Digital Watermarking-Based DCT and JPEG Model

Mohamed A. Suhail, *Member, IEEE*, and Mohammad S. Obaidat, *Senior Member, IEEE*

***Abstract*—In recent years, digital watermarking techniques have been proposed to protect the copyright of multimedia data. Different watermarking schemes have been suggested for images. The goal of this paper is to develop a watermarking algorithm based on the discrete cosine transform (DCT) and image segmentation. The image is first segmented in different portions based on the Voronoi diagram and features extraction points. Then, a pseudorandom sequence of real numbers is embedded in the DCT domain of each image segment. Different experiments are conducted to show the performance of the scheme under different types of attacks. The results show that our proposed watermark scheme is robust to common signal distortions, including geometric manipulations. The robustness against Joint Photographic Experts Group (JPEG) compression is achieved for a compression ratio of up to 45, and robustness against average, median, and Wiener filters is shown for the 3×3 up to 9×9 pixel neighborhood. It is observed that robustness against scaling was achieved when the watermarked image size is scaled down to 0.4% of its original size.**

***Index Terms*—Discrete cosine transform (DCT), digital watermarking, Joint Photographic Experts Group (JPEG) model, Voronoi diagram.**

I. Introduction

DIGITAL watermarking is an important technology that has many applications. Many watermarking schemes have been suggested for images, audio, and video streams. A large number of these schemes address the problems of implementing invisible watermarks. Basic watermarking concepts are discussed in [1]–[7]. These papers review developments in transparent data embedding and watermarking for audio, image, and video. Researchers define a digital watermark as an identification code carrying information (an author's signature, a company logo, etc.) about the copyright owner, the creator of the work, the authorized consumer, and so on. It is permanently embedded into digital data for copyright protection and may be used for checking whether the data have been modified [1]. On the other hand, the detectable watermark can be detected only if its content is known in advance. The readable/detectable nature of the watermark heavily affects the way it can be used in practical applications.

Visible and invisible watermarking are two categories of digital watermarking. The concept of the visible watermark is very simple; it is analogous to stamping a mark on paper. The data is said to be digitally stamped. An example of visible watermarking is seen in television channels when their logo is visibly superimposed in the corner of the screen. Invisible watermarking, on the other hand, is a far more complex concept. It is most often used to identify copyright data such as author, distributor, etc. This paper focuses on this category, and the word "watermark" will mean, by default, the invisible watermark.

The most suitable data for watermarking are still images, video, and audio [2]. It is important to point out that not all digital data are suitable for watermarking, despite their capacity to be watermarked and, therefore, require some other means of protection. For example, executable files are not suitable for watermarking because they can easily be converted to a canonical format and thus lose the watermark. Another unsuitable media is text, which has been watermarked simply by introducing slight shifts between characters and lines. The problem with this is that using a commercial optical-character-recognition (OCR) package [1] can circumvent the watermark.

The main contribution of this paper is to present a new watermarking scheme that is based on discrete cosine transform (DCT) and Joint Photographic Experts Group (JPEG) model in the feature domain. It also gives an up-to-date overview of the field of watermarking. Section II presents the main applications and properties of watermarking. Section III elaborates on the techniques of digital watermarking. The proposed watermarking scheme is presented in Section IV. This is followed by the experiments and results in Section V. Finally, the conclusions are presented in Section VI.

II. Applications and Properties

The two major applications for watermarking are protecting copyrights and authenticating photographs. The main reason for protecting copyrights is to prevent image piracy when the provider distributes the image on the Internet [4]. One way to achieve this goal is by embedding a digital watermark that automatically adjusts itself during image modification [4]. The practice of using images as evidence against crimes, for example, assumes that the images are reliable. Ensuring this requires image authentication [4], [5]. Ensuring the authenticity of an image, i.e., that it has not been tampered with, is needed by many organizations, such as hospitals, insurance companies, etc. Many methods are used to authenticate physical images, but this is not the case for digital images. Digital images must be authenticated by digital means. One method authenticates digital images by embedding a digital watermark that breaks or changes as the image is tampered with. This informs the authenticator that the image has been manipulated. In the case of images captured by a digital camera, this can be accomplished by a special chip in the camera, which encrypts a watermark into captured images. This technique can also be applied to video and audio formats as well.

There are three functional components that are required in order to embed a watermark in an image. These are a water-

Manuscript received May 14, 2002; revised April 19, 2003.

M. A. Suhail is with the University of Bradford, Bradford, U.K.

M. S. Obaidat is with the Department of Computer Science, Monmouth University, West Long Branch, NJ 07764 USA (e-mail: Obaidat@monmouth.edu; http://www.monmouth.edu/mobaidat).

