# A Copyright Protection Scheme for Gray-Level Images Based on Image Secret Sharing and Wavelet Transformation

Shang-Lin Hsieh and Bin-Yuan Huang
*Computer Science and Engineering, Tatung University, Taiwan*
*slhsieh@ttu.edu.tw*

**Abstract**- *A copyright protection scheme for gray-level images based on image secret sharing and wavelet transformation is proposed in this paper. The scheme contains a secret image generation phase and a watermark retrieval phase. In the generation phase, the proposed scheme extracts the features from a host image using the discrete wavelet transformation (DWT), and then employs the features and the watermark, a visually recognizable pattern, to generate the secret image using the image secret sharing (ISS). In the retrieval phase, the watermark is retrieved by combining the secret image and the features obtained from the suspect image. The retrieved watermark is then compared with the original watermark for copyright verification. The experiment shows that the proposed scheme can withstand 5 kinds of common image processing operations, including JPEG compression, blurring, sharpening, scaling, and cropping.*

***Keywords:*** copyright protection, discrete wavelet transformation, gray-level images, image secret sharing, watermark.

## 1. Introduction

The popularity of the Internet makes copyright protection more and more important today. Because copyright digital media such as images, music, etc. can be copied or distributed quickly and easily on the Internet, media content owners are very concerned about the potential loss of revenue resulting from digital media piracy.

Digital watermarking and fingerprinting are two feasible techniques for copyright verification. Digital watermarking embeds some pattern, called watermark, into the digital media for later verification. On the contrary, fingerprinting does not add anything to the digital media. Instead, special characteristics, known as features, are extracted for later verification.

As mentioned, digital watermarking [1-9] is a technique used to protect the digital media property. Digital watermarking embeds a watermark into the host image. The watermark can be embedded in the spatial domain or the frequency domain. The spatial-domain watermarking scheme changes some pixels in the host image [1-3] while the frequency domain watermarking scheme changes some coefficients obtained from the host image using frequency transformation such as DWT, DCT, and DFT [4-9]. However, both of the watermarking schemes change some pixels of the host image, thus decreasing the image quality.

Fingerprinting [10-13] is another technique used to protect digital media property. Fingerprinting uses features that can uniquely identify an object among others. Features are extracted without altering the host image. Some fingerprinting schemes have been proposed in recent years. A. N. Skodras [10] extracted a matrix as a feature from DCT coefficients of a host image. In the verification phase, a simple point-to-point multiplication of the feature matrix and the matrix obtained from the suspect image is carried out. The result is the number of the same values found at the same positions in both images. However, the scheme performs poorly when noise is added to the image. Chang and Chuang [11] combined the Torus-automorphism technique and the visual secret sharing scheme (VSS) with the watermark to generate a secret image as a feature from the host (public) image. In the verification phase, the Torus-automorphism transformation is used to retrieve the possible public image from the suspect image. Then VSS is applied to retrieve the watermark that could be identified using the human visual system. However, the scheme deteriorates as the JPEG compression ratio increases. Chang et al. [12] also used the Torus-automorphism technique to select pixels of the host image by referring to the watermark image, and then create a mapping table of the selected pixels as a feature. In the verification phase, the mapping table is used to pick up pixels in the suspect image. Then, those selected pixels are used to retrieve the watermark for copyright verification. However, the problem with the scheme is that the retrieved watermark obtained from the host image is different from the original one even when the host image has not been modified.

In this paper, we propose a copyright protection scheme based on image secret sharing (ISS) and discrete wavelet transformation (DWT). The proposed scheme has several advantages. First, it does not modify the host image. Therefore, it is

suitable for the application in which the modification of the image is not allowed. For example, satellite images can not allow any modification on them because it will affect their precision. Second, the scheme is secure. By applying the technique of ISS, only the user who has the secret image can retrieve the watermark. Last, the scheme is robust. The experimental results show that the scheme can withstand 5 kinds of image processing operations.

The rest of this paper is organized as follows. Chapter 2 explains the DWT and the observation. Chapter 3 describes the proposed image protection scheme. Chapter 4 examines the experimental results. Finally, Chapter 5 states the conclusions.

## 2. Consideration on DWT Coefficients

The proposed scheme generates features from the DWT coefficients. This section briefly explains the discrete wavelet transformation and the observation on the DWT coefficients, which leads to the adoption of the $LL_2$ subband.

