests include: Digital Imagine, Computer Vision, Space and satellite imaging, medical imaging, biometrics, watermarking, 3D image representation and machine learning. His publications include around 80 refereed journal papers and conference proceedings, more than 25 conference presentations and 5 PhD completions. He has refereed research proposals for different funding bodies. He is also a reviewer for several international journals such as IET Proc. Radar, Sonar & Navigation, Pattern Recognition Letters, Neural Computing and Applications, Solar Physics, Signal Processing and others. He is also member of the Editorial board of International Journal of Imaging Science and Engineering. Dr Qahwaji is the Conference Co-Chair of the Int. Conference on CYBERWORLDS 2009 (UK) and the Int. Conference on Computer Science from Algorithms to Applications (CSAA 2009 – Egypt). He is fellow of the Higher Education academy (HEA) and full member of IET, IEEE, AGU, SCIP and IASTED.

Ayman Tawfik received his PhD in Electrical Engineering from Univ. of Victoris, Canada in 1995. He received BSc and MSc in Electrical Engineering from Ain-Shams Univ., Cairo, Egypt in 1983 and 1989, respectively. He is currently working (on sabbatical leave) as Associate-Prof in Ajman University of Science & Technology, Ajman, UAE. His current research interests are digital signal processing theory and applications, digital image processing and wireless communications.