INFORMATICA, 2006, Vol. 17, No. 2, 187–198

A Copyright Protection using Watermarking Algorithm *

Abou Ella HASSANIEN
Quantitative Methods and Information Systems Department
College of Business Administration, Kuwait University, Kuwait
e-mail: abo@cba.edu.kw, a.hassanien@fci-cu.edu.eg

Received: June 2005

Abstract. In this paper, a digital watermarking algorithm for copyright protection based on the concept of embed digital watermark and modifying frequency coefficients in discrete wavelet transform (DWT) domain is presented. We embed the watermark into the detail wavelet coefficients of the original image with the use of a key. This key is randomly generated and is used to select the exact locations in the wavelet domain in which to embed the watermark. The corresponding watermark detection algorithm is presented. A new metric that measure the objective quality of the image based on the detected watermark bit is introduced, which the original unmarked image is not required for watermark extraction. The performance of the proposed watermarking algorithm is robust to variety of signal distortions, such a JPEG, image cropping, geometric transformations and noises.
Key words: discrete wavelet transforms, watermarking, image distortions, copyright protection, e-security.

1. Introduction

The rapid expansion of the Internet and the overall development of digital technologies in the past years have sharply increased the availability of digital multimedia content. One of the great advantages of digital data is that it can be reproduced without loss of quality. However, it can also be modified easily. In many contexts, such for legal evidence and for video security systems, any modifications of image, video or audio data have to be detected. Therefore, some work needs to be done in order to develop security systems to protect the information contained in digital data (Cox, 1997).

Watermarking (Chiou, 1999; Cox, 2002; Cox, 2001; Nikolaidis, 1996; Wolfgang, 1996; Wolfgang, 1999) is the process of embedding data into a multimedia element such as an image, audio or video file. This embedded data can later be extracted from, or detected in, the multimedia for security purposes. A watermarking algorithm consists of the watermark structure, an embedding algorithm, and an extraction, or detection, algorithm. Watermarks can be embedded in the pixel domain or a transform domain. In multimedia applications, embedded watermarks should be invisible, robust, and have a high capacity.

*This work was supported by Kuwait University, Research Grant Number [IQ05/04].

In the classification of watermarking schemes, an important criterion is the type of information needed by the detector. For example, non-blind schemes require both the original image and the secret key(s) for watermark embedding, and semi-blind schemes require the secret key(s) and the watermark bit sequence; while blind schemes require only the secret key(s).

The most important uses of watermarks include copyright protection and ownership authentication for the multimedia data that flourish at the advent of the Internet (Chang, 2002; Nikolaidis, 1996; Petitcolas, 2000). The requirements for digital watermarks in these scenarios are different. Identification of the origin of content requires the embedding of a single watermark into the content at the source of distribution. To trace illegal copies, a unique watermark is needed based on the location or identity of the recipient in the multimedia network. In both of these applications, non-blind schemes are appropriate as watermark extraction or detection needs to take place in a special laboratory environment only when there is a dispute regarding the ownership of content. For access control, the watermark should be checked in every authorized consumer device, thus requiring semi-blind or blind schemes. Note that the cost of a watermarking system will depend on the intended use, and may vary considerably. A lot of effort has been dedicated to the development or robust watermarking schemes to achieve these goals, the study of watermarking has moved in force to the transformed domains induced by such as DCT and wavelets. In particular, wavelet based transforms and algorithms gained much popularity in recent years (AboulElla, 2005; Shen, 2003; Wang, 2002; Zhu, 1998). These include adding pseudo-random codes to the large coefficients at the high and middle frequency bands, storing filters as the private authentication data, and embedding decomposed watermarks of different resolutions into the corresponding resolution of the decomposed images. In a wavelet-transformed domain, a traditional scheme will typically embed a watermark by superposing or replacing a selected sub-band with a signature image pattern.

In this paper, we introduce a robust image watermarking algorithm for copyright protection based on two-dimensional discrete wavelet transform using Human Visual System (HVS). To make watermark robust we embed the watermark in the higher level sub-band (but not in the scaling coefficients), even though it may affect the perceptual invisibility of the image. By carefully embedding the watermark, it will not cause much change in the image fidelity. The wavelet transform breaks an image down into four sub-sampled, or images. The results consist of one image that has been high pass in the horizontal and vertical directions, one that has been low passed in the vertical and high passed in the horizontal, and one that has been low pass filtered in both directions.