### 2.1 Discrete Wavelet Transformation

The DWT is identical to a hierarchical subband system. The basic idea of the DWT for an image is described as follows. An image is first decomposed into four subbands $LL_1$, $LH_1$, $HL_1$, and $HH_1$. The subbands $LH_1$, $HL_1$, and $HH_1$ represent the finest scale wavelet coefficients. To obtain the next coarser scale wavelet coefficients, the $LL_1$ subband can be decomposed similarly and divided into four subbands $LL_2$, $LH_2$, $HL_2$, and $HH_2$ . The same decomposing procedure can be applied until there is only one coefficient left in the $LL$ subband. Fig. 1 shows the image "Lena" and it's two-level DWT decomposition.

### 2.2 Observation on DWT Coefficients during Lossy Image Compression

Lossy image compression can effectively attack the features of an image with slightly decreasing the image quality. The SPIHT lossy image compression

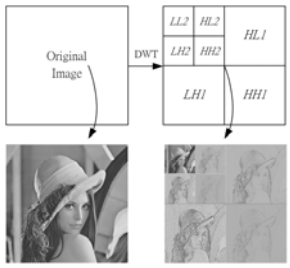



Figure. 1. Two-level DWT decomposition of Lena.

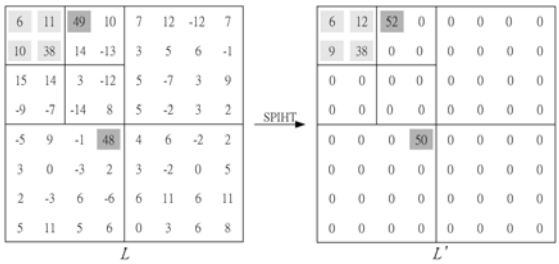



Figure. 2. DWT coefficients after compression.

[14] is one kind of lossy image compression schemes in JPEG 2000. The SPIHT compression uses the characteristic of DWT to discover important coefficients that need to be preserved as well as unimportant coefficients that can be discarded.

To find out which subband of DWT coefficients is reliable after SPIHT compression, the SPIHT is used to compress the image $L$ to obtain the image $L'$, and then DWT is applied two times on $L'$ (Fig. 2 shows an example of the result). We noticed that most of the coefficients in each subband except $LL_2$ became zero and only a small amount of coefficients were preserved after the compression. The coefficients in the $LL_2$ subband were mostly preserved. Moreover, the change of the $LL_2$ coefficients was slighter than that in the other subbands. Hence, the proposed scheme generates features from the coefficients in the $LL_2$ subband.

## 3. The Proposed Copyright Protection Scheme

The proposed scheme contains two phases: *secret image generation* and *watermark retrieval*. Fig. 3 shows the block diagram of the proposed

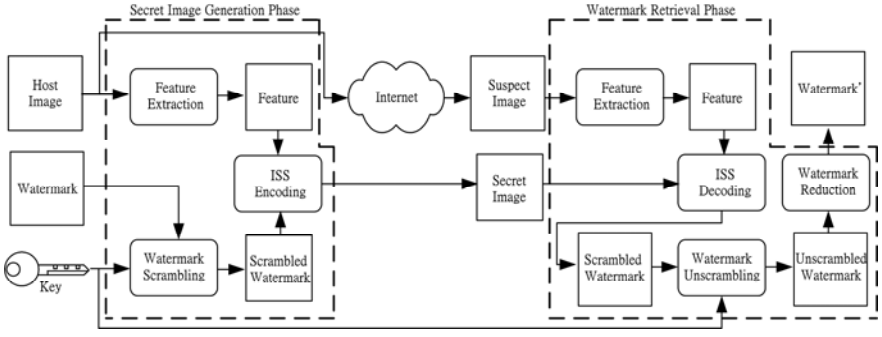



Figure. 3. The block diagram of the proposed scheme.

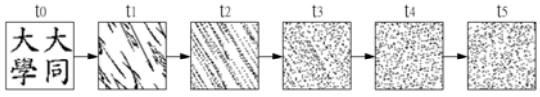



Figure. 4. The scrambled watermark.

scheme. The *feature extraction* in the *secret image generation* phase first extracts the features of the host image. Then, the *watermark scrambling* disarranges the watermark with a secret key. Finally, the *ISS encoding* generates the secret image using the features and the scrambled watermark. To retrieve the watermark, the *feature extraction* in the *watermark retrieval* phase first extracts the features of the suspect image. The *ISS decoding* then uses the features and the secret image to retrieve the scrambled watermark. Next, the *watermark unscrambling* rearranges the scrambled watermark. Finally, the *watermark reduction* regains the watermark. The retrieved watermark is then used to verify the copyright.

