

AN OWNERSHIP PROTECTION SCHEME BASED ON VISUAL CRYPTOGRAPHY AND THE LAW OF LARGE NUMBERS

YOUNG-CHANG HOU AND PEI-HSIU HUANG

Department of Information Management
Tamkang University
No. 151, Yingzhuan Rd., Danshui Dist., New Taipei City 25137, Taiwan
{ ychou; mr.huang }@mail.im.tku.edu.tw

Received January 2011; revised September 2011

ABSTRACT. *Digital watermarking is a technique for the protection of intellectual property rights. In this study, a novel ownership protection scheme based on visual cryptography and the law of large numbers is proposed, where 2 phases, namely an ownership construction phase and an ownership authentication phase, each with 3 steps, are designated to illustrate how it works. In our scheme, two pixels at a time are selected randomly from the host image, then compared with each other and the results determine the corresponding content of the shares. The law of large numbers is employed to ensure the random distribution of half-black-and-half-white shares, which satisfies the demand needed for security in visual cryptography. The proposed method enjoys several advantages over conventional methods such as it does not alter the host image, it can identify the ownership without the help of the original host image, and it allows multiple watermarks or larger watermarks to be registered in a smaller host image. Finally, experimental results are given to illustrate the robustness of our scheme against several common attacks.*

Keywords: Visual cryptography, Law of large numbers, Intellectual property rights protection, Unexpanded share

1. **Introduction.** In recent years, the rapid development and growth in popularity of the Internet have made it rather easy for digital data (whether text, voice, or images) to be transmitted and exchanged over the World Wide Web. However, the convenience of sharing and spreading digital data on the Internet has brought about the problems of abuse and violation of intellectual property rights. Therefore, finding a way to protect the ownership of digital data has become a very important issue. Digital watermarking is a method that inserts a digital signal sequence into the protected digital image for the purpose of copyright protection, integrity checking and captioning. Should the ownership of the image need to be verified, the hidden watermark can be extracted through the watermarking retrieval procedure to prove the ownership.

Naor and Shamir [1] introduced a perfectly secure method called visual cryptography (VC) for protecting the secret images. The prominent feature provided by the VC decryption method is that it can be done with the human eye, without the need of a complicated mathematical computation. The basic model of VC consists of “splitting” the image or watermark into two transparencies (shares). One share can be regarded as the ciphertext and the other one as the secret key (called the key share). Each share looks like random noise, without any clue to disclose the outlines of the secret image. However, the original image can be revealed simply by superimposing these two shares. Due to its simplicity, the model can be used by anyone, even without knowledge of cryptography and without performing any complex computations.

Recently, many VC-based copyright protection schemes have been proposed, such as those in [2-9]. Chang et al. [2] utilized VC and the discrete cosine transform (DCT) to satisfy the requirements of security and robustness. The DC coefficients of all DCT blocks are extracted from the host image to form a master share. However, their method requires the size of the watermark to be much smaller than that of the host image. Hou's method [3] uses the most significant bits of the host image to generate the first share so as to satisfy the robustness requirements. Hou's method has the advantages that the watermark can be any size, and that the host image is not altered. Wang et al. [4] adopted the visual secret sharing scheme, dividing the watermark into a public watermark and a secret watermark. The former is embedded into the intellectual property right image. Hsu and Hou [5] proposed a novel copyright protection scheme for digital images based on VC and statistics. Luo et al. [6] proposed a scheme for hiding multiple watermarks in VC transparencies. Not only might the encrypted image be visible when stacking the transparencies, but also two extra watermarks can be extracted with simple computations. Fan and Yang [7] employed the VC technique to generate the authentication information and realize both visual verification and asymmetric public verification at the same time.

In this paper, an intellectual property protection scheme is proposed for digital images based on VC and the law of large numbers. The rest of this paper is organized as follows. The concepts of VC, digital watermarking, law of large numbers, and the related works on VC-based watermarking schemes are reviewed in Section 2. Section 3 describes the details of our proposed method. Experimental results and discussion are given in Section 4 and some conclusions are offered in Section 5.













2. Related Work.

2.1. Visual cryptography. In 1995, Naor and Shamir [1] proposed the technique of VC to decrypt image information without computer operations. This differs from the traditional cryptography in the way that the secret is partitioned into n shares, with each participant receiving only one share. As any k or more shares are stacked together, the secret image will be visually revealed. The secret image will remain invisible if the number of stacked shares is less than k . This is called the (k, n) -threshold mechanism. If we have no access to computers, VC is a good way of decrypting the secret image.