The rest of this paper is organized as follows. A brief description about the watermark methodology is given in Section 2. A proposed watermark in wavelet domain algorithm is discussed in Section 3. Finally, experimental results are given in Section 4 and concluding remarks are made in Section 5.

2. Watermark Methodology

Watermarking is not a new technique. It is descendent of a technique known as steganography which has been in existence for at least a few hundred years (Chiou, 1999; Podilchuk, 2001). Steganography is a technique for concealed communication. In contrast to cryptography where the content of a communicated message is secret, in steganography the very existence of the message that is communicated is a secret and its presence is known only by parties involved in the communication (Chiou, 1999). Steganography is technique where a secret message is hidden within another unrelated message and then communicated to the other party. Some of the techniques of steganography like use of invisible ink, word spacing patterns in printed documents, coding messages in music compositions, etc., have been used by military intelligence since the times of ancient Greek civilization. Watermarking can be considered as a special technique of steganography where one message is embedded in another and the two messages are related to each other in some way. The most common examples of watermarking are the presence of specific patterns in currency notes which are visible only when the note is held to light and logos in the background of printed text documents. The watermarking techniques prevent forgery and unauthorized replication of physical objects. Digital watermarking is similar to watermarking physical objects except that the watermarking technique is used for digital content instead of physical objects. In digital watermarking a low-energy signal is imperceptibly embedded in another signal. The low-energy signal is called watermark and it depicts some metadata, like security or rights information about the main signal. The main signal in which the watermark is embedded is referred to as cover signal since it covers the watermark. The cover signal is generally a still image, audio clip, video sequence or a text document in digital format.

The digital watermarking system essentially consists of a watermark encoder and a watermark decoder (see Fig. 1). The watermark encoder inserts a watermark onto the host signal and the watermark decoder detects the presence of watermark signal. Note that an entity called watermark key is used during the process of embedding and detecting watermarks. The watermark key has a one-to-one correspondence with watermark signal (i.e., a unique watermark key exists for every watermark signal). The watermark key is private and known to only authorized parties and it ensures that only authorized parties can detect the watermark. Further, note that the communication channel can be noisy and hostile (i.e., prone to security attacks) and hence the digital watermarking techniques should be resilient to both noise and security attacks. Fig. 1 illustrates the digital watermark methodology.

2.1. *The Encoder Process*

Let us denote an image by f, a key by $Key = key_1, key_2, \ldots$ and the watermarked image by WI. E is an encoder function, it takes an image f and a key Key, and it generates a new image which is called watermarked image WI, mathematically,

$$E(f, Key) = WI. \tag{1}$$

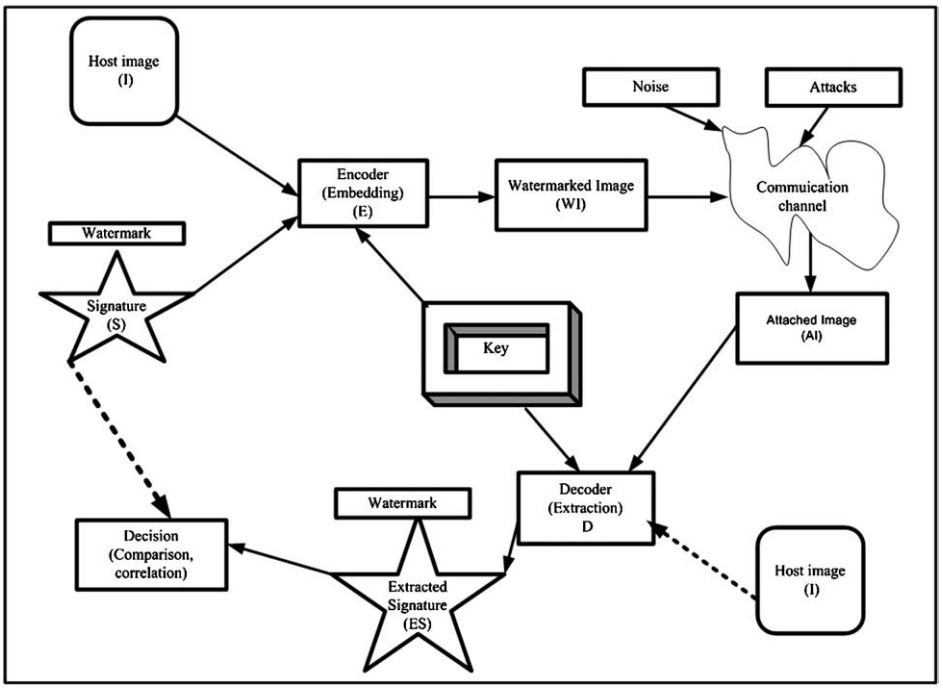

Fig. 1. Digital watermark methodology.