## 3.1 The Major Parts in the Proposed Scheme

The proposed scheme contains four major parts. The following sections describe the details of them.

### 3.1.1 Watermarking Scrambling & Unscrambling

Torus-automorphism is used to scramble the watermark in the *secret image generation* phase and unscramble the scrambled watermark in the *watermark retrieval* phase. Voyatzis and Pitas [12] proposed a Torus-automorphism with a single coefficient. The transform function is represented by the following equation:

$$\begin{pmatrix} x_{t+1} \\ y_{t+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ k & k+1 \end{pmatrix} \begin{pmatrix} x_t \\ y_t \end{pmatrix} \bmod N \qquad (1)$$

where ($x_t$ , $y_t$) are the coordinates in the two dimensional space, and $t$ is the number of states. $N$ denotes the size of the given image and $k$ denotes the secret key, which can be arbitrarily chosen by the owner. If a pixel $p$ is placed in the coordinates ($x_0$ , $y_0$), then after $t$ states, the pixel $p$ will be placed in the coordinates ($x_t$ , $y_t$). Fig. 4 shows the watermark that has been scrambled five times using Eq. (1).

### 3.1.2 Feature Extraction

Before the feature extraction, the host image is divided into non-overlapping 8 × 8 blocks and the pixels of each block are transformed to DWT coefficients.

After applying DWT two times, the $LL_2$ subband of each block has four coefficients. Let $M$ be the average of the four coefficients and $C'_n$ ($n$=1, ..., 4) be the four coefficients in descending order (i.e., $C'_1 \geq C'_2 \geq C'_3 \geq C'_4$). The feature type $n$ of this block is obtained by the following equation:

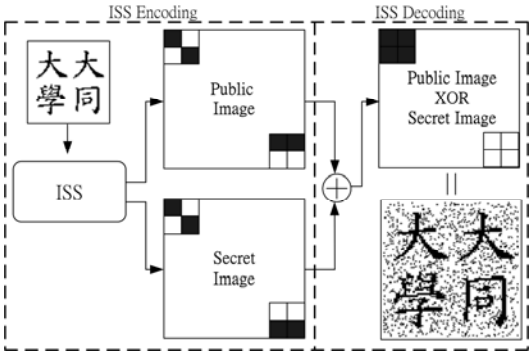



Figure. 5. The image secret sharing scheme.

$$n = \begin{cases} 1, & if \quad C'_1 \geq M > C'_2 \\ 2, & if \quad C'_2 \geq M > C'_3 \\ 3, & if \quad C'_3 \geq M > C'_4 \\ 4, & otherwise \end{cases} \qquad (2)$$

### 3.1.3 ISS Encoding & Decoding

According to the average $M$ and the extracted feature type $n$, a public block (block1) of 2 × 2 pixels is generated. Then, each pixel of the watermark can be mapped into a secret block (block2) of 2 × 2 pixels according to the pixel value of the watermark. The public blocks form the public image and the secret blocks form the secret image.

Fig. 5 shows the proposed ISS scheme. Table 1 lists the mapping table used in the proposed ISS. Each generated image has a size of $2s \times 2s$, when the watermark has a size of $s \times s$.

The encoding process uses the extracted feature types and the watermark to generate the secret blocks of the secret image. The secret block is generated according to one of the following rules:

(a) If a pixel of the watermark is white and the 2 × 2 block1 of the public image is type $n$ ($n$=1, …, 4), then the corresponding secret 2 × 2 block2 in Table 1 is selected.

(b) If a pixel of the watermark is black and the 2 × 2 block1 of the public image is type $n$ ($n$=1, …, 4), then the corresponding secret 2 × 2 block2 in Table 1 is selected.

The decoding process applies XOR operation on the block1 of the public image obtained from the suspect image and the corresponding block2 of the saved secret image generated from the original host image to retrieve the scrambled watermark. The scrambled watermark is then processed by the *watermark unscrambling*.