Digital Object Identifier 10.1109/TIM.2003.817155

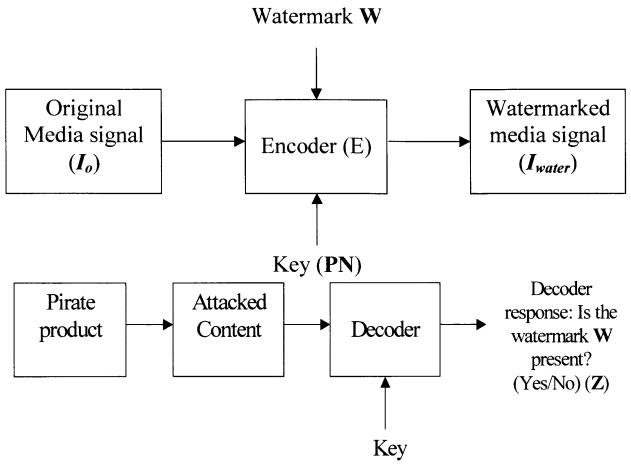

Fig. 1. Embedding and detecting systems of digital watermarking.

mark carrier, a watermark generator, and a carrier modifier. A watermark carrier is a list of data elements from the original image used for encoding the watermark. The watermark is a sequence of noise-like signals, based on a secret decryption key and generated pseudorandomly. The carrier modifier adds the generated noise signals to the selected carrier [2]. Embedding the watermark and detecting the watermark are the operations in the watermarking of digital media, which enable the owner to be identified [3]. The watermarking scheme can be represented symbolically by

$$I_W = E(I_0, W) \tag{1}$$

where I_0, W, and I_W denote the original multimedia signal (audio, image or video), the watermark containing the information that the owner wishes to embed, and the watermarked signal, respectively. The embedding function E modifies I_o according to W. Fig. 1(a) shows a general watermarking scheme. For watermark detection, a detecting function D is used. This operation is represented by

$$W' = D(R, I_0) \tag{2}$$

where R is the signal to be tested, whether it is watermarked or not and R could be a distorted version of I_W. The extracted watermark sequence (W') is compared with W and a Yes/No decision is made. The decision is based on a correlation measure Z, as follows:

$$Z(W', W) = \begin{cases} 1, & c \geq \gamma_0 \\ 0, & \text{otherwise} \end{cases} \tag{3}$$

where c is the value of the correlation and γ_0 is a positive threshold. The detection process is shown in Fig. 1(b). Watermarking techniques that are intended to be widely used must satisfy several requirements. The type of application decides which watermarking technique to be used. However, three requirements have been found to be common to most practical applications and the discussion below concentrates on these.

A. Watermark Imperceptibility

The watermark should be hidden in the media signal in such a way that it cannot be seen. However, watermark invisibility can conflict with other requirements such as robustness. Sometimes it is necessary to exploit the characteristics of the human visual system (HVS) or the human auditory system (HAS) in the watermarking embedding process [1]. The watermark should also be statistically invisible. An unauthorized person should not be able to detect the watermark using statistical methods.

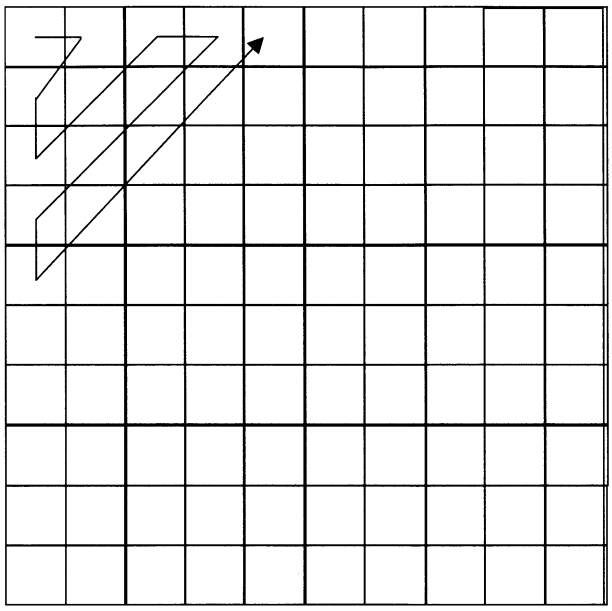

Fig. 2. Zig-zag ordering for the JPEG model.

B. Robustness

The watermark should be detectable even if intentional or unintentional attacks are made on the watermarked image. If this is the case, then the watermark is robust. To achieve a high degree of watermark robustness, the watermark must be placed in significant parts of the media signal. In the case of image watermarking, resistance to geometric manipulations, such as translation, resizing, rotation, and cropping is still an open issue.

C. Detecting the Watermark

The probability of failing to detect the embedded watermark and detecting a watermark when, in fact, one does not exist, must be very small even after the media has been subjected to attacks or signal distortion. As a result, detection of the embedded watermark proves the ownership of the media signal.

It must be understood that the above requirements compete with each other. Also, other requirements [1]–[3] may be significant. Different watermarking applications result in the corresponding design requirements. In any case, a watermarking technique should be widely accepted and used on a large, commercial scale, so that it might then stand up in a court of law.

III. Techniques of Digital Watermarking

Current techniques to be found in the literature for watermarking concentrate mainly on images and can be grouped into two main classes. The first group includes transform domain methods, which embed the data by modulating the transform

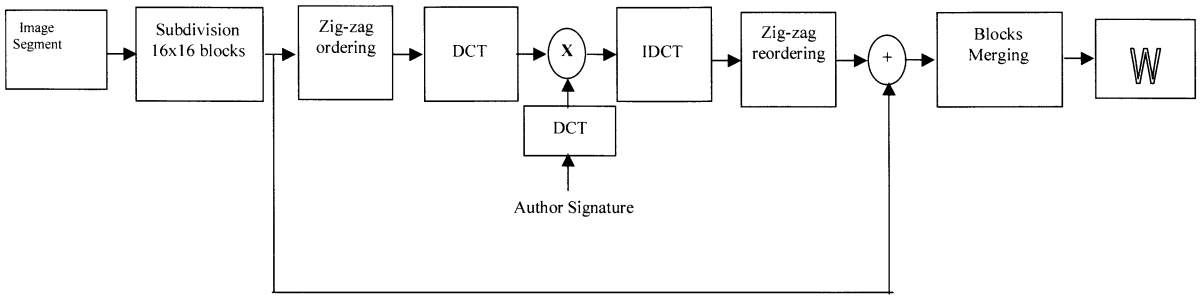

Fig. 3. Proposed watermarking scheme based on JPEG model.