It should be noted that the key may be dependent on image. In such cases, the encoding process still holds.

2.2. *The Decoder Process*

A decoder function D takes an image J (J can be a watermarked or un-watermarked image, and possibly corrupted) whose ownership is to be determined and recovers a signature from the image. In this process an additional image I can also be included which is often the original and un-watermarked version of J. This is due to the fact that some encoding schemes may make use of the original images in the watermarking process to provide extra robustness against intentional and unintentional corruption of pixels. Mathematically,

$$D(J, f) = S. \tag{2}$$

The extracted signature S will then be compared with the owner signature sequence by a comparator function.

3. DWT Watermarking Scheme

The hierarchical property of the DWT offers the possibility of analysing a signal at different resolutions (levels) and orientations. This multiresolution analysis gives both space and frequency localization, and different orientations extract different features of the frame, such as vertical, horizontal, and diagonal information. Through wavelet analysis, an original image can be decomposed into an approximate image LL and three detail images LH, HL and HH. Using wavelet analysis on the approximate image again, four lower-resolution sub-band images will be got, and among them, the approximate image hold most of the information of the original image, while the others contain some details such as the edge. Generally speaking, edges and textures will be represented by large coefficients in the high frequency sub-bands, and they are well localized within the sub-band. In practice, wavelet analysis is performed using multilevel filter banks. Essentially this comprises a succession of filtering and sub sampling operations and has been widely described in the literature (AboulElla, 2005; Chiou, 1999; Wang, 2002; Wolfgang, 1999). The DWT of an image has two parts: an approximation part (this is an image with smaller dimensions) and a detail part (this is a set of images with smaller dimensions containing the details of the original image). Hence the DWT gives the access to the details of the original image. This is very important because changing only the less important details of an image is easy to insert a watermark in this image, keeping the insertion procedure invisible.

Fig. 2 shows three-level wavelet decomposition with gray area indicating highest-frequency components, black area indicating lowest-frequency component, and white areas indicating the hiding places. Where, H and L mean the high pass and low pass filter, respectively. While HH means that the high pass filter is applied to signals of both directions. The results of DWT decomposition are four types of coefficients:

- coefficients that result from a convolution with g in both directions (HH) represent diagonal features of the image;

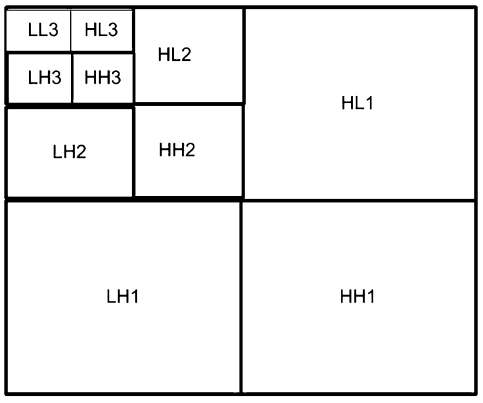

Fig. 2. DWT pyramid decomposition of an image.

- coefficients that result from a convolution with g on the columns after a convolution with h on the rows (HL) correspond to horizontal structures;
- coefficients from high pass filtering on the rows, followed by low pass filtering of the columns (LH) reflect vertical information;
- the coefficients from low pass filtering in both directions are further processed in the next step.

We apply discrete wavelet transform 4-times in order to get the 28×3 sub-images (i.e. 84 features). By combining these 84 features in the HH sub-image of the high-pass filter of the fourth transform (HH4) and each average value for the three remaining high-pass filters areas (HH1, HH2, HH3), the dimension of the resulting feature vector is 87. Each value of 87 dimensions has a real value between -1.0 and 1.0. By quantizing each real value into binary form by convert the positive value into 1 and the negative value into 0. Therefore, we can represent the embedded watermark with only 87 bits.