### 3.1.4 Watermark Reduction

When the original watermark pixel is white and the feature type is 1 or 3, some redundant noise on

Table 1. The mapping table in ISS.

| Feature Type $n$ | Average Location | The watermark pixel is white | | Block1 XOR Block2 | The watermark pixel is black | | Block1 XOR Block2 |
|---|---|---|---|---|---|---|---|
| | | Pubic Block1 | Secret Block2 | | Pubic Block1 | Secret Block2 | |
| 1 | $a \geq M > b,c,d$ | | | | | | |
| | $b \geq M > a,c,d$ | | | | | | |
| | $c \geq M > a,b,d$ | | | | | | |
| | $d \geq M > a,b,c$ | | | | | | |
| 2 | $a,b \geq M > c,d$ | | | | | | |
| | $c,d \geq M > a,b$ | | | | | | |
| | $a,d \geq M > b,c$ | | | | | | |
| | $b,c \geq M > a,d$ | | | | | | |
| | $a,c \geq M > b,d$ | | | | | | |
| | $b,d \geq M > a,c$ | | | | | | |
| 3 | $b,c,d \geq M > a$ | | | | | | |
| | $a,c,d \geq M > b$ | | | | | | |
| | $a,b,d \geq M > c$ | | | | | | |
| | $a,b,c \geq M > d$ | | | | | | |
| 4 | $M = a,b,c,d$ | | | | | | |

| | |
|---|---|
| a b / c d | The four coefficients of the LL2 subband ( a is in the top left, b in the top right, c in the bottom left, and d in the bottom right position) |
| | one of the three dotted blocks is black and the other two are white |
| | one of the three dotted blocks is white and the other two are black |
| | The blocks with slanted lines may be black or white depending on the XOR operation of the corresponding subblocks of block1 and block2 |

the background of the unscrambled watermark will be generated due to the nature of ISS. To regain the original watermark from the unscrambled watermark, a watermark reduction process is used to remove the redundant noise caused by the image secret sharing scheme. According to the generated block by XOR, one of the following two steps will be adopted:

(a) when the number of white pixels of the generated block is equal to 1 or 0, the block is reduced to a black pixel.

(b) when the number of white pixels of the generated block is greater than 1, the block is reduced to a white pixel.

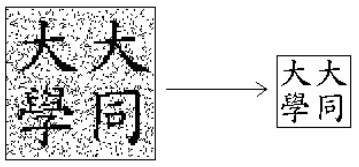


Figure. 6. The reduced watermark.

Fig. 6 shows an example of the result after the watermark reduction.

### 3.2 Secret Image Generation Phase

The following lists the detailed steps in the proposed secret image generation phase.

#### Secret Image Generation Algorithm

***Input*:** a gray-level host image $h$ ($N_1 \times N_2$), a watermark $l$ ($n_1 \times n_2$), and a secret key.

***Output*:** a secret image $s$ ($s_1 \times s_2$) used to retrieve the watermark.

***Step1.*** Use Torus-automorphism and the secret key to scramble the watermark $l$ into $l'$

***Step2.*** Divide the host image $h$ into non-overlapping $8 \times 8$ blocks $h(k)$, $k$=1, 2, …, $N_1 / 8 \times N_2 / 8$ and the scrambled watermark $l$ into a binary-digit sequence $l(k)$, $k$=1, 2, ..., $n_1 \times n_2$.

***Step3.*** Set $k$ to be 1.

***Step4.*** Transform the host image block $h(k)$ into 4 DWT coefficients by two-level decomposition.

***Step5.*** Use the mapping table and the relationship between the 4 coefficients and their average to find out the feature type of block $h(k)$, and hence the corresponding public block $p(k)$.

***Step6.*** Map the corresponding scrambled watermark block $l'(k)$ into the secret block $s(k)$.

***Step7.*** Increase $k$ by 1. If $k \leqq (N_1 / 8 \times N_2 / 8)$ go to ***step4***.

***Step8.*** Save the secret key and the secret image $s$ for the watermark retrieval phase.

### 3.3 Watermark Retrieval Phase

The following lists the detailed steps in the proposed watermark retrieval phase.

#### Watermark Retrieval Algorithm

***Input*:** a gray-level suspect image $h'$ ($N_1 \times N_2$), a secret image $s$ ($s_1 \times s_2$), and the secret key.

***Output*:** a reduced watermark $l_R$ ($n_1 \times n_2$).

***Step1.*** Divide the host image $h'$ into non-overlapping $8 \times 8$ blocks $h'(k)$ , $k$=1, 2, ..., $N_1 / 8 \times N_2 / 8$ and the secret image $s$ into non-overlapping $2 \times 2$ blocks $s(k)$, $k$=1, 2, ..., $s_1 / 2 \times s_2 / 2$.

