

## An IPR protection scheme based on wavelet transformation and visual cryptography

Young-Chang HOU<sup>1,\*</sup>, A-Yu TSENG<sup>2,3</sup>, Zen-Yu QUAN<sup>4</sup>, Hsin-Ju LIU<sup>1</sup>

<sup>1</sup>Department of Information Management, Tamkang University, Taipei, Taiwan

<sup>2</sup>Department of Management Science, Tamkang University, Taipei, Taiwan

<sup>3</sup>Computer Center, National Open University, Taipei, Taiwan

<sup>4</sup>Department of Information Management, National Central University, Taoyuan, Taiwan

Received: 28.05.2014

Accepted/Published Online: 06.07.2015

Final Version: 20.06.2016

**Abstract:** As information technology is fast developing, it brings great convenience to our everyday life. However, hackers may also access confidential data illegally and easily from computers over the Internet. Therefore, how to protect property rights against infringement is an essential issue. Digital watermarking is a method that adds personal information to an intellectual property to protect one's ownership rights. Should the intellectual property be disputed, the owner can retrieve the watermark and prove ownership rights. Based on the principles of visual cryptography and the law of large numbers, our study generates shares by comparing pseudorandomly selected value pairs during the processes of embedding and verifying the hidden watermark. The wavelet transformation coefficients of the  $LL_3$  region are used as the sample population. Experimental results indicate that our method has good robustness against darkening, lightening, blurring, sharpening, noising, distortion, jitter, JPEG, and cropping attacks. There are 3 advantages to our method: 1) robustness is retained when the protected image suffers from attacks; 2) unexpanded shares are created to reduce the size of every share; 3) the embedded watermark is decoded by the human visual system during the verification process.

**Key words:** Digital watermarking, wavelet transformation, visual cryptography, law of large numbers, copyright protection

### 1. Introduction

With the advent of the digital age and the rapid development of network bandwidth, information delivery is easier and faster than ever. The general public can surf the Internet for information they want at any time and any place. However, from another perspective, although retrieving information easily is indeed one of the advantages of the new era, without proper protection of information from being stolen and tampered with, protection of property ownership cannot be guaranteed. Nowadays, numerous mechanisms for protection of intellectual property rights (IPR) have been proposed, including digital watermarking technology.

Digital watermarking refers to using characteristics that human eyes cannot notice, i.e. the subtle changes caused by embedding a set of digital signals into a digital image. These signals can be a trademark, personal data, etc. When it is necessary to verify ownership of the data, the original embedded signals can be extracted from the image via the watermark extraction process. The person can then claim that he or she owns this property. The purpose of the protection of IPR is then achieved. This set of digital signals is called the "watermark".

\*Correspondence: [yhou@mail.im.tku.edu.tw](mailto:yhou@mail.im.tku.edu.tw)

Watermarking technology can be classified into different categories according to the attributes of watermark visibility, resistance against attacks, embedding methods, and extraction methods [1,2]. For visibility, it can be divided into 2 types: visible and invisible; by the strength of its resistance to attacks, it can be classified into 3 types: robust, fragile, and semifragile; by different watermark extraction methods, it can be classified into 3 groups: the blind, nonblind, and semiblind; and by embedding methods, it can be divided into the spatial domain [3,4] and the frequency domain [5–10].

The concept of visual cryptography was originally proposed by Naor and Shamir [11] as a mechanism for protecting information. The secret image is decomposed into multiple haphazard share images (shares). To decrypt, we can simply superimpose these sharing images and take advantage of the human visual system to visualize the secret content of the stacked shares without any need for complex computation.

Since the concept of visual cryptography was proposed, several related works [12–28] have been presented. However, Naor and Shamir's visual cryptography has the drawback that the size of share images needs to be extended to several times larger than that of the original secret image, which results in image distortion and waste of storage. To handle this problem, Ito et al. [26] utilized the concept of probability and proposed a pixel nonexpansion method in which the share images have the same size as the secret image. While Ito et al.'s method avoids the problem of pixel expansion, the randomly selected sharing pixels may destroy the patterns of pixel distribution on share images. This may cause a messy visual effect on the superimposed image. Tu and Hou [28] proposed a multipixel encryption scheme. They used each continuous  $m$  white (black) pixel of the secret image as an encrypted object, which ensured that each corresponding  $m$ -white-pixel ( $m$ -black-pixel) area of the share images had an equal probability to be black. The chaos of the share images is well controlled and thus the superimposed image can have higher quality of visual effects.

As the decryption process of visual cryptography does not require computing machines, many works began to apply visual cryptography to the watermarking field [12–21]. Hou [12] employed the highest bit-plane of the secret image to produce the share images needed in visual cryptography, but the drawback is that the size of the share images is twice that of the secret one. Hsu and Hou [13] produced share images by comparing the sample means with the population mean of the secret image based on the central limit theorem. One of the drawbacks of this technique is that, to ensure the security of share images, its sampling process must strictly comply with the statistical norm of the normal distribution. Another drawback is that the share images and the restored image are expanded to 4 times the original one. Hou and Huang [14] improved on Hsu and Hou's [13] shortcomings. They used the statistical characteristics of the law of large numbers to produce nonexpanded share images through comparing randomly selected pixel pairs. However, when the image has been attacked, employing a single pixel value to perform the comparison is more vulnerable than engaging the sample mean of a plurality of pixels. Because after some attacks those pixel pairs with different values might have equal values, or those pairs with an equal pixel value might have unequal values, it tends to result in different consequences when those 2 pixels are compared. This will cause more errors when retrieving the watermark.

The aforementioned methods are based on the spatial domain. The major problem of the spatial domain is its weak robustness after receiving an attack. Therefore, most of the watermarking researchers have focused on the frequency domain. The common practice is to exploit different transformation technologies to convert the pixel values of the image in the spatial domain to amplitude coefficients in the frequency domain. The advantages of the frequency domain include not only its better resistance to attacks, but also its varying information importance represented by diverse frequencies. Therefore, we can perform different levels of processing to an image in accordance with the importance of different frequencies and user requirements.

Rawat and Raman [15] proposed a copyright protection scheme based on fractional Fourier transform, singular value decomposition, and visual cryptography. The first singular value of each  $4 \times 4$  image block is collected as the population base. Each singular value is then compared with the average singular value to determine how to generate the shares needed. Singh et al. [16] proposed a copyright protection scheme for video. Scene changes are detected from the video by first applying the histogram difference method to the video stream. The frames mean of the same scene of the video is then compared with the global mean to generate the shares needed. Benyoussef et al. [17] proposed a copyright protection scheme based on the dual tree complex wavelet transform where  $7 \times 7$   $LL$  subblocks are randomly selected and the average  $LL$  coefficient of each subblock is then calculated. The subblock average is compared with the average of all  $LL$  subbands to generate the shares. The main concept of [15–17] is quite similar to that of [13]; the only difference is the method of selecting the population base. However, the sampling methods in [15–17] need more computation time than those in [12–14]. In addition, the locality effect of the frames mean in [16] may prevent the share image from having disorderly 1/2 black dots and 1/2 white dots, which compromises the security requirements of visual cryptography. Luo et al. [18] used the QR (quick response) code as the watermark and proposed a watermarking scheme based on the dual transform domains of discrete wavelet transform and discrete fractional random transform. Unlike [12–17], Luo et al. [18] embedded the watermark into the original host image, which may degrade the quality of the original image; this is the reason why their watermark size is only  $25 \times 25$ , which is much smaller than the size of the protected image.

Chang et al. [19] extracted DC coefficients from the original image to produce share images. Hsieh et al. [20] extracted a feature from every 4 neighborhood  $LL_2$  (second-level low-frequency band) coefficients of wavelet transformation of the host image to produce the share images. Lou et al. [21] also used wavelet transformations to extract the coefficients of the medium frequency and the low frequency to generate share images. The common drawback of the above 3 works is that the sizes of the watermarks have to be much smaller than the protected images at only 1/144, 1/64, and 1/64, respectively. In addition, Chang et al. [19] had to calculate the number of white dots in every  $3 \times 3$  block when extracting the watermark to restore the color of the watermark. Hsieh et al. [20] and Lou et al. [21] needed to do the exclusive-or (XOR) operation on share images. All 3 methods were unable to take advantage of visual cryptography to decrypt the superimposed images by using only the human visual system.