3.1. *The Watermark Embedded Algorithm in Wavelet Domain*

Research into human perception indicates that the retina of the eye splits an image into several frequency channels each spanning a bandwidth of approximately one octave. The signals in these channels are processed independently. Similarly, in multiresolution decomposition, the image is separated into bands of approximately equal bandwidth on a logarithmic scale. It is therefore expected that use of the discrete wavelet transform will allow the independent processing of the resulting components without significant perceptible interaction between them, and hence makes the process of imperceptible marking more effective. Since digital watermarking involves the merging of a watermark with a host signal it follows that wavelets are attractive for the watermarking of images. The technique is "unsupervised" since the original image is not required for watermark extraction (AboulElla, 2005; Cheng, 2001).

In the embedded algorithm, we first decompose the image into several bands with a pyramid structure as shown in Fig. 2, and then add pseudo-random sequence to the large coefficients which are not located in the lowest resolution. DWT Watermark embedded algorithm is composed of four parts: original image, calculation of multi-level thresholds for selecting perceptually significant coefficients, watermark insertion process, and inverse wavelet decomposition (IDWT) of the coefficients with watermarks. Fig. 3 illustrates the overall process of watermark embedded algorithm.

The original image and digital watermark are represented as

$$f = \big\{f(i,j),\ 0 \leqslant i < M_1,\ 0 \leqslant j < M_2\big\}, \tag{3}$$

$$WI = \big\{w(i,j),\ 0 \leqslant i \leqslant N_1,\ 0 \leqslant j < N_2\big\}, \tag{4}$$

where $f(i,j) \in \{0, 1, \ldots, 2^y - 1\}$ is the intensity of pixel (i,j) and y is the number of bits used in each pixel, $w(i,j) \in \{0,1\}$.

To find the perceptually significant wavelet coefficients for each sub-band, the threshold value is calculated according to the decomposition level. For example, in the 3-level

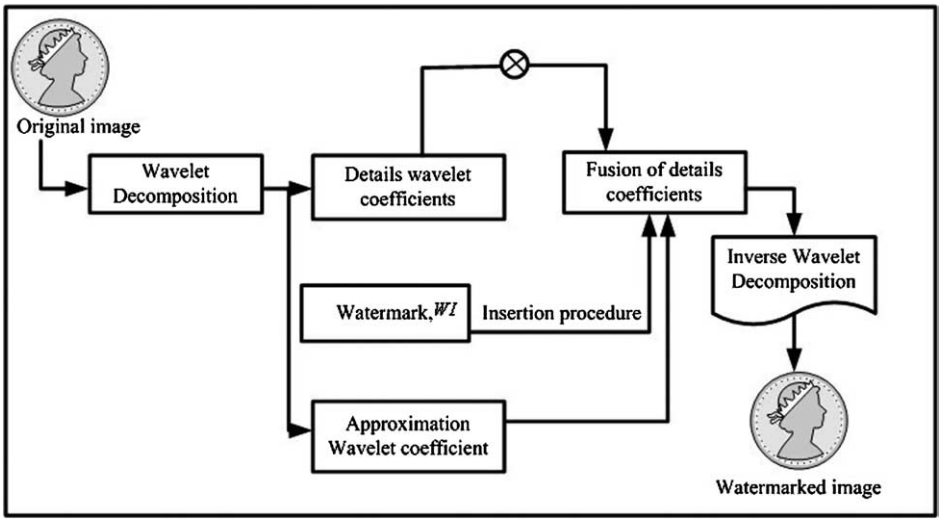

Fig. 3. The embedded algorithm in wavelet domain.

decomposition, the largest coefficients C_1 for 1-level sub-bands (LH_1, HL_1, HH_1) is selected and the threshold T_1 is calculated by Eq. 5. T_2 and T_3 for the subsequent levels are respectively calculated using the same process.

$$T_i = 2^{\lfloor Log_2 C_i \rfloor - 1}, \tag{5}$$

where i is the decomposition level and $\lfloor X \rfloor$ represents the largest integer which is not greater than X.

The watermark embedded algorithm is described as follows:

Algorithm-1: Watermark embed algorithm

Input:

- f be the original image of size$M_1 \times M_2$,
- $WI \in \{-1, 1\}$ be the digital watermark image of size $N_1 \times N_2$.