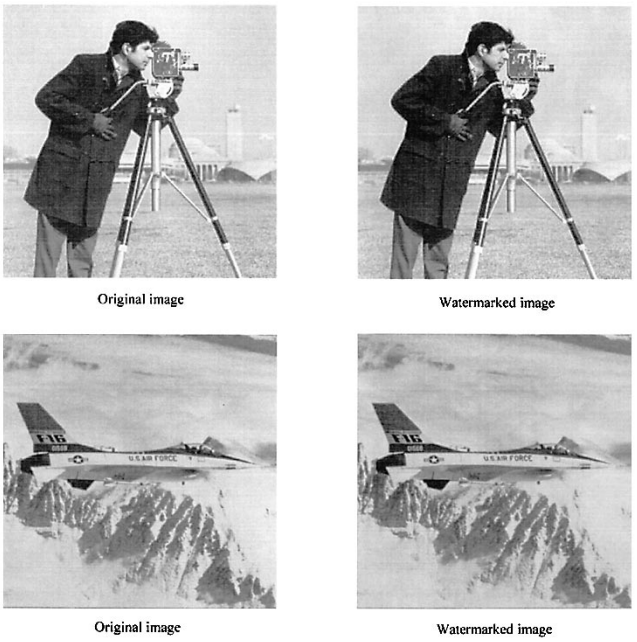

Fig. 4. "Cameraman" and "F16" images and their watermarked images.

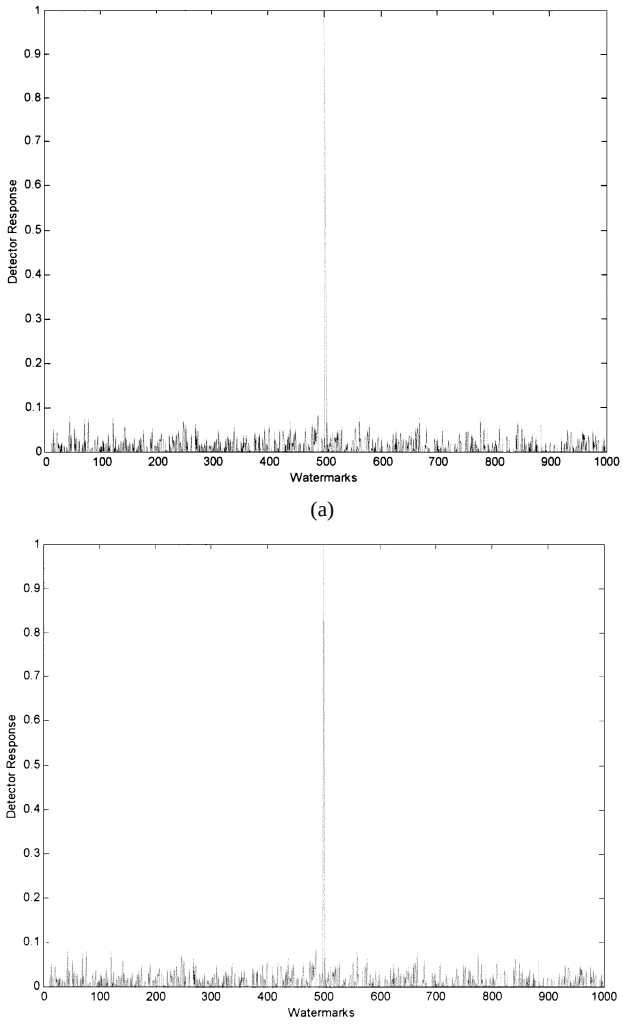

Fig. 5. Detector response correlates the extracted watermark with the embedded one to measure robustness and detection capability of the proposed algorithm. (a) Cameraman image. (b) F16 image.

domain coefficients. The other group includes spatial domain techniques. These embed the watermark by directly modifying the pixel values of the original image. The transform domain techniques have been found to give better robustness to common signal distortion. There are numerous papers that deal with watermarking schemes. However, some of these approaches share common principles and in this section these watermarking techniques are reviewed briefly.

Some of the watermarking techniques are based on adding fixed amplitude pseudonoise (PN) sequences to an image that are utilized as a "spreading key." In this case, the watermark is treated as a transmitted signal in a spread spectrum system and the host media is considered to be noise. The PN sequence is used to spread the data bits over the spectrum to hide the digital watermark. According to Hartung [3], most proposed watermark methods utilize the spatial domain. This may be due to the simplicity and efficiency of such methods.

A. Spatial Domain Techniques

To design a digital watermark in the spatial or temporal domains, these approaches need to modify the least significant bits (LSB) of the host data. These lowest order bits are visually insignificant, so the watermark will be invisible. After embedding it, the watermark is recovered using knowledge of the PN sequence and watermark location [2]. Also, the statistical properties must be known for the recovery process. Two LSB techniques are described in [9]. The first replaces the LSB of the image with a pseudonoise (PN) sequence, while the second adds a PN sequence to the LSB of the data. In [6], a direct sequence spread spectrum technique is proposed to embed a watermark in audio signals. Another PN sequence

spread spectrum approach is proposed in [8], where the data are hidden by adding a fixed-amplitude PN sequence to the image. In [8], a fixed-amplitude two-dimensional (2-D) PN sequence is obtained from a long one-dimensional (1-D) PN sequence to the image.