This research aims to improve the abovementioned drawbacks. The authors employed a nonexpanded scheme and used the method of embedding the watermark in the frequency domain to produce share images with good resistance to attacks. Once the protected image encountered an attack, the watermark could still be extracted robustly. The process of extracting the watermark uses the mechanism of visual cryptography. By superimposing share images, the watermark emerges naturally without the help of any complex arithmetic computation.

The remainder of this paper is organized as follows: in the next section, we concisely introduce the related background of the proposed scheme. In Section 3, the proposed protection schemes are presented. The experimental results and comparisons with related studies appear in Section 4. Finally, conclusions are given in Section 5.

**2. Literature review**

**2.1. Visual cryptography**

The concept of visual cryptography (VC) was first proposed by Naor and Shamir [11]. The idea of VC is to break the secret image down into  $n$  noise-like share images that show no clues about the original image. During the decryption process, no complex arithmetical computation is required. As long as  $k$  ( $2 \leq k \leq n$ ) or more share images are superimposed, the original secret image will be recovered on the superimposed images and the content of the secret image can be identified via the human visual system. On the other hand, if the number of stacked share images is less than  $k$ , the secret image will not be restored on the superimposed images. This is called the  $(k, n)$ -threshold ( $k$ -out-of- $n$  threshold) mechanism.

Take the  $(2, 2)$ -threshold, for example (Table 1). Each pixel of the secret image will be decomposed into a 1-white-and-1-black image block. When a white pixel of the secret image needs to be shared, the 2 participants will get image blocks of the same type; when sharing a black secret pixel, both will get the complementary blocks. Thus, when 2 share images are superimposed, the area corresponding to the secret white pixels will show half-black-and-half-white blocks, and the area corresponding to the black pixels of the secret image will show as fully black. Hence, the superimposed images will be shown at 50% contrast, and the human visual system can easily tell the content of the secret information.

**Table 1.** The sharing model of the  $(2, 2)$ -threshold visual cryptography scheme.

Secret image	Share 1	Share 2	Stacked image
■	■□	□■	■
	□■	■□	■
□	■□	■□	■□
	□■	□■	□■

**2.2. Watermarking technology**

In terms of the embedding method, the watermarking technology can be classified into 2 types, the spatial domain [3,4] and the frequency domain [5–10]. To represent the image as a collection of pixels is one way of presenting the image in the spatial domain. If each pixel is composed of several bits, the image can then be shown in different colors. The watermark embedding methods in the spatial domain often modify the least significant bits of an image pixel directly. Due to the characteristics of the human eye, one is unable to distinguish the slight change in pixels. This method uses relatively simple calculation and has low computational loading. The 2 most common watermarking techniques of the spatial domain are the least significant bit method [29,30] and the patchwork method [31,32]. However, in order to keep the original image from revealing any clues about the watermark, the amount of information that can be hidden in an image becomes small. Moreover, as the embedded information is placed directly into the bits of image pixels, it has high sensitivity and thus low resistance to attacks.

We can also regard an image as the superimposed result of the waveforms of various frequencies. Generally speaking, the change between the pixels of the low-frequency region is smaller. The low-frequency regions, which usually constitute the most important part of the whole image, look visually smoother and clearer. In contrast, pixels of the high-frequency region have a larger variance. The high-frequency regions, which usually represent

the boundary of the image block, look visually discontinuous and messy. Through mathematical computation, we can convert the pixel values of the original image (in a data form of spatial domain) to the waveforms of different frequencies (in a data form of frequency domain). After the transformation process, the different frequency portions of the image are separated off, and the amplitudes of the wave of different frequencies are produced. The method for watermark embedding in the frequency domain is to modify the amplitudes of some frequencies based on the watermark one wishes to embed.

As the low-frequency region is the most important part of the image, and the human visual system is more sensitive to changes in low-frequency regions, any subtle change is likely to be detected by the human eye. Therefore, we usually do not hide the watermark information in a low-frequency region, to improve the imperceptibility of the watermark. On the other hand, humans do not easily detect small changes in the high-frequency region. In terms of visual quality, the high-frequency region is less important as compared to the low-frequency region. Therefore, it is the first target to be processed by all image processing software. Hence, to increase the robustness of the watermark, the watermark information will not usually be hidden in the high-frequency region, either. Between the low and high frequencies is the intermediate-frequency band, which has moderate sensitivity to modification and visual quality and is the most suitable place for most watermarking technologies to embed their watermarks. The advantage of frequency domain watermarking techniques is their better resistance to attacks, but the watermark computational process is also more complex than those in the spatial domain. In frequency domain watermarking techniques, discrete cosine transform (DCT) [5,6], fast Fourier transform (FFT) [1], and discrete wavelet transform (DWT) [7–10] are the 3 most common transformation methods.

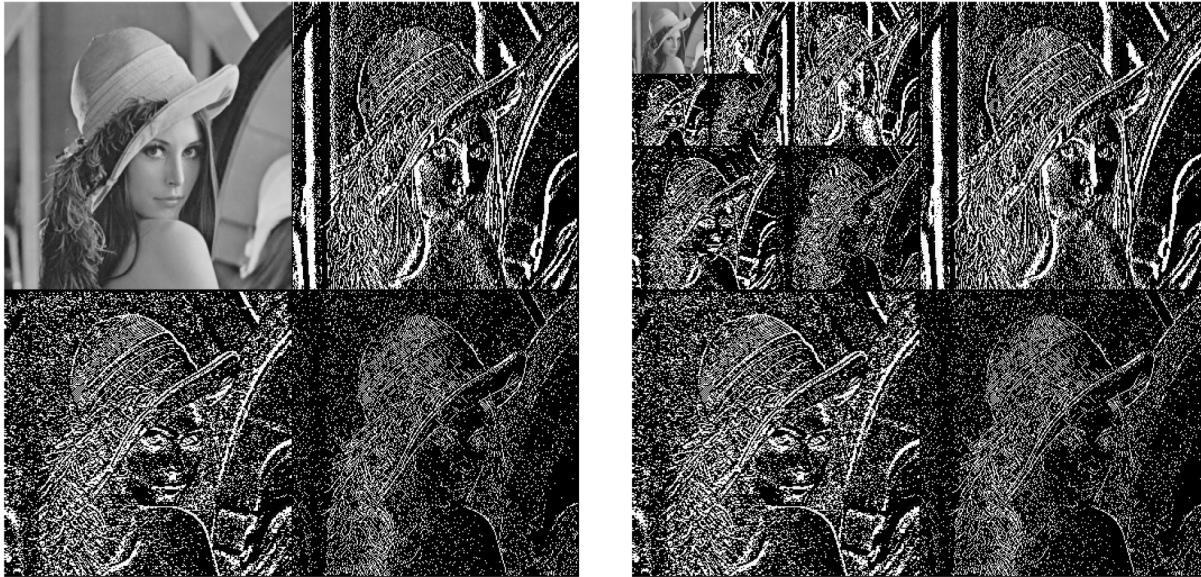
### 2.3. Discrete wavelet transform

There are many ways to transform images from the spatial domain to the frequency domain. The Haar wavelet transform (HWT) [33] is one of the most common methods. During the transformation process, the wavelet function performs the arithmetic summation and difference operations on the gray values of every adjacent pixel pair, 2 pixels at a time. The mean value of every pixel pair, called the approximation coefficient, is allocated in the first half of the sequences, and the mean value of each pairwise subtraction, called the detail coefficient, is placed in the rear section. The process continues row-wise first until the entire image is processed. The same procedure is then performed in every column of the image. The amplitude coefficients in the frequency domain of the image, as shown in Figures 1a and 1b, can then be obtained.