Processing

1. For $l = 1$ to L
2. For $k = 1$ to K
   - compute $f_{k,l}(m, n)$
3. Generate random key $Key \in \{0, 1\}$
   - if $Key = 0$ then do not embed a mark Else
     - sort the detail coefficients such that:
       $f_{k1,l}(m, n) \leqslant f_{k2,l}(m, n) \leqslant f_{k3,l}(m, n)$

– do quantization by divide $f_{k1,l}(m,n)$ and $f_{k3,l}(m,n)$ into bins using the following form:

$$\Delta = \frac{f_{k3,l}(m,n) - f_{k1,l}(m,n)}{2Q-1}.$$

4. The fused transform coefficients in each band are scaled back to the levels of the original image transform coefficients using the minimum and maximum coefficient values.
   - the fused coefficients f_{useed} are computed as follows:

$$f_{used} = \alpha f_{k,l}(m,n) + W(i,j).$$

5. An inverse transform is now computed to give the watermarked image.

Output: Watermarked image.

We embed the watermark into the detail wavelet coefficients of the original image with the use of a key. This key is randomly generated and is used to select the exact locations in the wavelet domain in which to embed the watermark. For each coefficient within the wavelet domain, the key has a corresponding value of one or zero to indicate if the coefficient is to be marked or not, respectively. The number of ones in the key must be greater or equal to the size of the watermark. The watermark values are repeatedly embedded in different coefficients selected by the key if the length of the watermark is less than the number of ones in the key. Where α the scale factor is determines the relative percentage of the original and watermark image components in the new image. Where Q in the quantization process is user-defined variable and is set to establish an appropriate trade-off between the visibility and robustness of the watermark and $f_{k2,l}(m,n)$ is quantized to the nearest value. We have to note that, an attacker cannot easily determine the exact key given a watermarked image if the specific wavelet transform used in the decomposition is kept a secret and Q is unknown.

3.2. *The Watermark Detection Algorithm in Wavelet Domain*

The aim of the watermark extraction process is to reliably obtain an estimate of the original watermark from a possibly distorted version of the watermarked image. The detection process is inverse procedure of the watermark insertion process. It requires knowledge of the watermarked image $WI(m,n)$ and the key $Key(m,n)$. One of the advantages of wavelet-based watermarking is its ability to spread the watermark all over the image. If a part of the image is cropped, it may still contain parts of the watermark. These parts of watermark may be detected by certain mechanism even if the image has been further scaled or rotated. The watermark extraction algorithm is presented in Fig. 4.

The watermark extraction algorithm is described as follows:

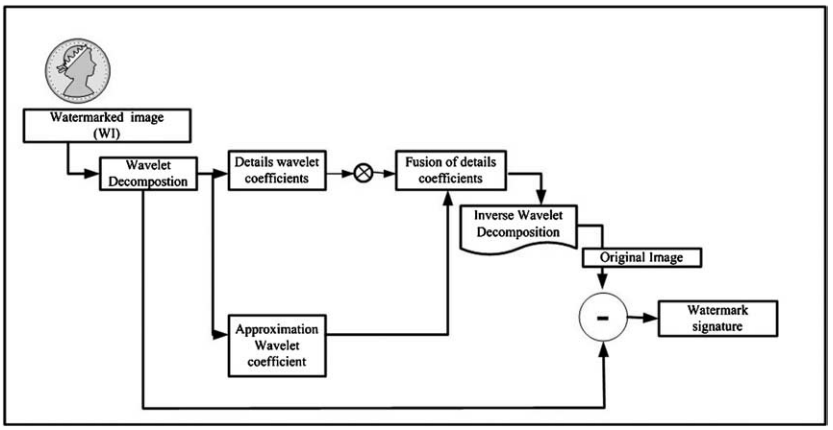

Fig. 4. Watermark extraction algorithm in wavelet domain.