The method of VC is explained in Table 1. Every pixel of the original image is expanded to a 2×2 pixel blocks. If the pixels of the original image are black, we randomly choose any one of the bottom two rows and distribute them to the corresponding position on the corresponding shares. If the pixels of the original image are white, we then randomly choose any one of the top two rows and distribute them accordingly. Since the white will be presented as a see-through color on the transparency, therefore, the pixels with black secret dots will still be seen as fully black after the corresponding shares are superimposed, and the pixels with the white secret dots will be half-black-and-half-white (50% of black), so will be perceived as grey pixels.

2.2. Digital watermarking. The traditional way for an author or publisher to protect intellectual property rights is to either sign his/her name or affix his/her seal to the document, to make sure that the signature will not be easily erased and the property will not be misused. In case the signature/seal is indeed erased, there is a risk of destroying the integrity of the image and lowering the value of the property. Unfortunately, in the digital world, anybody with image processing software can effortlessly erase such signature/seal without leaving a trace. The traditional means are simply no longer sufficient to safeguard the intellectual property. A new technique of digital watermarking is developed to solve this problem. It involves inserting a sequence of invisible digital signals into a protected

TABLE 1. The sharing and stacking scheme of visual cryptography

Pixel	Share 1	Share 2	Stacked
□			
			
■			
			

digital image, which, in turn, can be retrieved to prove the ownership, should a dispute about the legal ownership of the image arise.

Generally speaking, the research related to watermarking can be categorized into four schools: (a) visible vs. invisible watermarks: however, as a consequence of what one can do with image processing software, the technique of visible watermarking may not be appropriate in the digital world; (b) non-blind vs. blind: During the watermark detection process, the original image may or may not be needed. As far as the availability and portability are concerned, techniques that can reveal a watermark without the presence of the original image are preferred; (c) robust vs. fragile watermarks: Robustness means that the hidden watermark is not easily deleted or damaged when the image is being attacked. While fragile watermarks, in contrast, are sensitive, damageable and unable to be recovered. Robust watermarks are mainly applied to the protection of intellectual property rights, while fragile watermarks are utilized to ensure the integrity of the information; (d) spatial [8,9] vs. frequency domain [2,10,11]: The spatial domain methods employ the property that a tiny change of pixels that cannot be detected by the human eye, can be used to directly modify the pixel's grey value to embed the watermark. The Least Significant Bit (LSB) [12] is the simplest and the most commonly used technique of the spatial domain. In the frequency domain methods, the host image is mainly turned into frequency space; the watermarks embedded by modifying the coefficients of the frequency space, and then transformed back to form a watermarked image. The main transformation techniques include the Fast Fourier Transform (FFT), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT) techniques.

Usually, the data in the host image need to be adequately adjusted or altered when embedding the digital watermarks, and most related techniques use many pixels or transformed coefficients to conceal one piece of information. Thus, the size of the watermark is much smaller than the size of the host image so that the requirements of imperceptibility can be satisfied. This property makes it impossible to embed a larger watermark into a smaller host image. In addition, if multiple watermarks need to be registered for a single digital image, it is also impossible with such a method to embed the later watermark without destroying earlier ones.

In general, an effective watermarking scheme should satisfy certain requirements such as imperceptibility, robustness, unambiguousness, security, large capacity and low computational complexity [13]. Some of these requirements may conflict with each other and thereby create many technical challenges. A reasonable compromise is required to achieve better performance for the intended applications. The watermarking scheme developed in this study answers exactly this call. It has the qualities of being invisible, being blind, being robust, belonging to the spatial domain, making it possible to embed a bigger watermark into a smaller host image and allowing to register multiple watermarks.

2.3. VC-based digital watermarking. Usually, the most significant bit (MSB) of every pixel of the protected image will seldom be changed when being attacked. Therefore, the MSB has the property of robustness that can be used to generate the shares needed in VC. Hou [3] proposed an intellectual property protection scheme based on VC and MSB. Hou first extracted every MSB of the protected image and recorded them in Bitplane0, then randomized Bitplane0 in order to eliminate the contours of the secret image shown in Bitplane0, and then expanded every pixel in Bitplane0 to a 1×2 block. If the MSB is 1, then 10 is filled in the corresponding block; otherwise, 01 is filled. By doing this, Share1 can be generated. The corresponding Share2 is generated according to the encryption rules of VC and the pixel values of both the watermark (W) and Share1. Although Hou's scheme has all the advantages of VC, it needs to expand the shares, which causes the problems of needing more storage space and longer transmission time.