As the average of pixel values retains the most important information that can be used to best represent most of the image's appearance, these portions of data are more important in displaying the image. In addition, as most adjacent pixels have little difference in value, the variations between them are much more moderate after the pairwise average operation. Therefore, this area is referred to as the low-frequency region (upper left of Figure 1). On the contrary, the subtraction results represent the gaps between pixels. As most adjacent pixels have only small differences in value, most of the subtraction results are close to 0. Only at the edges of the image blocks will the differences between adjacent pixels become greater, and dramatic enough to particularly highlight the image contours. Hence, we refer to this area as the high-frequency region (bottom right of Figure 1). Repeating the abovementioned transformation operation in the low-frequency region, we can get a higher level result for the discrete wavelet transformation (Figure 1b).

Since data of the low-frequency  $LL_3$  region (upper left region in Figure 1b) are the average results of 64 corresponding pixel values, these values are more representative of their original pixels. Even when the protected image is under attack, the  $LL_3$  coefficients are not easily modified to any great degree. In our

research, 2 pseudorandomly selected  $LL_3$  coefficients were compared to determine the content of the share images needed in visual cryptography. Due to the conservative property of  $LL_3$  coefficients, the comparison results can be almost identical before and after suffering attacks, which ensures better robustness.



(a) the result after 1-level DWT.

(b) the result after 3-level DWT.

**Figure 1.** Different results of DWT: a) the result after 1-level DWT; b) the result after 3-level DWT.

Although conventional watermarking algorithms in the wavelet domain are operating either on a subband or a block base, some researchers, for example, Barni et al. [10], adapted the watermark strength pixel-wise by taking into account the texture and the luminance content of all of the image subband. The watermark strength is modulated according to the local image characteristics and is accomplished through a mask, giving a pixel-by-pixel measure of the sensibility of the human eye to local image perturbations. Performance improvement on watermark robustness and invisibility is obtained by means of exploiting the characteristics of the human visual system.

#### 2.4. The law of large numbers

In any large group of individuals, there will be individual differences owing to various contingent factors. When we focus on a single individual, its behavior will be disorganized, irregular, and difficult to predict. However, due to the operation of the law of large numbers, the entire group as a whole will appear in some kind of stable manner [34]. For example, when we roll the dice, any number between 1 and 6 may appear on any throw of the dice. Each time, the number changes randomly. Although the results of these throws will be an irregular number series, the occurrences of the various figures will conform to a stable uniform probability distribution, which will be close to 1 in 6 if we throw the dice a large number of times. Using the example of the dice, the individuals of a group may seem unrelated and diverse, but an indicator reflecting the group's condition will tend to keep steady with limited variation when the group is sufficiently large. This is due to the operation of the law of large numbers.

According to Bernoulli's definition of the law of large numbers, if  $n_A$  is the number of occurrences of event A in  $n$  independent tests, and  $p$  the probability of A's occurrence in each test, then for any  $\varepsilon > 0$ , we have

$\lim_{n \rightarrow \infty} \text{Prob} \left\{ \left| \frac{nA}{n} - p \right| < \varepsilon \right\} = 1$ ; i.e.  $\frac{nA}{n}$  will get closer to  $p$  as  $n$  approaches infinity. Bernoulli's law of large numbers states that, when  $n$  is large, the probability that event  $A$  occurs will be very close to the probability  $p$ . In practice, how many tests should be done in all so that the probability that the difference between  $\frac{nA}{n}$  and  $p$  is less than a particular value  $\varepsilon$  will be greater than  $1 - \alpha$ ? According to an estimation of Bernoulli's law of large numbers,  $n$  must satisfy the condition  $n \geq \frac{1}{4\alpha\varepsilon^2}$  so that  $\text{Prob} \left\{ \left| \frac{nA}{n} - p \right| < \varepsilon \right\} \geq 1 - \alpha$  can be met, where  $0 < \alpha < 1$ . Take flipping a coin, for example. The result of a flip is either a head or a tail, which means that each side has a probability of  $p = 1/2$ . If  $f_n$  represents the probability of heads occurring in the first  $n$  tests, we will have to toss  $n \geq \frac{1}{4 \cdot (0.01) \cdot (0.02)^2} = \frac{1}{0.000016} = 62,500$  times to have a 99% probability that the difference between  $f_n$  and  $p$  is less than 0.02.

### 3. Proposed watermarking model

#### 3.1. Theoretical bases

Watermark embedding techniques must often take the following points into account. First, for spatial domain embedding methods, decisions on the quantity and the location of the hidden information are particularly critical, to avoid making them too easily found. Their utility also decreases with these restrictions. Second, for frequency domain embedding methods, the computation is more complex and requires more calculation in the processes of watermark embedding and extraction. Third, adding a watermark will modify the information of the original image, which may destroy the quality of the original image. Fourth, nonblind watermarking methods often need to refer to the original image when extracting the watermark. If the original image cannot be accessed, the watermark will not be extracted either. This will inhibit the flexibility of watermark verification in ownership disputes.

The concept of visual cryptography is to produce some half-black and half-white share images from the corresponding secret image. When those share images are superimposed, the content of the secret image can be revealed. Therefore, when given a previously registered share image for identity authentication, if we can produce another share image from the controversial image and the superimposed image of these 2 shares can show the watermark we need, the purpose of verifying IPR is achieved.

In this study, the basic concept is that every share image processed by the visual cryptography scheme has 50% black points and 50% white points in it. From the viewpoint of coding theory, each share image is a series of 0s and 1s. If we can generate the proper 0/1 series from the protected digital asset (protected image,  $P$ ), then we can produce the share image (master share,  $M$ ) we need. With the master share ( $M$ ) and the watermark ( $W$ ), following the encryption rules of visual cryptography, we can create another share image (ownership share,  $O$ ). The master share ( $M$ ), which represents some features of the protected image, can be discarded, but the ownership share ( $O$ ), which represents the certificate of our identity authentication, should be kept. We can register this ownership share ( $O$ ) to a certification authority (CA), and then use it to verify our intellectual property rights in the future, as shown in Figure 2.

If there are disputes over the ownership of the intellectual property someday, we can simply generate the master share ( $M'$ ) from the controversial image and superimpose it onto the ownership share ( $O$ ) registered to the CA. If the result shows the watermark information, the ownership of this asset is proved to be ours. This method achieves the purpose of ownership verification, as shown in Figure 3.

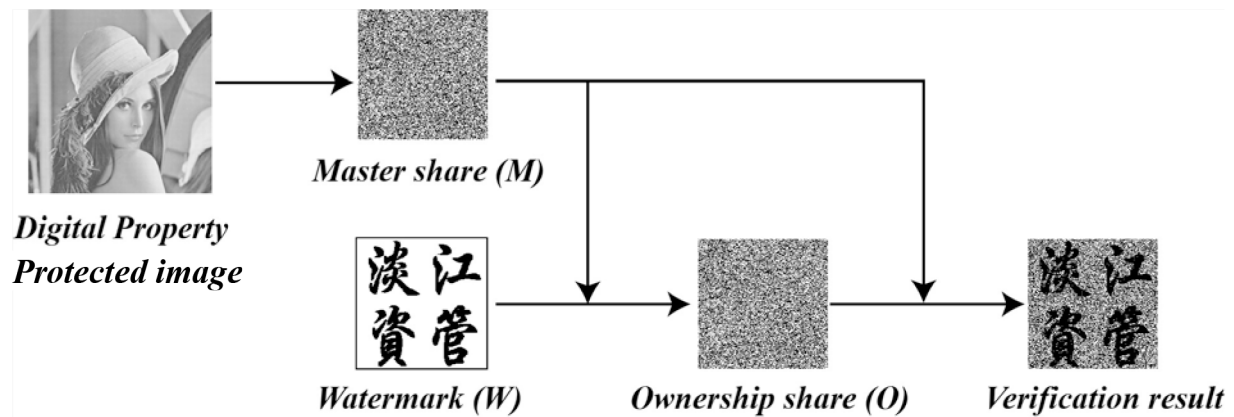


Figure 2. The model of applying visual cryptography to embed a watermark.