Algorithm-2: Watermark extraction algorithm

Input:

- The watermarked image (attacked image) $WI(m,n)$
- The Key

Processing

1. For $l = 1$ to L
2. For $k = 1$ to K
   - apply Lth level DWT on the watermarked image $WI(m,n)$;
   - compute $f_{k,l}(m,n)$ // Get the image details coefficients;
   - find the closest quantize value Q from relative position of $f_{k2,l}(m,n)$;
   - sort the detail coefficients such that:
     $f_{k1,l}(m,n) \leqslant f_{k2,l}(m,n) \leqslant f_{k3,l}(m,n)$.
3. Check if Q was used to embed a one or a negative one.
4. If the watermark had been embedded in different locations several times, then the most common bit value extracted is assigned for the estimated watermark.
5. If an equal number of ones and negative ones were extracted, then a random guess is made to its value.
6. Set a threshold $\rightarrow T$.
7. Compute the correlation coefficient $\rho(S, \widetilde{S})$ between S (given watermark) and $\tilde{S}$ (extracted watermark) using the following equation:

$$\rho(S,\tilde{S}) = \frac{\sum S(n)\tilde{S}(n)}{\sqrt{\sum S^2(n)\sqrt{\sum \tilde{S}^2(n)}}}.$$

8. If $\rho(S, \widetilde{S}) \geqslant T$ then the watermarked is extracted else go to Step 6.

Output: The original image.

In the Algorithm-2, we use the *key* to find the locations in which the watermark was embedded for each resolution level.

4. Results and Discussion

In this section, some experimental results are demonstrated to show the effectiveness and the robustness of the proposed watermarking algorithm; several 256×256 test images are used for the simulations including Lena, Cameraman, and Baboons.

Figs. 5(a) and 5(b) show the original Lena image and the watermark image, respectively. Fig. 5(c) shows the watermarked image. We see that the watermarked image is not distinguishable from the original image. The watermark length is 750 bits. To evaluate the quality between the attacked image and the original image, first we use Peak Signal-to-Noise Ratio (PSNR). When the PSNR value of a watermarked image is greater than 30 dB, the quality is still acceptable to the human eyes. Table 1 shows PSNR of watermarked images; Lena, Cameraman and Baboon. We separately embedded watermark sequence and considered its results in each level of DWT resolutions (levels 1 to 3). PSNR must require the existences of the original image, which is often not convenient to the receiver. So, we will introduce a new metric that measure the objective quality of the image based on the detected watermark bit. A quality estimation parameter, named the Correct Rate (CR) is computed as an index to the objective quality of the image. Where,

$$\text{CR} = \frac{\text{Number of correctly detected watermark bits}}{\text{Total number of watermark bits}} \tag{6}$$

Table 2 shows we use StirMark 4.0 as a benchmark for testing robustness of a watermarking scheme for predicting the effect on image quality of JPEG compression. To verify the robustness of the introduced algorithm, we use StirMark 4.0[2] to test the robustness of the when image processing is applied as shown in Table 3. The result shows that the introduced algorithm is robust against cropping attack up to 50% of the watermarked image could be resisted.

(a) Lena original image (b) Watermark Image (c) Watermark image Domain

Fig. 5. Results of the proposed algorithm.

[2]StirMark 4.0 as a benchmark for testing robustness of a watermarking scheme.

Table 1
PSNR of watermarked images embedded in levels 1, 2 and 3

PSNR	Level-1	Level-2	Leve-3
Lena	42.12 dB	46.32 dB	54.32 dB
Cameraman	39.24 dB	40.10 dB	51.13 dB
Baboon	37.02 dB	39.21dB	43.09dB

Table 2
The correct rate under the JPEG compression

Image	CR
Lena	0.9775
Cameraman	0.9271
Baboon	0.8862

Table 3
Robustness verification for Lena image

Attack	Correlation
Cropping 50%	0.8921
3x3 Median Filter	0.9226
JPEG compression	0.8652
Rotation 30%	0.9726

5. Conclusion

A robust image watermarking algorithm for copyright protection based on the discreet wavelet transform is presented in this paper. The process of the proposed algorithm, including watermark embedding, and watermark detection, is described in detail The proposed algorithm helps us to place watermark in a higher level sub band with an appropriate energy resulting in watermarked image that has more invisibility but still robust. A new metric that measure the objective quality of the image based on the detected watermark bit is introduced. The experimental results have shown that the proposed watermark is invisible to human eyes and very robust to various attacks, such as image compression, image filtering, geometric transformations and noises.

References

Aboul Ella, H. (2005). Watermarking algorithm for copyright protection using discrete wavelet transform. In *8th International Conference on Pattern Recognition and Information Processing* (*PRIP'05*). May, 18–20, Minsk, Belarus. pp. 121–127.