The spatial domain approaches, which modify the LSB of the data using a fixed magnitude PN sequence, are highly sensitive to signal processing operations and are easily corrupted. The watermark must also be invisible and those portions (smooth regions) of the image or audio limit the magnitude of the embedded noise, which most clearly reveal the embedded noise.

B. Transform Domain Techniques

Many transform based watermarking techniques have been proposed. To embed a watermark, a transformation is applied to the host data. Then, modifications are made to the transform coefficients. Possible image transformations include the fast Fourier transform (FFT), DCT, wavelet, sub-band coding, fractal, and others.

DCT Transform: The first efficient watermarking scheme was introduced by Koch *et al.* [3]. In their method, the image is first divided into square blocks of size 8×8 for DCT computation. A pair of mid-frequency coefficients is chosen for modification from 12 predetermined pairs. Bors and Pitas [9] developed a method that modifies DCT coefficients satisfying a block site selection constraint. After dividing the image into blocks of size 8×8, certain blocks are selected based on a Gaussian network classifier decision. The middle range frequency DCT coefficients are then modified, using either a linear DCT constraint or a circular DCT detection region [9]. A DCT domain watermarking technique based on the frequency masking of DCT blocks was introduced by Swanson [10]. Cox [6] developed the first frequency-domain watermarking scheme.

Wavelet Transform: multiresolution-based methods were first introduced in [11]. Their watermark is defined by a pseudorandom 2-D sequence. The image and watermark are first decomposed using a 2-D wavelet transform and then the watermark is embedded in the image. Subsequently, several wavelet-based schemes have been introduced. The difference between these methods depends on the way the watermark is weighted. The reason for this is to reduce the presence of visual artifacts [2].

Fractal Transform: There are not many papers that describe invisible watermarks based on the fractal transform. This might be because of the computational complexity and cost of the fractal transform. Puate and Jordan [12] have used fractal compression analysis to embed a signature in an image. In fractal analysis, similar patterns are identified in an image. However, only a limited amount of binary code can be embedded using this method. This technique may not be suitable for general use because fractal analysis is computationally expensive and some images do not have many large self-similar patterns.

IV. Proposed Watermarking Scheme

Our proposed scheme is based on embedding a pseudorandom sequence of real numbers in the DCT coefficients of each segment of the host image. It relies on some of the ideas proposed by Cox *et al.* [6]. In our scheme, rather than embedding the watermark globally in the host image as the Cox algorithm, the host image is first segmented in different segments based on Voronoi diagram and the feature extraction points. Then, a pseudorandom sequence of real numbers is embedded in the DCT domain of each image segment. This will boost the watermark robustness with affecting the invisibility.

Fig. 6. Watermarked image after passing through median filter of size 9×9.

We will be using the Voronoi diagram to define group of segments in the host image based on feature points to be watermarked. There are several ways to generate the Voronoi diagram [13]–[15]; we use an optimal method known as the plane sweep algorithm or Fortune's algorithm [13]. The strategy in the plane sweep algorithm is to sweep a horizontal line—the sweep line—from top to bottom over the image. While the sweep is performed, information is maintained about the intersection of the structure with the sweep line. When the sweep line moves downwards, the information does not change, except at certain special points—the event points. The feature extraction point which is used to form the Voronoi cells is built based on Tommasini *et al.* algorithm [16].

The 2-D forward DCT kernel used in our algorithm can be defined as

$$g(x,y,0,0) = \frac{1}{N} \tag{4a}$$

$$g(x,y,u,v) = \frac{1}{2N^3}[\cos(2x+1)u\pi][\cos(2y+1)v\pi] \tag{4b}$$

for $x, y = 0, 1, \ldots, N-1$, and $u, v = 0, 1, \ldots, N-1$ [8]. Here, a watermark consists of a sequence of randomly generated real numbers. These numbers have a normal distribution with zero mean and unity variance

$$W = \{w_1, w_2, \ldots, w_N\}. \tag{5}$$

Then, the DCT of the whole image is computed. The DCT coefficients are chosen to be watermarked. After that, the watermark is added by modifying the DCT coefficients of each segment