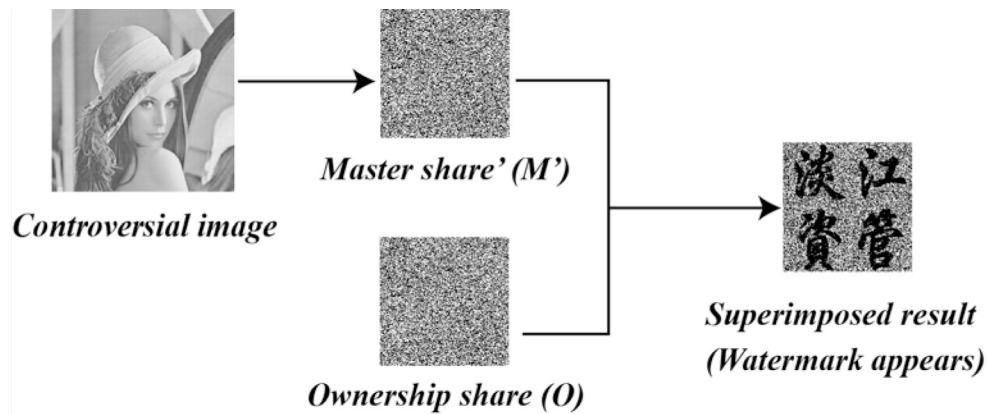


Figure 3. The verification process of the digital asset.

There are 2 advantages to applying visual cryptography to the watermarking mechanism. First, the original image remains intact. As the watermark is not actually embedded into the original image, the image will not be damaged. This benefit is particularly suitable for applications where the original images are not allowed to be modified, such as medical images, satellite images, and so on. Second, the watermark is easily extracted. By superimposing the share images on each other, we can take advantage of the human visual system to extract the watermark. This extraction process does not need complex mathematical calculation, even without the aid of computers. Therefore, the research that combines visual cryptography and the watermarking technology focuses on how to obtain the 0/1 series of the share image (master share,  $M$ ) through the protected asset, and how to combine the master share and the watermark to produce another share image (ownership share,  $O$ ) for verifying ownership.

We found that an image can usually maintain a certain image quality when subjected to attacks by some image processing software. That is, after being attacked, the original image still keeps the same mountains or the same seas; a red region is still red and a green part is also kept green. Although the pixel values of the attacked image have been changed, the appearance is almost the same as before. It is not difficult to find that the gray value distribution of the image pixels, owing to the statistical conservation property, will not be changed significantly and will still maintain a certain regularity.

This study combines probability theory, the law of large numbers, and the transformation of the frequency domain with the characteristics of nonexpanded visual cryptography to construct a digital image protection



scheme for IPR. First of all, we adopt the frequency domain approach by performing a 3-level HWT to the protected image ( $P$ ). Because each coefficient of the  $LL_3$  low-frequency band compresses the values of 64 corresponding pixels, it retains the most plentiful information about the original image. We then compare 2 pixel values ( $a, b$ ) of each pixel pair that is pseudorandomly retrieved from the  $LL_3$  data. Only the 2 cases of ( $a \geq b$ ) and ( $a \leq b$ ) may occur.

According to the law of large numbers, the occurrence probabilities of the cases ( $a > b$ ) and ( $a < b$ ) are equal. As for the case ( $a = b$ ), the half of which whose sum of pixel coordinates is even can be classified into the ( $a > b$ ) case; the other half whose sum of pixel coordinates is odd can be classified into the ( $a < b$ ) case. In this method, all results of the comparison may seem like a chaotic arrangement initially, but according to the law of large numbers, the occurrence count of case ( $a \geq b$ ) or ( $a \leq b$ ) will be very close to half of the number of tests. Take a  $256 \times 256$  watermark, for example. There will be at least 65,000 trials executed. When the case of ( $a \geq b$ ) appears, we will produce a black point (1) on the master share ( $M$ ); when the case of ( $a \leq b$ ) appears, we will produce a white point (0) instead. Thus, we can let the share image have half black dots and half white dots to meet the security requirements of visual cryptography.

When the protected image ( $P$ ) encounters an attack, because the  $LL_3$  coefficients are less sensitive to the image attack, the comparison results of the coefficient pairs will not be changed easily. In the course of this study, we could still extract a master sharer ( $M'$ ) with good robustness. Therefore, when the identity of the intellectual asset needs to be verified, the master shareec ( $M'$ ) is produced from the asset first. Then, given the ownership share ( $O$ ) in our possession, if both the master and ownership shares can be superimposed to show the watermark, we can claim that the ownership of the asset is ours. Thus, the aim of ownership verification of the intellectual asset is achieved.

### 3.2. Protection method of the digital image copyright

The image protection process can be divided into 2 parts: the first part is to produce the ownership share of the digital asset and the second part is to verify ownership.

#### 3.2.1. Watermark embedding: establishment of digital image ownership

In the production process of the digital asset's ownership share, the ownership share ( $O$ ) is regarded as the object to be produced. After a 3-level HWT, all  $LL_3$  band coefficients are extracted as the population base. Based on the pixel-sharing rules of visual cryptography, we embed the watermark ( $W$ ) into 2 corresponding share images, which are called the master share ( $M$ ) and the ownership share ( $O$ ). The details of the processing steps are shown in Figure 4.

The watermark embedding algorithm produces 2 share images: the master share ( $M$ ) and the ownership share ( $O$ ). In order to achieve the purpose of ownership verification, after these 2 share images are generated, we register the ownership share ( $O$ ), as well as the seed ( $S$ ), to a certification authority (CA) in case of the need for authentication in the future. The master share ( $M$ ) can then be discarded.

#### 3.2.2. Watermark extraction: ownership verification of the digital image

The second part of the image protection process, the ownership verification process of the digital asset, is shown in Figure 5. If there is a controversial image ( $P'$ ) and we want to verify its ownership, first we execute a 3-level HWT on this image and extract the coefficients from the  $LL_3$  block as the population base to produce a master

sharee ( $M'$ ). Then we superimpose the generated master sharemp( $M'$ ) onto the ownership share ( $O$ ) that we keep on hand for identity verification. If the superimposed image can reveal the watermark patterns, it means that the ownership of this controversial image  $P'$  has been verified, and the image belongs to the person who owns the ownership share ( $O$ ) and the seed ( $S$ ).

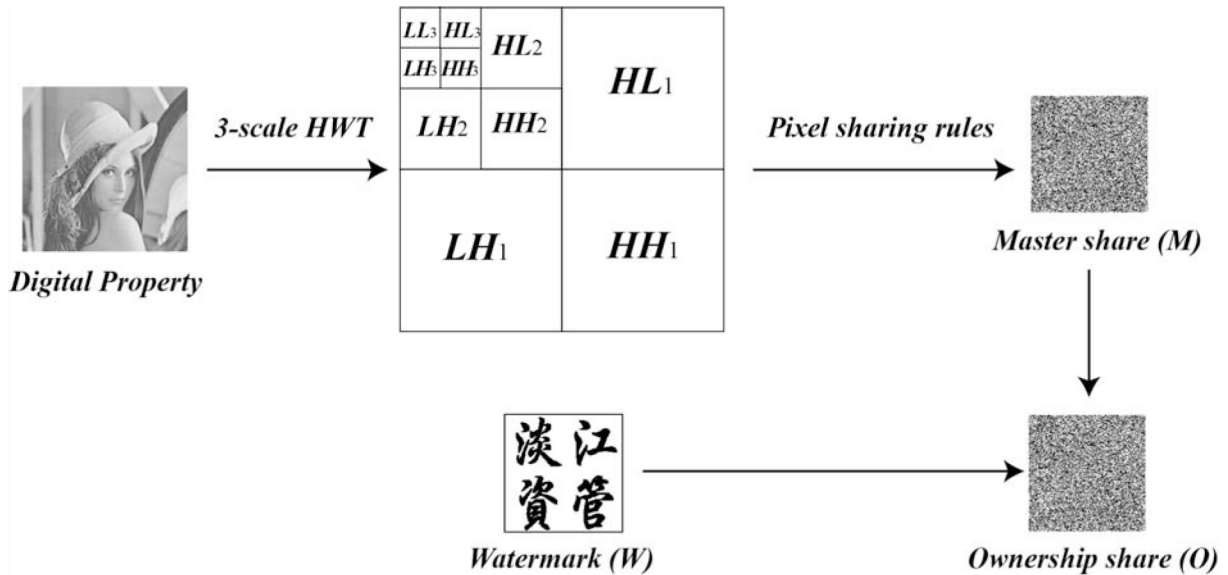


Figure 4. The watermark embedding process.