Hsu et al. [6] adapted the properties of VC and sampling distribution of means (SDM) to satisfy the requirements of digital watermarking, as mentioned in Section 2.2. Hsu's scheme comprises two phases: the ownership registration phase and the ownership identification phase. According to the central limit theorem and unbiased property of SDM, if the sample size is large enough, the distribution of the sample mean will be approximated by a normal distribution. In theory, the normal distribution is bell-shaped and symmetric about its mean value. Therefore, we can find the probability $\Pr(\bar{X} \geq \mu) = \Pr(\bar{X} < \mu) = 0.5$, where \bar{X} is the sample mean and μ is the population mean. In the ownership registration phase, if $\bar{X} < \mu$ then $m_{i,j} = \blacksquare$; otherwise, \blacksquare is filled. In consequence, we can generate the randomly distributed half-black-and-half-white share according to the normal distribution property of SDM, which satisfies the demand of VC for security.

Hsu's method applied the central limit theorem and the symmetric property of normal distribution to ensure that there is an equal chance of \blacksquare and \blacksquare occurring on each share. It will then satisfy the security constraint that requires 50% black pixels and 50% white pixels on each share. However, Hsu's method relies on pixel expansion to generate shares, which leads to the consumption of more storage space and longer transmission times.

2.4. Law of large numbers. Owing to all kinds of accidental factors, the results of an individual experiment with a large number of trials seem to be disordered, irregular, and hard to predict when we focus on a single individual. However, the effect of the law of large numbers makes the experimental results, as a whole, steady and stable. Bernoulli's law of large numbers illustrates that, after a large number of repetitions of an experiment, we can expect the proportion of times event A will occur to be near the probability p that event A happens in every experiment. For example, the rolling of dice should produce a number from 1 to 6 randomly. However, if dice are rolled in a large number of times, the probability of producing any number from 1 to 6 is likely to be very close to $1/6$. In other words, every roll occurs randomly and seems to have no relationship with the others, but the total effect from a large number of trials will be stable and predictable. We will apply the law of large numbers to ensure that there is an equal chance of \square and \blacksquare occurring on each share. This not only satisfies the security constraint of VC but also avoids the problem of pixel expansion.

3. The Proposed Scheme.

3.1. Basic theory. Although Hsu's method can generate shares to satisfy the needs of VC and digital watermarking, it still has several drawbacks. First, in order to meet the requirements for a normal distribution, central limit theorem and unbiased property of SDM and to generate randomly distributed half-black-and-half-white shares, the sample

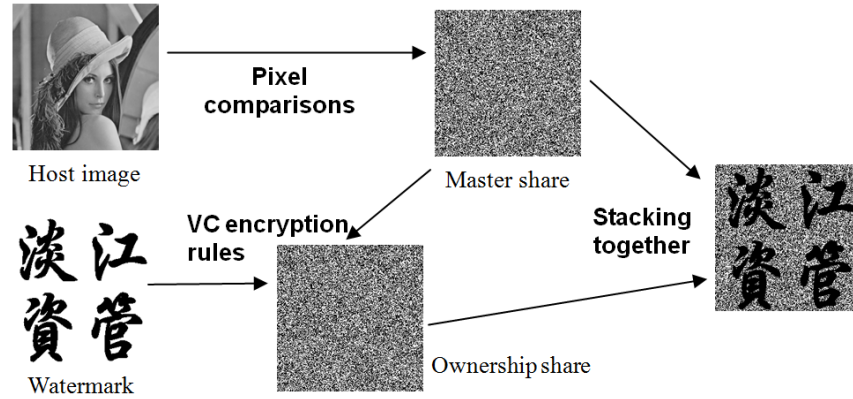


FIGURE 1. Our proposed scheme

size should be large enough. However, a large sample size means it takes more time to compute sample means. Second, the shares need to be expanded 4 times larger, which causes problems of more storage space and longer transmission time. Finally, the security constraint of 50% black pixels and 50% white pixels on each share is guaranteed by dispatching pixel blocks \blacksquare and \blacklozenge to each share, not because of the results of the normal distribution and the central limit theorem.