$$C = \{c_1, c_2, \ldots, c_N\}. \tag{6}$$

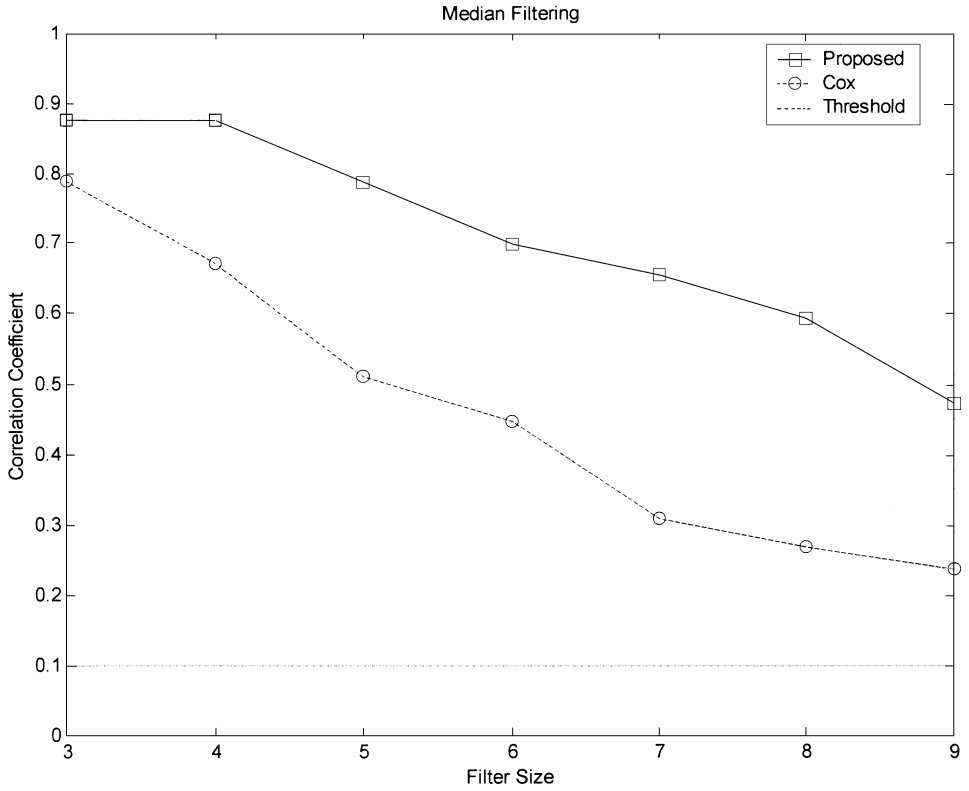

Fig. 7. Correlation output of watermark detector response of different Median filter size.

According to

$$c_i' = c_i + \alpha c_i w_i \tag{7}$$

where $i = 1, 2, \ldots, N$, and α is a coefficient for tuning robustness that is taken here to be $\alpha = 0.1$ (empirical value). If the original image can be denoted by I_0 and the watermarked -possibly distorted- image I_w^*, then, a possibly corrupted watermark W^* can be extracted. The extracting process considers the inverse DCT. The two-dimensional DCT pair is given by the expressions

$$C(0,0) = \frac{1}{N} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x,y) \tag{8a}$$

$$C(u,v) = \frac{1}{2N^3} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x,y)[\cos(2x+1)u\pi] \times [\cos(2y+1)v\pi] \tag{8b}$$

for $u, v = 1, 2, \ldots, N-1$, and

$$f(x,y) = \frac{1}{N} C(0,0) + \frac{1}{2N^3} \sum_{u=1}^{N-1} \sum_{v=1}^{N-1} C(u,v)[\cos(2x+1)u\pi] \times [\cos(2y+1)v\pi] \tag{8c}$$

for $x, y = 0, 1, 2, \ldots, N$. To check the similarity between W, the embedded watermark and W^*, the extracted one, a correlation measured between them can be found using:

$$\rho(W, W^*) = \frac{W \cdot W^*}{\sqrt{W^* \cdot W^*}} \tag{9}$$

where $W \cdot W^*$ is the scalar product between these two vectors.

Fig. 8. Watermarked image after JPEG compression with a compression ration (CR) of 45:01.

In our proposed algorithm, we will not watermark the entire image as done in [6]. However, we will embed the watermark in each segment of the original image. So, for each segment, the image segment is subdivided into pixels of size 8×8 (64 pixels). The DCT of the block is then computed. After that, the DCT coefficients are reordered into a zigzag scan. This reordering is similar to the JPEG compression algorithm [7]. The

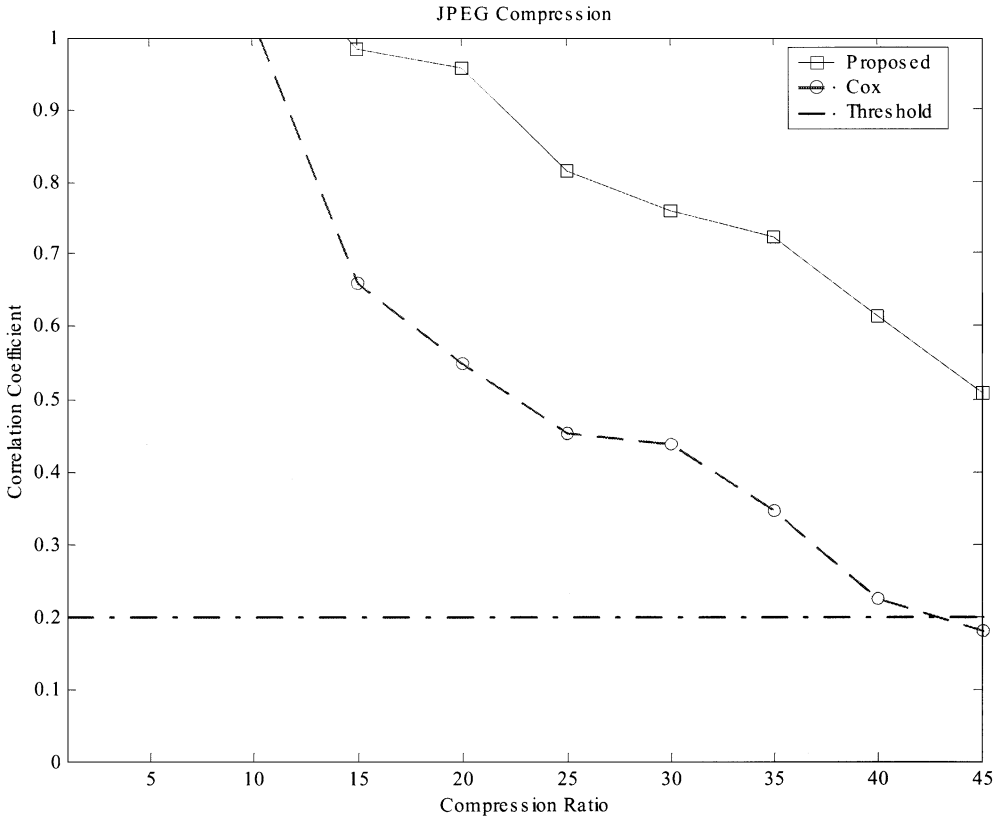

Fig. 9. Correlation output of watermark detector response of successive compression ratios from 5 to 45 using JPEG.