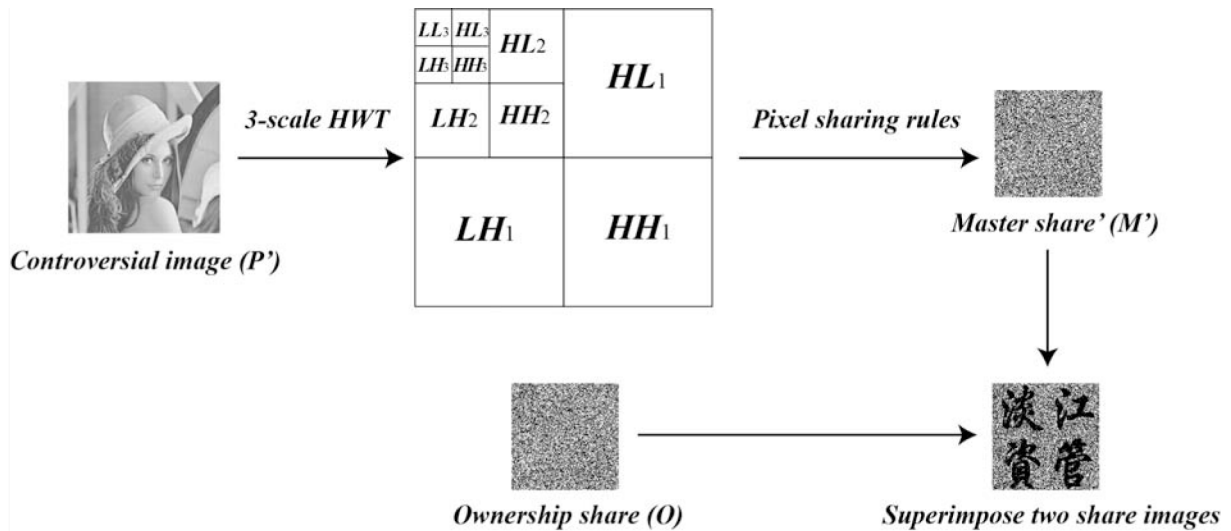


Figure 5. The verification process of the watermark.

### 3.2.3. Verification of the similarity between the attacked image and the original image

If an image encounters a critical attack, the attacked image will become less similar to the original image and may lose information about the embedded watermark. Therefore, if the extracted watermark can remain similar to the original one, the corresponding watermark embedding technology is said to be good at contributing high resistance to attacks or image processing. The more similar the extracted watermark is to the original

watermark, the higher resistance the embedding technology shows to attacks, or the better the embedding technology is. Because the sensitivity of the human visual system is not high enough, sometimes we cannot recognize the differences between the attacked image and the original one. Therefore, in order to clearly define the degree of the image distortion after attacks, people usually employ the peak signal to noise ratio (PSNR) to measure the distortion of the image. The calculation method is shown in Eqs. (1) and (2):

$$PSNR = 10 \log_{10} \frac{255^2}{MSE}, \tag{1}$$

$$MSE = \frac{1}{m \times n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} (a_{ij} - b_{ij})^2, \tag{2}$$

where MSE is the mean square error of the  $2 m \times n$  grayscale images,  $a_{ij}$  represents the gray value of the original image at position  $(i, j)$ , and  $b_{ij}$  represents the gray value of the attacked image at position  $(i, j)$ . The higher the PSNR value is, the more similar these 2 images are. Conversely, if the PSNR value is lower, these 2 images have a lower similarity. Therefore, the PSNR can be used as an approximation to human perception of reconstruction quality and is commonly used in image science for evaluating the quality of the reconstructed image. A higher PSNR generally indicates that the reconstruction is of higher quality.

In order to verify the similarity of the extracted watermark and the original one, as a measurement metric, we take the improved normalized correlation (NC) proposed by Hsu and Hou [13] as follows:

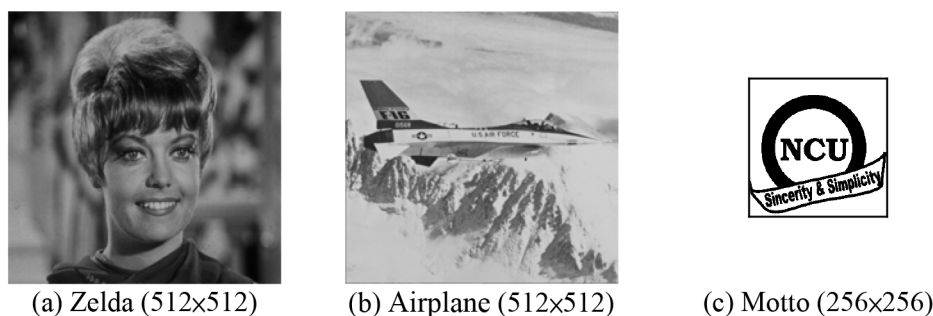
$$NC = \left( \frac{\sum_i \sum_j W_{i,j} \times W'_{i,j}}{\sum_i \sum_j W_{i,j}^2} \times \frac{\sum_i \sum_j (1 - W_{i,j}) \times (1 - W'_{i,j})}{\sum_i \sum_j (1 - W_{i,j})^2} \right)^{0.5}, \tag{3}$$

where  $W_{ij}$  and  $W'_{ij}$  are the pixel values of the original watermark and the extracted watermark at positions  $(i, j)$ , respectively. Suppose that the value of the black pixel is 1 and the value of the white pixel is 0. In the NC formula, the first part represents the ratio of the black pixels on the original watermark that still remain black on the extracted watermark. It can accumulate values when both  $W_{ij}$  and  $W'_{ij}$  are 1. The second part represents the ratio of the white pixels on the original watermark that still remain white on the extracted watermark. It can accumulate values when both  $W_{ij}$  and  $W'_{ij}$  are 0. The NC value ranges between 0 and 1. If the value is close to 1, it means that the verified watermark is quite similar to the original one. On the contrary, if the NC value is close to 0, it means that these 2 watermarks have less similarity. The higher the NC value of the extracted watermark is, the higher resistance to attacks the embedding technology demonstrates, or the better the embedding technology is.

## 4. Experimental results and discussion

### 4.1. Experimental environment

In this study, we ran our experiments using Microsoft Windows XP with Service Pack 3 on a personal computer equipped with an Intel Core 2 duo processor and 2 GB memory. We used Java SE 6.0 SDK as our program development tool. The experimental subjects were two  $512 \times 512$  grayscale images, Zelda and Airplane (Figures 6a–6b). The embedded watermark was a  $256 \times 256$  black and white image motto: National Central University: Sincerity and Simplicity (Figure 6c).



**Figure 6.** The protected images and the watermark: a) Zelda ( $512 \times 512$ ); b) Airplane ( $512 \times 512$ ); c) Motto ( $256 \times 256$ ).

To observe the robustness of the proposed method in resisting various attacks and its unambiguity in verification, we used Photoshop CS4 as a tool to deliberately perform a variety of destructive attacks. After that, we employed the NC formula to examine the similarity degree between the watermarks retrieved from the attacked and the original images. If the NC value was larger, then the watermark generated from the attacked image was more similar to the original one. We then measured the PSNR value to check the similarity between the attacked image and the original one. If the PSNR value was lower, it meant that there was a greater difference between the 2 images. Generally speaking, if the PSNR value is low and the NC value is high, it demonstrates that the hidden watermark has a higher resistance to attacks. The results of the experiments are shown in Table 2.

The experimental results show that, despite a certain degree of destruction that various attacks can cause to the original image, we are still able to clearly recognize the content presented in the retrieved watermark. We think that when an image encounters any attack, the basic statistical properties of the image will not be changed. Perhaps, from a microscopic point of view, every pixel value is subjected to a varying degree of modification, but from a macroscopic perspective, the original appearance of the image after attacks can still be recognized; i.e. the original black area is still black and the original white region is still white.