***Step2.*** Set $k$ to be 1.

***Step3.*** Transform the host image block $h'(k)$ into 4 DWT coefficients by two-level decomposition.

***Step4.*** Use the mapping table and the relationship between the 4 coefficients and their average to find out the feature type of block $h'(k)$, and hence the corresponding public block $p'(k)$.

***Step5.*** Apply XOR operation on the public block $p'(k)$ and the corresponding secret block $s(k)$ to produce the corresponding scrambled watermark block $l'(k)$.

***Step6.*** Increase $k$ by 1. If $k \leqq (N_1 / 8 \times N_2 / 8)$ go to ***step3***.

***Step7.*** Use Torus-automorphism and the secret key to rearrange the watermark $l'$ into $l$.

***Step8.*** Use watermark reduction process to reduce the unscrambled watermark $l$ into the reduced watermark $l_R$.

## 4. Experimental Results

We conducted a series of experiments to measure the feasibility of the proposed scheme. Fig. 7 shows the 256 gray-level host image "Lena" used in the experiment. Fig. 8 shows the watermark and the generated secret image. The commercial image processing software, Ulead PhotoImpact 7.0, was used to simulate different kind of attacks.

The peak signal to noise ratio (*PSNR*) is used to evaluate the image quality after image processing operations. The *PSNR* of gray-level image is defined as follows:

$$PSNR = 10\log_{10}\frac{255^2}{MSE}dB \tag{3}$$

The mean square error (*MSE*) for an $N \times N$ gray-level image is defined as follows:

$$MSE = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N}(x_{ij} - x_{ij}^{'})^2}{N^2} \tag{4}$$

where $x_{ij}$ denotes the original pixel value, and $x'_{ij}$ denotes the test pixel value.

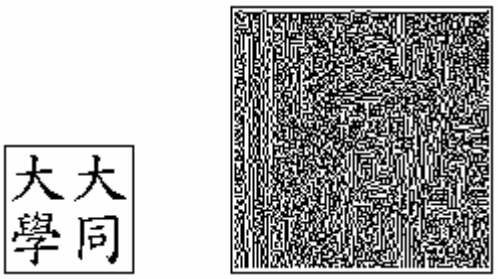
The *Accuracy rate* (*AR*) is used to measure the original watermark and retrieved one. *AR* is defined as follows:

$$AR = \frac{CP}{NP} \tag{5}$$

where *NP* is the number of pixels in the original watermark and *CP* is the number of the correct pixels obtained by comparing the pixels of the original watermark with the corresponding ones of the retrieved watermark. The more closely *AR* approaches 1, the more closely the retrieved watermark resembles the original one.

Table 2 lists the experimental results (the PSNR results denote the quality of "Lena" after image processing operations). The experiment results show

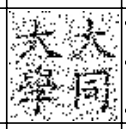
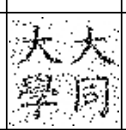
Figure. 7. The test image "Lena" (512×512).



(a) (b)

Figure. 8. (a) the watermark (64×64); (b) the secret image (128×128).

Table 2. The experiment results.

| Quality factor | 25% | 50% | 75% |
|---|---|---|---|
| **JPEG** |  |  |  |
| AR(PSNR) | 0.873(34.2) | 0.895(36.4) | 0.939(38.6) |
| Variance | 3 | 2 | 1 |
| **Blurring** |  |  |  |
| AR(PSNR) | 0.860(29.3) | 0.875(29.8) | 0.908(34.2) |
| Variance | 3 | 2 | 1 |
| **Sharpening** |  |  |  |
| AR(PSNR) | 0.863(23.6) | 0.917(29.3) | 0.950(35.2) |
| Width&Heigh | 64x64 | 128x128 | 256x256 |
| **Scaling** |  |  |  |
| AR(PSNR) | 0.732(24.2) | 0.861(28.1) | 0.926(34) |
| Cropped area | 50% | 25% | 10% |
| **Cropping** |  |  |  |
| AR | 0.874 | 0.938 | 0.975 |

(a) (b)

Figure. 9. (a) the test image "Tiffny"; (b) the retrieved watermark.

that the retrieved watermarks are still recognizable under the attacks of the JPEG compression, the blurring, the sharpening, the scaling (except for 64 × 64), and the cropping. The accuracy rate also shows that when *AR* is closer to 1, the retrieved watermark is more distinct. Moreover, when the suspect image is actually a different image from the original one, the retrieved watermark will contain nothing more than noise. Fig. 9 shows the test image "Tiffny" and the retrieved watermark. The image "Tiffny" is different from our original image "Lena". After the watermark retrieval, the accuracy rate of the retrieved watermark of "Tiffny" is 0.517. The retrieved watermark contains only noise and no information about the original watermark.