Fig. 10. Remaining percentage after cropping the watermarked image by 50%.

JPEG standard defines three coding systems. One of them is the lossy baseline coding system, which is based on the DCT and is adequate for most compression applications. However, in the proposed watermarking method, we will borrow the concept of zigzag reordering of JPEG model, which is shown in Fig. 2. For more about JPEG, one can refer to [7]. Then, the coefficients in the zigzag ordering of the DCT spectrum are selected. These selected coefficients are modified, according to (7) where c_i is the original DCT coefficient, and w_i is the watermark coefficient. To tune the watermark energy, the term α is used. The higher the α value, the more robust and the more visible the watermark will be. Finally, we need to reverse the above procedure to get our watermarked image. Therefore, the modified DCT coefficients are reinserted in the zigzag scan. Then, the inverse DCT is applied. Finally, the blocks are merged. Thus, we can obtain the watermarked image I_w after merging all image segments. The block diagram of the proposed system is shown in Fig. 3. Also, Fig. 4 shows the original and watermarked image of cameraman and F16 images using the proposed algorithm.

V. Experiments and Results

In order to test the proposed watermark scheme, 1000 watermarks were randomly generated. Different types of images were used in this experiment. Several common signal processing techniques and geometric distortions were applied to these images to evaluate if the detector can reveal the presence of the image owner's watermark. This way, we can measure the algorithm robustness to various kinds of attacks. In this section, we are displaying experimental results obtained on the "cameraman" and "F16" images as in Fig. 4. This Figure shows both the original and watermarked images. The magnitude of the response of the watermark detector to all the code marks is shown in Fig. 5. The response of a given mark is compared to $T_{\rm p}$ ($T_{\rm p} = 0.1$, experimentally found to be the maximum detector response of extracting the virtual watermarks) to decide whether the mark is present or not. On the other hand, if one does not know which is the mark whose presence must be checked, then the responses to all the code marks are compared and the largest one is selected. From Fig. 5, it is clear that the response to the correct mark is stronger than the others. This reflects the possibility of achieving very low false positive and false negative rates.

The watermarked images are exposed to common image processing operations including the geometric manipulations to test the algorithm robustness. The results of median filtering, JPEG compression, and cropping are discussed. Also,

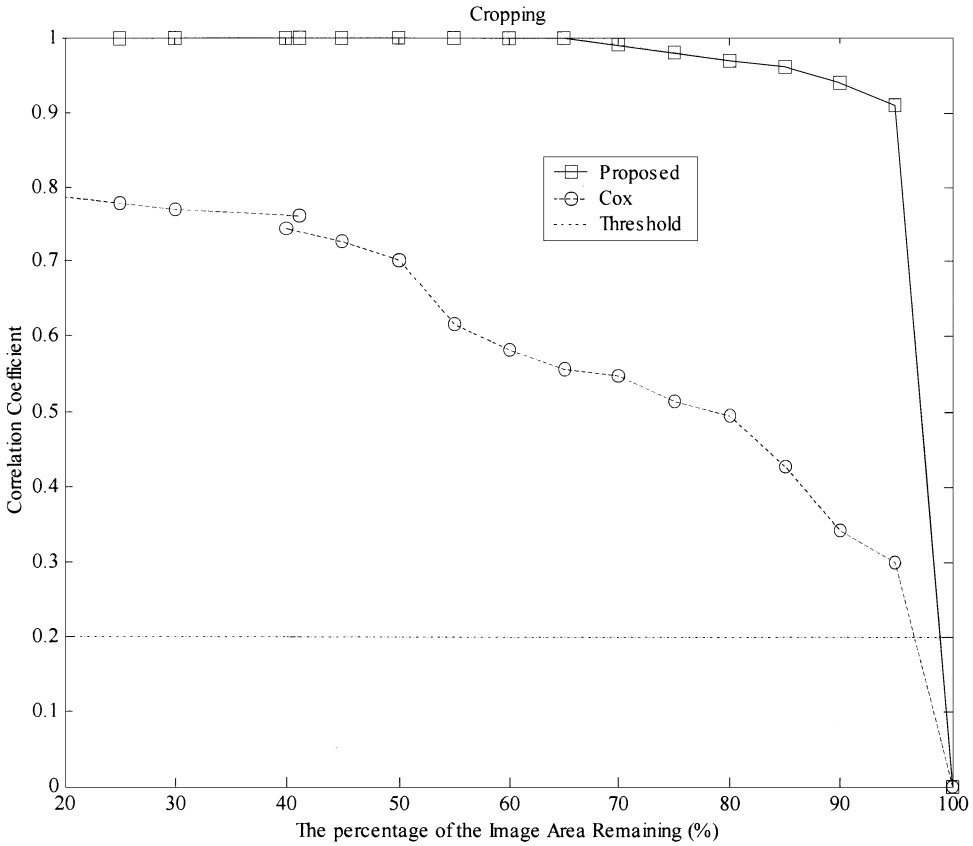

Fig. 11. Correlation coefficient as a function of the percentage of the image area remaining.