Since data of the low-frequency  $LL_3$  region are the mean values of 64 corresponding pixel values, these values are more representative of their original pixels and not easily greatly modified. Thus, when the values of the pixel pairs are compared, the same comparison results as those on the original image can almost be kept, which ensures greater robustness. Due to the reasons above, general lightening or darkening attacks have almost no effect on our method and will not alter the extracted watermark at all. The proposed method can also retain good resistance to a higher compression ratio of the JPEG compression attack. Not only do those attacked images that look only a little different from the original image have a high NC value, but images that encounter a more severe attack, such as noising, cropping, blurring, and distortion, also keep a high NC value where the reconstructed watermark can still clearly be identified. This also proves that the watermark produced by the characteristic of the statistical properties has very good resistance to attacks and can meet the unambiguous and robust requirements of the digital watermark.

Since our approach employs the concept of nonexpanded visual cryptography, it is necessary to check in watermark embedding whether the occurrence probability of case ( $a \geq b$ ) or case ( $a \leq b$ ) is close to  $1/2$  as it will affect the proportion of black to white pixels on the share image. Figure 7 shows the experimental results of various seeds. The  $X$ -axis represents the number of comparisons. The  $Y$ -axis represents the ratio of the occurrence count of case ( $a \geq b$ ) to the total number of comparisons. We found that no matter what the seed value is, when the number of experiments is in excess of 4000, all ratio values approach  $1/2$ . The gaps between

**Table 2.** The experimental results of different attacks.












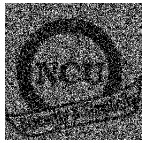
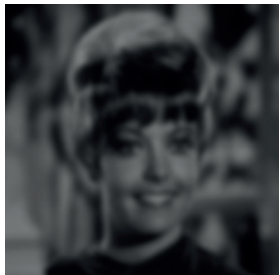


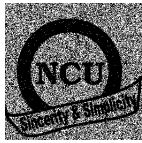







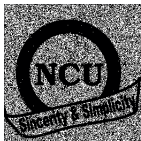


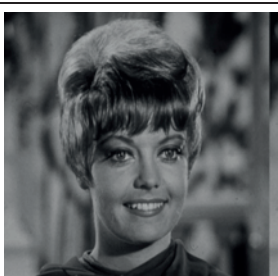

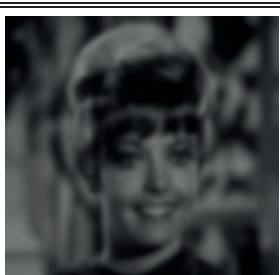
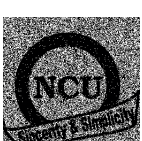


Attacked image	Reconstructed watermark	Attacked image	Reconstructed watermark
			
JPEG 1: JPEG compression at a 1% ratio <i>PSNR</i> = 34.15 dB <i>NC</i> = 99.34%		Sharpening 10 <i>PSNR</i> = 25.75 dB <i>NC</i> = 96.39%	
			
Lightening 20: 20% brighter <i>PSNR</i> = 21.35 dB <i>NC</i> = 99.68%		Darkening 20: 20% darker <i>PSNR</i> = 16.43 dB <i>NC</i> = 99.64%	
			
Rescaling 1/2: Reduce to 1/2 of the original size first, and then zoom back to the original size <i>PSNR</i> = 32.22 dB <i>NC</i> = 99.10%		Jitter 16: Cut off a 16-pixel column from the leftmost of the picture, and then append it to the rightmost side <i>PSNR</i> = 17.59 dB <i>NC</i> = 84.29%	
			
Blurring 5: Gaussian blur (5 pixels) <i>PSNR</i> = 17.87 dB <i>NC</i> = 97.29%		Distortion 100: Geometric Distortion of a 100% ripple effect <i>PSNR</i> = 18.28 dB <i>NC</i> = 98.94%	



Table 2. Continued.

Attacked image	Reconstructed watermark	Attacked image	Reconstructed watermark
			
JPEG 1: JPEG compression at a 1% ratio <i>PSNR</i> = 34.15 dB <i>NC</i> = 99.34%		Sharpening 10 <i>PSNR</i> = 25.75 dB <i>NC</i> = 96.39%	
			
Lightening 20: 20% brighter <i>PSNR</i> = 21.35 dB <i>NC</i> = 99.68%		Darkening 20: 20% darker <i>PSNR</i> = 16.43 dB <i>NC</i> = 99.64%	
			
Rescaling 1/2: Reduce to 1/2 of the original size first, and then zoom back to the original size <i>PSNR</i> = 32.22 dB <i>NC</i> = 99.10%		Jitter 16: Cut off a 16-pixel column from the leftmost of the picture, and then append it to the rightmost side <i>PSNR</i> = 17.59 dB <i>NC</i> = 84.29%	
			
Blurring 5: Gaussian blur (5 pixels) <i>PSNR</i> = 17.87 dB <i>NC</i> = 97.29%		Distortion 100: Geometric Distortion of a 100% ripple effect <i>PSNR</i> = 18.28 dB <i>NC</i> = 98.94%	

1/2 and those ratio values are almost 0.01. Therefore, even if the size of the watermark is only  $64 \times 64$ , the number of comparisons can still satisfy the requirement of the law of large numbers.

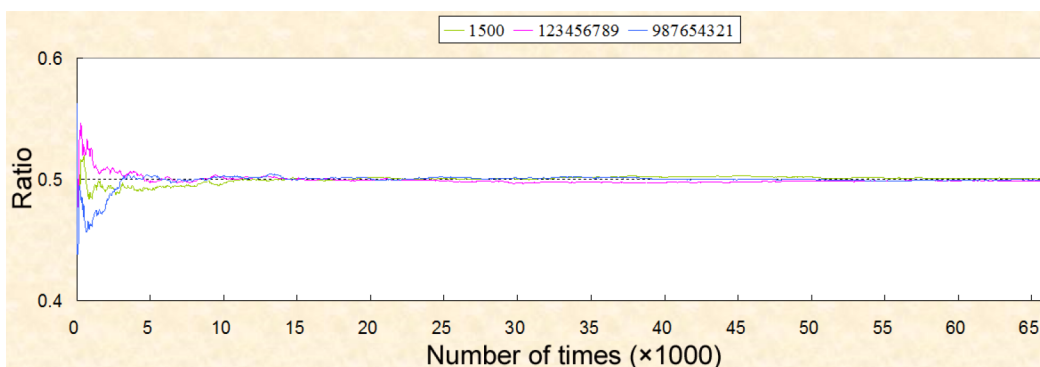


Figure 7. The verification of the law of large numbers.

## 4.2. Comparisons of our study with related works

### 4.2.1. The frequency domain approaches

The approaches of our method and the related works of Chang et al. [19], Hsieh et al. [20], and Lou et al. [21] all belong to the frequency domain category. Chang et al. [19] divided the original image into  $4 \times 4$  blocks to extract their DC coefficients respectively after the DCT. They used the concept of pixel expansion to generate the share image with a size  $3 \times 3$  times that of the watermark. Hence, the size of the watermark will be  $M_1/12 \times M_2/12$  at most, where  $M_1$  and  $M_2$  are the length and width of the protected image. Hsieh et al. [20] used the average  $LL_2$  coefficients of wavelet transformation and their relative positions in  $LL_2$  as the distribution basis to produce the share image. They also used the concept of pixel expansion, which makes the size of the share image  $2 \times 2$  times the size of the watermark. Therefore, the size of the watermark can only be  $M_1/8 \times M_2/8$  at most. Moreover, each block on their share images is distributed with different numbers of black pixels, i.e., 0–4, depending on different situations (cf. Table 1 in [20]). This violates the security requirement of visual cryptography. Lou et al. [21] also used wavelet transformation by comparing the coefficients of the medium frequency and the low frequency to produce the share image with size doubling. As the low-frequency coefficients must be larger than the coefficients of the medium frequency, the comparison results are one-sided inclined. To be specific, the results of  $f(i, j)$  and  $f'(i, j)$  calculated by Eqs. (2) and (5) in [21] are always equal to 0, so that before and after attacks the public image and the original secret image are well matched, which completely loses the sense of verification. Since Lou et al. adopted the 3-level wavelet transformation, the size of the watermark can only be  $M_1/8 \times M_2/8$  times the original image. One common drawback of the aforementioned works is that the size of the watermark should be much smaller than that of the protected image. Their watermarks can only have a size of  $1/144$ ,  $1/64$ , and  $1/64$ , respectively, of the original image. In addition, when extracting the watermark, Chang et al. needed to count the number of white dots in each  $3 \times 3$  block to restore the corresponding color of the watermark. Hsieh et al. and Lou et al. needed to perform XOR operations on the share image. All of these approaches are not able to take advantage of visual cryptography to decrypt the secret information from the superimposed images using only the human visual system.