Chang, C.C., K.F. Hwang and M.S. Hwang (2002). Robust authentication scheme for protecting copyrights of images and graphics. In *IEE Proc. – Vis. Image Signal Process*, vol. 149. pp. 43–50.
Chiou-Ting Hsu and Ja-Ling Wu (1999). Hidden digital watermarks in images. *IEEE Transaction on Image Processing*, **8**(1), 58–68.
Cheng, O., and T.S. Huang (2001). An image watermarking technique using pyramid transform. In *Proc. of the Ninth ACM Multimedia*, Ottawa, Canada. pp. 319–328.
Cox, I.J., and M.L. Miller (2002). The first 50 years of electronic watermarking. *EURASIP JASP*, **2**, 126–132.
Cox, I.J., J. Kilian, T. Leighton and T.G. Shamoon (1997). Secure spread spectrum watermarking for multimedia. *IEEE Trans. on Image Processing*, **6**(12), 1673–1687.
Cox, I.J., M.L. Miller and J.A. Bloom (2001). *Digital Watermarking*. Morgan Kaufmann publisher.
Neil, F.J., D.C. Zoran and J. Sushil (2000). *Information Hiding*: *Steganography and Watermarking – Attacks and Countermeasures*. Kluwer Academic Publishers.
Nikolaidis, N., and I. Pitas (1996). Copyright protection of images using robust digital signatures. In *Proceedings of ICASSP'96*, Atlanta, Georgia. pp. 2168–2171.
Shen, J. (2003). A note on wavelets and diffusions. *J. Comp. Anal. Appl.*, **5**, 147–159.
Shen, J. (2002). On some quantum and analytical properties of fractional Fourier transforms. In D.-X. Zhou (Ed.), *Wavelet Analysis*: *Twenty Year's Developments*. World Scientific. pp. 252–265.
Petitcolas, F.A.P. (2000). Watermarking schemes evaluation. *IEEE Signal Processing*, **17**(5), 58–64.
Podilchuk, C.I., and E.J. Delp (2001). Digital watermarking: algorithms and applications. *IEEE Signal Processing Magazine*, 33–46.
Wolfgang, R.B., and E.J. Delp (1996). A watermark for digital images. In *Proc. ICIP'96*, vol. 3. pp. 219–222.
Wang, Y., J.F. Doherty and R.E. Van Dyck (2002). A Wavelet-based watermarking algorithm for ownership verification of digital images. *IEEE Transactions on Image Processing*, **11**(2), 77–88.
Wolfgang, R.B., C.I. Podilchuk and E.J. Delp (1999). Perceptual watermarks for digital images and video. *Proc. IEEE*, **87**(7), 1108–1126.
Zhu, W., Z. Xiong and Y.Q. Zhang (1998). Multiresolution watermarking for images and video: a unified approach. *IEEE Trans. Circuits Syst. Video Technol.*, **9**, 545–550.

A.E. Hassanien received his BSc with honors in 1986 and MSc degree in 1993, both from Ain Shams University, Faculty of Science, Pure Mathematics and Computer Science Department, Cairo, Egypt. On September 1998, he received his doctoral degree from the Department of Computer Science, Graduate School of Science & Engineering, Tokyo Institute of Technology, Japan. He is an associated professor at Cairo University, Faculty of Computer and Information, Information Technology Department. Currently, he is a visiting professor at Kuwait University, College of Business Administration, Quantitative and Information System Department. Currently, he is a member of the Interim Advisory Board Committee of the International Rough Set Society. His research interests include, rough set theory, wavelet theory, X-ray mammogram analysis, medical image analysis, fuzzy image processing and multimedia data mining. `http://www.cba.edu.kw/abo`

Autorinių teisių apsauga panaudojant vandenženklių algoritmą

Aboul Ella HASSANIEN

Straipsnyje aprašytas vandenženklių algoritmas, pagrįstas diskrečiąja vilnelių transformacija. Vandenženkliai talpinami į aukštadažnias vilnelių komponentes kad sumažinti pradinių skaitmeninių vaizdų iškraipymus. Pasiūlyta tam tikra metrika skirta įvertinti pradinio vaizdo iškraipymo dydžiui remiantis aptiktais vandenženklių bitais. Pateikti eksperimentiniai rezultatai iliustruojantys algoritmo atsparumą skaitmeninių vaizdų kompresijai, filtravimui, geometrinėms transformacijoms ir triukšmui.