a comparison with Cox algorithm will be provided. In the median filtering, the value of an output pixel is determined by the median of the neighborhood pixels. Median filtering is able to remove the outliers in the image without reducing the sharpness of the image. Fig. 6 show the results for the median filtering, of size 9×9. The results show that the robustness of our system still good even with larger sizes of the filters. This is shown in Fig. 7, where the effect of image filtering on watermark detection as the output of correlation coefficient versus the filter size is displayed. Also, this figure shows that when the watermarked image is watermarked based on the proposed scheme then filtered using median filtering, it will not have a severe impact on the watermarking robustness as it has when it is watermarked based on Cox algorithm.

The watermarked images are exposed to JPEG for different compression ratios (CRs). The watermarked image exposed to JPEG of compression ratio 1:45 is shown in Fig. 8. The resulting compressed image shows visible blocking artifacts as displayed in the Figure. The correlation coefficients of the watermarking detector after compression using JPEG is presented in Fig. 9. The JPEG compression attack results in compression ratios ranging from 1:1 (no compression) to 45:1. To achieve compression, high frequency discrete cosine transform (DCT) terms can be eliminated without affecting the image quality, but it might affect the integrity of the watermark information placed in the high frequency terms. This is clear form Fig. 9 which reveals that the robustness declines as the watermarked image is compressed more. However, the proposed system robustness is better than Cox algorithm due to the distribution of the watermark in all DCT coefficients of the host image.

Following the watermark insertion, the images were cropped, and the detection procedure was applied. A percentage of the image is cropped from 10% to 90%. The watermarked image cameraman is cropped, and the remaining percentage 50% of the watermarked image is displayed in Fig. 10. The corresponding correlation output at each cropping level is shown beside the remaining image. The correlation coefficient as a function of the percentage of the image area remaining is displayed in Fig. 11. It can be concluded from this figure that the proposed system method is robust enough to the cropping attack, even when only a small percentage of the image area remains. The correlation coefficient for the proposed technique is high and above the detection threshold. This is because the watermark is inserted in each watermark segment as explained. Fig. 11 also demonstrates the superiority of our system compared to the Cox scheme. This is because the watermark at the DCT watermark coefficients in the Cox algorithm is inserted globally throughout the image content, which leads to losing some of these coefficients while the watermarked image is cropped.

VI. Conclusion

To conclude, we have presented a new robust watermarking scheme and demonstrated its superior performance using different experiments. The results of experiments show that this approach is very promising, because it is robust to common image processing distortions. Our proposed system outperforms the Cox algorithm. For the compression attacks, it is found that the robustness against JPEG compression is achieved for a compression ratio (CR) of up to 45. Moreover, robustness against

average, median and Wiener filters is shown for the 3×3 up to 9×9-pixel neighborhood. Also, the proposed system is inherently resistant to geometric manipulation. This is because we are utilizing the robust extracted features, which are covariant to these geometric transformations. It is observed that robustness against scaling was achieved when the watermarked image size is scaled down to 0.4 of its original size. Finally, we have shown that cropping attack is not effective in destroying the watermark.

REFERENCES

[1] C. Busch, W. Funk, and S. Wolthusen, "Digital watermarking: From concepts to real-time video applications," *IEEE Comput. Graphics Applicat.*, vol. 19, pp. 25–35, Jan./Feb. 1999.

[2] M. D. Swanson, M. Kobayshi, and A. H. Tewfik, "Multimedia data-embedding and watermarking technologies," *Proc. IEEE*, vol. 86, pp. 1064–1087, June 1998.

[3] F. Hartung and M. Kutter, "Multimedia watermarking techniques," *Proc. IEEE*, vol. 87, pp. 1079–1106, July 1999.

[4] C.-Y. Lin and S.-F. Change. Multimedia authentication. presented at *Proc. SPIE Int. Conf. Security and Watermarking of Multimedia Contents*. [Online]. Available: http://www.ctr.columbia.edu/~cylin/auth/mmauth.html.

[5] Summaries of current projects: Content-based image/video copyright protection and authentication (1999, Oct.). [Online]. Available: http://www.ee.columbia.edu/~elylin/auth/mmauth.html.

[6] I. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Processing*, vol. 6, pp. 1673–1687, Dec. 1997.

[7] R. Gonalez and P. Wintz, *Digital Image Processing*, Second ed. Reading, MA: Addison Wesley, 1987.

[8] P. Wolfgang and E. Delp, "A watermark for digital images," in *Proc. IEEE Int. Conf. Image Processing*, Lausanne, Switzerland, Sept. 1996, pp. 219–222.

[9] A. Bors and I. Pitas, "Image watermarking using DCT domain constraints," in *Proc. IEEE. Int. Conf. Image Processing*, Lausanne, Switzerland, Sept. 1996, pp. 231–234.

[10] M. Swanson, B. Zhu, and A. Tewfik, "Transparent robust image watermarking," in *Proc. IEEE. Int. Conf. Image Processing*, Lausanne, Switzerland, Sept. 1996, pp. 211–214.