The proposed research employs the sampling method to pseudorandomly select 2 coefficients ( $a, b$ ) from the wavelet-transformed coefficients of the  $LL_3$  region. These 2 coefficient values are compared to determine the color of the share image. According to the law of large numbers, the occurrences of  $(a \geq b)$  and  $(a \leq b)$  have an

equal opportunity. Thus, the generated share image will have randomly distributed half black dots and half white dots to meet the security requirements of visual cryptography. Moreover, the number of the sampling process is not limited to the size of the protected image or the watermark. This is quite different from the approaches of Chang et al., Hsieh et al., and Lou et al., which can only use a very small watermark. When extracting the watermark, our method employs the practice of visual cryptography, which allows the watermark to emerge naturally via superimposing the share images without the need for any complex mathematical operations.

To sum up the above descriptions, we make a comparison of our method with those of Chang et al. [19], Hsieh et al. [20], and Lou et al. [21]. The results are shown in Table 3.

**Table 3.** Comparisons of our study with the related works in the frequency domain.

Authors	Processing method	Share image/watermark	Watermark/protected image	Extracting method
Chang et al. [19]	DCT	$3 \times 3$ times	$1/12 \times 1/12$ times	Superimposing + counting
Hsieh et al. [20]	2-level DWT	$2 \times 2$ times	$1/8 \times 1/8$ times	XOR operation
Lou et al. [21]	3-level DWT	$2 \times 1$ times	$1/8 \times 1/8$ times	XOR operation
Our method	3-level DWT	$1 \times 1$ time	Unlimited	Superimposing

#### 4.2.2. The visual cryptography approaches

The basic idea of this series of studies is that every share image produced by visual cryptography has randomly distributed 50% black dots and 50% white dots. From the point of view of coding theory, each share image can be treated as composed of a series of 0s and 1s, and each has a chance of 50% occurrence. If we can produce the 0/1 series that contains the original information from the protected digital asset, we can generate the share image (master share) we need. Hou [12] retrieved the needed 0s and 1s from the highest bit-plane of the image. The share image's size was expanded to twice that of the embedded watermark. Hsu and Hou [13] compared the sample means with the population mean to extract the 0s and 1s they needed. Their share image was designed to be expanded to  $2 \times 2$  times the embedded watermark. Hou and Huang [14] adopted a nonexpanded design that compared 2 randomly selected pixel values to draw the 0s and 1s they needed. The scopes of the 3 aforementioned methods belong to the spatial domain category. This study, which adopted the use of the 3-level wavelet transformation, employed a method of the frequency domain category. In this approach, 2 coefficients of the  $LL_3$  region were compared to extract the desired 0s and 1s. It also employed a nonexpanded design. The 4 aforementioned papers are all based on sampling inspection. Therefore, the size of their watermark is not restricted to that of the protected image. The watermark extraction methods are also in accordance with the spirit of visual cryptography, where the share images are directly superimposed to reveal watermarks. The comparison of the results of the proposed method with those of [12–18] is shown in Table 4.

In addition, we used 'Airplane' as a subject on which to perform different kinds of attacks. We compared the results of the proposed method with those of [12–14]. The comparison results obtained are shown in Table 5.

Table 5 shows that in a variety of attacks, the NC values extracted from the watermark by this method are generally better than those of [12–14]. Especially in the blurring, noising, distortion, JPEG, and rescaling attacks, the NC values extracted by this method can have about a 2% increment compared to the methods of [12–14].



**Table 4.** The comparison of our study with the related works using visual cryptography.

Authors	Domain	Processing method	Share image watermark	Watermark protected image	Extracting method
Hou [12]	Spatial	Highest bit-plane	$2 \times 1$ times	Unlimited	Superimposing
Hsu and Hou [13]	Spatial	Sample mean	$2 \times 2$ times	Unlimited	Superimposing
Hou and Huang [14]	Spatial	Pixel comparison	$1 \times 1$ time	Unlimited	Superimposing
Rawat and Raman [15]	Frequency	Singular value decomposition	$2 \times 2$ times	$<1$	Superimposing
Singh et al. [16]	Frequency	Frame means	$2 \times 2$ times	$<1$	Superimposing
Benyoussef et al. [17]	Frequency	$7 \times 7$ $LL$ subblock average	$2 \times 1$ times	$<1$	Superimposing
Luo et al. [18]	Frequency	Discrete fractional random transform	$1 \times 1$ time	$<1$	Superimposing
Our method	Frequency	$LL_3$ coefficient comparison	$1 \times 1$ time	Unlimited	Superimposing

**Table 5.** The comparison of the resistance to attacks of the related works.

Attack type	PSNR value	NC value			
		Hou [12]	Hsu and Hou [13]	Hou and Huang [14]	Our method
Lightening 20	23.05 dB	97.48%	97.72%	99.43%	99.52%
Darkening 20	21.98 dB	92.31%	97.50%	99.39%	99.39%
Gaussian blurring 5	23.09 dB	93.63%	91.66%	90.85%	95.48%
Sharpening 10	21.56 dB	95.45%	93.19%	92.49%	92.55%
Noising 20	18.65 dB	83.86%	82.90%	80.59%	94.73%
Geometric distortion 100	21.98 dB	95.05%	94.83%	95.88%	98.18%
Jitter 16	17.10 dB	88.97%	82.25%	83.34%	86.88%
JPEG 5	38.58 dB	95.52%	97.55%	99.43%	99.44%
Cropping ( $1/2 \times 1/2$ )	14.87 dB	93.67%	80.44%	84.15%	84.73%
Rescaling $1/2$	32.81 dB	95.25%	96.64%	97.24%	99.28%

The reasons may be as follows. The operations of the practices in [12–14] are based directly on gray values of the image. Once the image is attacked, each pixel value of that image may have been changed; the images before and after the attacks may have some differences. Therefore, the master share, ( $M'$ ) generated by the image after the attacks may also have some differences with the master share ( $M$ ) generated by the image before the attacks. It creates a higher chance that the master share ( $M'$ ) will not match with the ownership share ( $O$ ) at hand. However, data of the  $LL_3$  low-frequency band are obtained from the average operation of 64 corresponding pixel values. Because of the smooth effect of the average operation, the variation of  $LL_3$  coefficients is much gentler (some pixel values may be increased while others may be decreased) through the wavelet transformation.

Therefore, the master share ( $M$ ) and the master share' ( $M'$ ) generated in this study from the  $LL_3$  region before and after attacks respectively can achieve a higher similarity. Table 6 shows that after blurring, noising, distortion, JPEG, and rescaling attacks, the PSNR values obtained from the  $LL_3$  region are higher than those from the original image itself. This reveals that the variation of the sampling population (the original  $LL_3$ ) of our method is smaller than that of the population (the original image) adopted in [12–14]. The results of this research show that the master share ( $M$ ) and the ownership share ( $O$ ) generated by combining the frequency domain approach with the statistical property have a better robustness to attacks.