In this study, we employ both the theories of VC and the law of large numbers to improve the above drawbacks and construct a new intellectual property rights protection protocol for digital images. The basic concept is that when we compare a pair of pixels, A and B, picked randomly from the protected image, the grey value of pixel A is either larger or smaller than that of pixel B. According to the law of large numbers, the probabilities for each situation to occur are equal, just like tossing a coin. If the first situation occurs, we put a white pixel on the master share; otherwise, it is a black one. If the grey value of pixel A and pixel B are equal, we then compare the grey value with the median of the host image. If the pixel value is greater than the median, we put a white pixel on the master share; otherwise, a black one. By doing this, under the rule of the law of large numbers, we can get a master share with 50% black pixels and 50% white pixels to satisfy the security demands asked for in VC. Once we get the master share M, we can generate the ownership share O based on the contents of the master share M and the watermark W according to the encryption rules of VC. The watermark can be visually revealed by stacking the master share and the ownership share together. The whole process is illustrated in Figure 1.

Since each comparison generates only one pixel on the master share, we generate a share without pixel-expansion, thereby eliminating the problems of more storage space and longer transmission time. The operation of pixel comparison is much easier than Hsu's [6] sample mean computation. It takes less computing time to generate shares.

3.2. Ownership construction phase – watermark registration. Assume that a copyright owner wants to register a watermark W of size $W_1 \times H_1$ pixels within a gray-level host image of any size, so that he/she can authenticate the ownership if there is a dispute about the intellectual property at some other time. We first use the private key K as the seed to generate a set of random pixel positions. Then, we pick out pairs of pixel positions from the protected image H to conduct comparison of the pixel's grey values in order to generate the master share M . Once we get the master share M , the ownership share O can be generated naturally. The algorithm for generating ownership share is as follows:

Input: A grey-level protected host image (H) of any size, a binary watermark (W) with $W_1 \times H_1$ pixels, the median of the protected host image (MD) and a random secret key (K).

Output: An ownership share (O) of size $W_1 \times H_1$ pixels.

Step 1: Generate a list of random numbers by the secret key K .

Input the secret key K as the seed to generate a list of random number $R = \{r_1, r_2, \dots, r_n \mid n = 2(W_1 \times H_1)\}$. Every element in R corresponds to the position of a pixel in the host image. Thus, we can randomly select $2(W_1 \times H_1)$ pixel positions, and pick out the gray value $P(r_1), P(r_2), \dots, P(r_n)$ of that position.

Step 2: Generation of the master share.

Successively take pixels A and B from among $P(r_1), P(r_2), \dots, P(r_n)$ to form a pair. These are then compared with each other to decide on the content of every pixel $m_{i,j}$ in the master share M. The following is the base upon which the judgment is made:

Rule 1: If $P(r_i) > P(r_{i+1})$, then $m_{i,j} = \square$

Rule 2: If $P(r_i) < P(r_{i+1})$, then $m_{i,j} = \blacksquare$

Rule 3: If $P(r_i) = P(r_{i+1})$, then we carry out the classification according to the median of the host image, that is, If $P(r_i) > MD$, then $m_{i,j} = \square$; If $P(r_i) < MD$, then $m_{i,j} = \blacksquare$

Repeat Step 2 until all positions in R are processed. We have now built a master share M of the same size as the watermark W is.

Step 3: Generation of the ownership share O.

After the master share M is generated, we can generate the ownership share O based on the master share M and binary watermark W. Every pixel in O is generated as follows:

Rule 1: If $W_{i,j} = 0$ and $m_{i,j} = \square$ then $o_{i,j} = \square$

Rule 2: If $W_{i,j} = 0$ and $m_{i,j} = \blacksquare$ then $o_{i,j} = \blacksquare$

Rule 3: If $W_{i,j} = 1$ and $m_{i,j} = \square$ then $o_{i,j} = \blacksquare$

Rule 4: If $W_{i,j} = 1$ and $m_{i,j} = \blacksquare$ then $o_{i,j} = \square$

Repeat Step 3 until all pixels of the watermark are processed. We have now built the ownership share O which has the same size as watermark W and master share M.

When the above algorithm finished, we can get half-black-and-half-white shares under governance of the law of larger numbers. By superimposing the master share M and the ownership share O, we can retrieve the watermark W visually. Master share M can be discarded, but ownership share O should be registered with a trusted third party, because it is needed to verify ownership in the future. The secret key K must also be secretly preserved, so that we can revisit the correct positions and retrieve the corresponding grey values from the image when a controversy over ownership of the host image occurs.