## 5. Conclusions

In this paper, we proposed a copyright protection scheme based on image secret sharing (ISS) and discrete wavelet transformation (DWT). The proposed scheme contains the secret image generation phase and the watermark retrieval phase. In the generation phase, the scheme extracts the features from a host image using DWT, and then uses the features and the watermark to generate the secret image using ISS. In the retrieval phase, the watermark is retrieved by combining the secret image and the features obtained from the suspect image. The accuracy rate is then used to measure the similarity between the retrieved watermark and the original one. The scheme has the following advantages: (1) it does not modify the host image because it only extracts features and does not change any pixels; (2) it is secure because of the application of the secret key and ISS, and (3) it is robust according to results of the experiment. Because the proposed scheme does not alter the host image, it is very suitable for unchangeable images such as medical images and satellite images.

## References


[1] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, "A digital watermark" Proc. IEEE Int. Conf. Image Processing, vol. 2, pp.86-90, 1994.

[2] C.-C. Wang, S.-C. Tai, and C.-S. Yu, "Repeating image watermarking technique by the visual cryptography," IEICE Trans. Fundamentals. Signal processing, vol.E83-A, pp.1589-1598, 2000.

[3] M. Kutter, F. Jordan, F. Bossen, "Digital signature of color images using amplitude modulation," Proc. of SPIE storage and retrieval for image and video databases, San Jose, USA, no. 3022-5, pp. 518-526, February 13-14, 1997.

[4] Inoue H., Miyazaki A., Yamamoto A. and Katsura T., "A Digital Watermark Technique Based on the Wavelet Transformation and Its Robustness on Image Compression and Transformation," IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences, vol. E82-A no. 1 pp. 2–10, Jan. 1999.

[5] M. Iwata, K. Miyake and A. Shiozaki, "Digital watermarking method to embed index data into JPEG images," IEICE Trans. Fundamentals, vol.E85-A, no.10, pp.2267-2271, Oct. 2002.

[6] S. Pereia and T. Pun, "Robust template matching for affine resistant image watermarks," IEEE Trans. Image Processing, vol. 9, pp. 1123-1129, 2000.

[7] Ming-Shing Hsieh, Din-Chang Tseng, and YH Huang, "Hiding digital watermarks using multiresolution wavelet transform," IEEE Trans. Industrial Electronics, vol.48, no.5, pp.875-882, Oct. 2001.

[8] M. Kuribayashi and H. Tanaka, "A new digital watermarking scheme applying locally the wavelet transform," IEICE Trans., Fundamentals, vol. E84-A, no. 10, pp. 2500-2507, 2001.

[9] SH Wang and YP Lin, "Wavelet tree quantization for copyright protection watermarking," IEEE Trans. Image Processing, Feb. 2004.

[10] FOTOPOULOS, V. and SKODRAS, AN: "A New Fingerprinting Method for Digital Images", Proc. First IEEE Balkan Conference. Signal Processing, Communications, Circuits and Systems, Istanbul, Turkey, June 1-3, 2000.

[11] C.C. Chang and J.C. Chuang, "An image intellectual property protection scheme for gray-level images using visual secret sharing strategy," Pattern Recognition Letters, vol. 23, pp. 931-941, June 2002.

[12] Chin-Chen Chang, Ju-Yuan Hsiao and Chi-Lung Chiang, "An Image Copyright Protection Scheme Based on Torus Automorphism," First International Symposium on Cyber Worlds (CW'02) November 06 - 08, 2002.

[13] Johnson, NF, Duric, Z., and Jajodia, S, "On Fingerprinting Images for Recognition," Submitted to Fifth International Workshop on Multimedia Information Systems (MIS'99), Palm Springs, CA, USA, 21-23 October 1999.

[14] Said, A. and Pearlman, WA, "A new fast and efficient image codec based on set partitioning in hierarchical trees," IEEE Trans on Circuits and Systems for Video Technology, 6, pp.243-250, 1996.