**Table 6.** Differences between the original image and the  $LL_3$  image after an attack.

 Original image (512x512)	After the attack☒	Lightening 20  PSNR = 23.05 dB	Darkening 20  PSNR = 21.98 dB
 Original $LL_3$ (64x64)	After the attack☒	 PSNR = 23.06 dB	 PSNR = 22.02 dB
Gaussian Blurring 5	Sharpening 10	Noising 20	Geometric distortion 100
 PSNR = 23.09 dB	 PSNR = 21.56 dB	 PSNR = 18.65 dB	 PSNR = 21.98 dB
 PSNR = 28.63 dB	 PSNR = 24.74 dB	 PSNR = 36.08 dB	 PSNR = 28.63 dB
Jitter 16	JPEG 5	Cropping (1/2x1/2)	Rescaling 1/2
 PSNR = 17.10 dB	 PSNR = 38.58 dB	 PSNR = 14.87 dB	 PSNR = 32.81 dB
 PSNR = 19.36 dB	 PSNR = 48.13 dB	 PSNR = 15.01 dB	 PSNR = 48.13 dB

## 5. Conclusion

This study takes advantage of the easy decryption benefit of visual cryptography and applies the statistical law of large numbers to produce an evenly distributed half-black and half-white share image. Based on the HWT, the wavelet transformation coefficients of the  $LL_3$  region are used as the sample population. These  $LL_3$  coefficients retain the most plentiful information about the original image, suffer less change from variations of single pixels, and can make the coefficient comparison results more stable based on the law of large numbers. Thus, even when the protected image is under attack, the coefficient comparison results are not easily changed. That is, the master share' from the attacked image and the master share from the original image are quite consistent. Therefore, the NC value of the superimposed watermark can still be mostly maintained at 95% or more, which reveals that our approach has good resistance to attacks. The advantages of the proposed image ownership protection method include: 1) the watermark embedding scheme does not affect the content of the original image; 2) the watermark extraction scheme does not need the use of the original image; 3) the watermark's size is not restricted to the size of the protected image; 4) additionally, the nonexpanded approach also solves the larger size problem of the share image.

## Acknowledgment

This paper was part of the research results of a project supported by the National Science Council, Republic of China, under Grant No. NSC100-2221-E-032-043.

## References

- [1] Lee SJ, Jung SH. A survey of watermarking techniques applied to multimedia. In: IEEE International Symposium on Industrial Electronics; 12–16 June 2001; Pusan, South Korea. Piscataway, NJ, USA: IEEE. pp. 272-277.
- [2] Cox I, Miller ML. A review of watermarking and the importance of perceptual modeling. In: 1997 Proceedings of SPIE 3016; 8 February 1997; San Jose, CA, USA. Bellingham, WA, USA: SPIE. pp. 92–99.
- [3] Karibali IG, Berberidis K. Efficient spatial image watermarking via new perceptual masking and blind detection scheme. *IEEE T Inf Foren Sec* 2006; 1: 256-274.
- [4] Nguyen TV, Patra JC. A simple ICA-based digital image watermarking scheme. *Digit Signal Process* 2008; 18: 762-776.
- [5] Patra JC, Phua JE, Bornand C. A novel DCT domain CRT-based watermarking scheme for image authentication surviving JPEG compression. *Digit Signal Process* 2010; 20: 1597-1611.
- [6] Zhu H, Liu M, Li Y. The RST invariant digital image watermarking using Radon transforms and complex moments. *Digit Signal Process* 2010; 20: 1612-1628.
- [7] Wang Y, Doherty JF, Van Dyck RE. A wavelet-based watermarking algorithm for ownership verification of digital images. *IEEE T Image Process* 2002; 11: 77-88.
- [8] Fakhari P, Vahedi E, Lucas C. Protecting patient privacy from unauthorized release of medical images using a bio-inspired wavelet-based watermarking approach. *Digit Signal Process* 2011; 21: 433-446.
- [9] Vahedi E, Zoroofi RA, Shiva M. Toward a new wavelet-based watermarking approach for color images using bio-inspired optimization principles. *Digit Signal Process* 2012; 22: 153-162.
- [10] Barni M, Bartolini F, Piva A. Improved wavelet-based watermarking through pixel-wise masking. *IEEE T Image Process* 2001; 10.5: 783-791.
- [11] Naor M, Shamir A. Visual cryptography. In: *Workshop on the Theory and Application of Cryptographic Techniques*; 9–12 May 1994; Perugia, Italy. pp. 1-12.

- [12] Hou YC. Copyright protection based on visual cryptography. In: Conference on Systemics, Cybernetics and Informatics 2002; 18 July 2002; Orlando, Florida. Orlando, FL: IIS. pp. 104-109.
- [13] Hsu CS, Hou YC. Copyright protection scheme for digital images using visual cryptography and sampling methods. *Opt Eng* 2005; 44: 077003.
- [14] Hou YC, Huang PH. An ownership protection scheme based on visual cryptography and the law of large numbers. *Int J Innov Comput Inform Control* 2012; 8: 4147-4156.
- [15] Rawat S, Raman B. A blind watermarking algorithm based on fractional Fourier transform and visual cryptography. *Signal Process* 2012; 92: 1480-1491.
- [16] Singh TR, Singh KM, Roy S. Video watermarking scheme based on visual cryptography and scene change detection. *AEU-Int J Electron C* 2013; 67: 645-651.
- [17] Benyoussef M, Mabtoul S, Marraki Me, Aboutajdine D. Robust image watermarking scheme using visual cryptography in dual-tree complex wavelet domain. *Journal of Theoretical and Applied Information Technology* 2014; 60: 372-379.
- [18] Luo X, Jiang DY, Li D. A blind holographic image watermarking algorithm based on dual transform domains and visual cryptography. *International Journal of Security and Its Applications* 2014. 8: 291-302.
- [19] Chang CC, Hsiao JY, Yeh JC. A colour image copyright protection scheme based on visual cryptography and discrete cosine transform. *Imaging Sci J* 2002; 50: 133-140.
- [20] Hsieh SL, Tsai IJ, Huang BY, Jian JJ. Protecting copyrights of color images using a watermarking scheme based on secret sharing and wavelet transform. *J Multimedia* 2008; 3: 42-49.
- [21] Lou DC, Tso HK, Liu JL. A copyright protection scheme for digital images using visual cryptography technique. *Comput Stand Inter* 2007; 29: 125-131.
- [22] Ateniese G, Blundo C, De Santis A, Stinson DR. Extended schemes for visual cryptograph. *Theor Comput Sci* 2001; 250: 143-161.
- [23] Hou YC. Visual cryptography for color images. *Pattern Recogn* 2003; 36: 1619-1629.
- [24] Hou YC, Quan ZY. Progressive visual cryptography with unexpanded shares. *IEEE T Circ Syst Vid* 2011; 21: 1760-1764.
- [25] Hou YC, Quan ZY, Tsai CF, Tseng AY. Block-based progressive visual secret sharing. *Inform Sciences* 2013; 233: 290-304.
- [26] Ito R, Kuwakado H, Tanaka H. Image size invariant visual cryptography. *IEICE T Fund Electr* 1999; E82-A: 2172-2177.
- [27] Shyu SJ. Image encryption by random grids. *Pattern Recogn* 2007; 40: 1014-1031.
- [28] Tu SF, Hou YC. On the design of visual cryptographic methods with smooth-looking decoded images of invariant size for gray level images. *Imaging Sci J* 2007; 55: 90-10.
- [29] Fridrich J, Goljan M, Du R. Detecting LSB steganography in color, and gray-scale images. *IEEE Multimedia* 2001; 8: 22-28.
- [30] Yang CH, Weng CY, Wang SJ, Sun HM. Adaptive data hiding in edge areas of images with spatial LSB domain systems. *IEEE T Inf Foren Sec* 2008; 3: 488-497.
- [31] Kalantari NK, Akhaee MA, Ahadi SM, Amindavar H. Robust multiplicative patchwork method for audio watermarking. *IEEE T Audio Speech* 2009; 17: 1133-1141.
- [32] Sluciak O, Vargic R. An audio watermarking method based on wavelet patchwork algorithm. In: 15th International Conference on Systems, Signals and Image Processing; 25-28 June 2008; Bratislava, Slovakia. Bratislava, Slovakia: Slovak University of Technology in Pub. House STU. pp. 117-120.
- [33] Stollnitz EJ, DeRose TD, Salesin DH. Wavelets for computer graphics: a primer. *IEEE Comput Graph* 1995; 15: 75-85.
- [34] Hogg RV, Tanis E. Probability and Statistical Inference. Boston, MA, USA: Pearson, 2009.