3.3. Ownership authentication phase – the revelation of the watermark. When the protected host image seems to be infringed, the owner of the image can retrieve the hidden watermark from the controversial image to authenticate that he or she is the true owner of the intellectual property. The same private K is used as the seed to generate the same set of pixel positions. Pairs of pixel positions are then picked from the controversial image H' to conduct the comparison so as to generate the master share M' from H' . Finally, M' and the original ownership share O are superimposed to generate the watermark W' . The algorithm for authentication is as follows:

Input: A grey-level controversial host image (H'), a watermark (W) of the size $W_1 \times H_1$, the median of the controversial host image (MD') and a random secret key (K).

Output: A master share (M') of $W_1 \times H_1$ pixels in size.

Step 1: Generate a list of random numbers by the secret key K .

The image owner offers the secret key K as the seed of the random number generator to generate the same random sequence $R = \{r_1, r_2, \dots, r_n \mid n = 2(W_1 \times H_1)\}$.

Step 2: Generation of the master share M' .

The same generation process as for the master share is used again to generate the master share M' . Two pixels are taken successively to form a pair from $P'(r_1), P'(r_2), \dots, P'(r_n)$. The former is compared with the later pixel to decide on the content of every pixel $m'_{i,j}$ in the master share M' . Repeat Step 2 until all positions in R are processed.

We have now built a master share M' of the same size as the watermark W is.

Step 3: Revelation of the watermark.

By superimposing the master share M' generated from the controversial image H' and the ownership share O in hand, we can identify the content visually, and judge whether the controversial image belongs to the owner who offers the secret key or not.

4. Experimental Results and Discussion. An image can be purposely altered or modified by a violator to make it somehow different from the original. We refer to these factors which cause the alteration of an original image as “attacks”. Watermarks should be sufficiently robust to resist attacks that change the positions or values of pixels (geometric distortion and volumetric distortion, respectively). Common attacks on a digital image include lightening, darkening, rescaling, blurring, sharpening, noising, geometric distortion, cropping, JPEG compression, jitter and so on.

To see if our method has the robustness to defend against any attack or has the ability to enable clear identification of intellectual property, we conducted various attacks on the original image. Later, we rebuilt the watermark W' from the image H' which suffered from attacks (as shown in Table 2) to see if we could identify the embedded watermark.


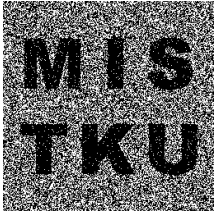
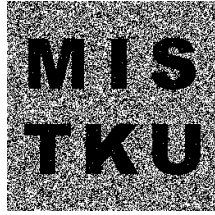

As to measure the degree of destruction that certain attacks have wrought on the original image, the Peak Signal-to-Noise Ratio (*PSNR*) is used to judge the similarity between the attacked image and the original one. The higher the value of *PSNR* is, the less the distortion is. In other words, the lower the value of *PSNR*, the more serious the attack suffered by the original image and the more different the signal from the original.

We took Normalized Correlation (*NC*) as another indicator to examine the degree of the similarity between the retrieved watermark and the original one. The objective of the *NC* is to calculate the ratio that a black (white) pixel of the original W is also a black (white) pixel in W' . The value of *NC* must be between 0 and 1. When the value of *NC* is larger, it indicates that the degree of similarity between W and W' is higher, and when the value of *NC* is smaller, the degree of similarity is lower.

4.1. Experimental results. Several experiments have been performed to demonstrate the robustness of the proposed scheme against several common attacks. The results are summarized in Table 2. The value of *PSNR* is used to judge the similarity between the attacked image and the original one (the higher the value of *PSNR* is, the less the effect of the attack), and the value of *NC* is used to judge the difference between the retrieved watermark and the original one (the higher the value is, the higher the similarity is).