[11] J. J. K. O'Ruanaidh, W. J. Dowling, and F. M. Boland, "Watermarking digital images for copyright protection," *Proc. Inst. Elect. Eng. Vision, Signal, and Image Processing*, vol. 143, no. 4, pp. 250–256, Aug. 1996.

[12] J. Puate and F. Jordan. Using compression scheme to embed a digital signature into an image. [Online]. Available: http://iswww.epfl.ch/~jordan/watremarking.html.

[13] W. Guan and S. Ma, "A list-processing approach to compute Voronoi diagrams and the Euclidean distance transform," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 20, July 1998.

[14] M. Berg, M. Kreveld, M. Overmars, and O. Schwarzkopf, *Computational Geometry: Algorithms and Applications*. Berlin, Germany: Springer, 1997.

[15] R. Klein, *Concrete and Abstract: Voronoi Diagrams*. Berlin, Germany: Springer-Verlag, 1987.

[16] T. Tommasini, A. Fusiello, E. Trucco, and V. Roberto, "Marking good features track better," in *IEEE Conf. Computer Vision and Pattern Recognition*, June 1998, pp. 178–183.

Mohamed A. Suhail (M'02) received the Ph.D. degree in telecommunications and electronics, with a minor in multimedia and information technology, from the University of Bradford, U.K., and the MS. dgree in electrical engineering from King Fahd University of Petroleum and Minerals, Saudi Arabia.

He has has published over 16 refereed technical articles in refereed scholarly international journals and proceedings of refereed international conferences. He contributed to a book entitled *Trends in Industrial and Applied Mathematics* (Dordrecht, MA: Kluwer, 2002). His research interests include signal processing, watermarking algorithms and applications, wavelet applications, applied neural networks and pattern recognition, and computer security.

Mohammad S. Obaidat (SM'90) received the M.S. and Ph.D. degrees in computer engineering, with a minor in computer science, from the Ohio State University, Columbus.

He is currently a tenured Full Professor of computer science at Monmouth University, West Long Branch, NJ. Among his previous positions are Chair of the Department of Computer Science and Director of the Graduate Program at Monmouth University and Faculty Member at the City University of New York. He has received extensive research funding and has published over 270 refereed technical articles in refereed scholarly international journals and proceedings of refereed international conferences. He is author of the book *Fundamentals of Performance Evaluation of Computer and Telecommunications Systems* (New York: Wiley, 2003). He is the coauthor of the two books *Wireless Networks* and *Multiwavelength Optical LANs* (New York: Wiley, 2003) and coauthor of the book *Security of E-based Systems* (Cambridge, U.K.: Cambridge University Press 2004). He is the Co-Editor of the book *Applied System Simulation: Methodologies and Applications* (Norwell, MA: Kluwer, 2003). He has served as a Consultant for several corporations and organizations worldwide. He is the Chief Editor of the *International Journal of Communication Systems*. He is also a Technical Editor of *Simulation: Transactions of the Society for Modeling and Simulations (SCS) International TSCS*. He is an Associate Editor/Editorial Board Member of seven other refereed scholarly journals, including Elsevier's *Computer Communications Journal* and *Journal of Computers and Electrical Engineering* and Kluwer's *Journal of Supercomputing*. He has guest edited several special issues of the *Simulation Journal* and of Elsevier's *Computer Communications Journal*, *Performance Evaluation Journal*, and *Journal of Computers and Electrical Engineering*. He is the Founder of the International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS) and has served as the General Chair of SPECTS'98, SPECTS'99, SPECTS'01, SPECTS'02, and SPECTS2003. He is the Founder and First Chairman of the SCS Technical Chapter (Committee) on Performance Evaluation of Computer and Telecommunication Systems. He has been invited to lecture and give keynote speeches worldwide. His research interests include performance evaluation of computer and telecommunications systems, modeling and simulation, telecommunications and computer networking, wireless networks, high performance and parallel computing/computers, applied neural networks and pattern recognition, computer security, instrumentation and measurement, and speech processing. He has served as the Sceitific Advisor/Program Leader for the World Bank/UNDP Workshop on Fostering Digital Inclusion which is part of the MDF-4.

Dr. Obaidat is a Fellow of the Society for Computer Simulation International and a member of the Board of Directors of the Society for Computer Simulation International and is currently the Vice President of Conferences of the Society for Modeling and Simulation International (SCS). He is an Associate Editor/Editorial Board Member of three IEEE Transactions. He has also guest edited two special issues of the IEEE TRANSACTIONS ON SYSTEMS, MAN AND CYBERNETICS (SMC), one titled Neural Network Applications and the other titled Learning Automata: Theory, Paradigms, and Applications. He has served as the Steering Committee Chair, General Chair, Program Chair, or Vice Chair of many international conferences, including the 1995 IEEE International Conference on Electronics, Circuits, and Systems, the 1996 IEEE International Phoenix Conference on Computers and Communications, the 1997 and 1998 IEEE International Performance, Computing, and Communications Conference, the 1997, 1998, 1999, 2000, 2001, 2002, and 2003 Summer Computer Simulation Conference, the 1997 IEEE International Conference on Computer Communications and Networks, and the 2001 International Conference on Parallel Processing. Between 1994 and 1997, he served as Distinguished Speaker/Visitor of the IEEE Computer Society. Since 1995, he has been serving as an ACM Distinguished Lecturer. Between 1996 and 1999, he served as an IEEE/ACM program evaluator of the Computing Sciences Accreditation Board/Commission (CSAB/CSAC). Recently, he was awarded a Nokia Research Fellowship and he has received a recognition certificate from the IEEE.