We can see from Table 2 that although attacks may cause some destruction of the original image; we can still clearly identify the characters “MIS TKU” as our watermark. Since we use pairs for pixel comparison to conceal our watermark in the shares, the effects of attacks such as lightening and darkening just cause all pixel values to shift a certain amount; therefore, it does not affect the comparison results at all. An *NC* value of 1 indicates that the watermark in the image being attacked is preserved, the same as the original one. Compression is the most commonly used image process. Compressing the original image to 5% by *JPEG* damages the image quality severely. We can even detect an obvious difference with the naked eye. In spite of this, however, the quality of the retrieved watermark is still good. Our experiment results show that even when the original image is destroyed due to serious attacks, such as cropping, geometric distortion, and jitter, the

TABLE 2. Experimental results of several common attacks

JPEG Compressing the image to 5%	Sharpening Sharpening the edge of the image	Lightening Lightening the image 20%	Darkening Darkening the image 20%	Noising Add 10% noise to the image
 <i>PSNR=28.04dB</i>	 <i>PSNR=25.21dB</i>	 <i>PSNR=20.17dB</i>	 <i>PSNR=20.35dB</i>	 <i>PSNR=28.37dB</i>
 <i>NC = 0.97</i>	 <i>NC = 0.96</i>	 <i>NC = 1</i>	 <i>NC = 1</i>	 <i>NC = 0.97</i>
Cropping Cutting the left-upper part ($1/4 \times 1/4$) of the image	Blurring Blurring of the image	Geometric distortion Twisting of the image	Rescaling Shrinking of the image by $1/2$ and then enlarging it to the original size	Jitter Cutting off a 6-pixel-wide strip from the right hand side and attaching it to the left hand side
 <i>PSNR=10.84dB</i>	 <i>PSNR=32.95dB</i>	 <i>PSNR=25.68dB</i>	 <i>PSNR=34.04dB</i>	 <i>PSNR=18.08dB</i>
 <i>NC=0.88</i>	 <i>NC=0.99</i>	 <i>NC=0.97</i>	 <i>NC=0.99</i>	 <i>NC=0.92</i>

content of the retrieved watermark can still be clearly identified. This means that our method has very good resistance to various attacks.

4.2. Discussion. Hsu's method involves the dispatching of pixel blocks \blacksquare and \blacklozenge to each share so as to ensure the security constraint of 50% black pixels and 50% white pixels on each share. Since the algorithm we used is for unexpanded VC, we only dispatch \square or \blacksquare to the shares. Therefore, if the results of comparison of two pixels are not equally distributed, it will affect the number of times the black and white pixels appear on the shares. How can we ensure that we meet the security constraint of VC? It is guaranteed by the law of large numbers. When we conduct comparisons many times, under the rule of the law of large numbers, the probabilities of dispatching \square or \blacksquare to each share will be

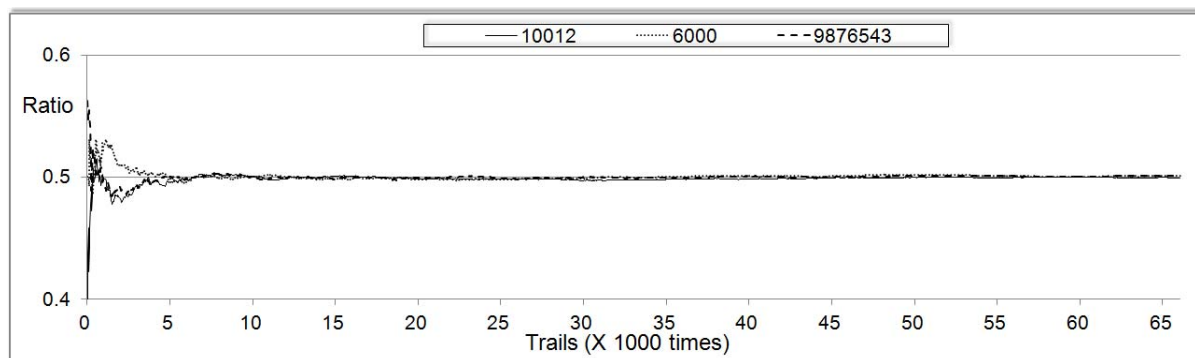


FIGURE 2. Ownership authentication process

the same, a 50% chance. Figure 2 shows that the ratio of the appearance of black pixels on the share with different secret seeds K will all converge to $1/2$ as the number of trials increases. We can see that regardless of the secret seed, the ratios maintained in any case are very close to $1/2$, with a deviation of less than 0.01.

In addition, we register the watermark by randomly comparing the grey value of pixels in the protected image to generate the corresponding shares. When the protected image suffers from an attack, almost every pixel value is changed. Why does our scheme still have such good resistance against attacks? It is because attacks will usually not significantly change the image's statistical property; otherwise, the protected image will be devalued. To illustrate further, when the protected image suffers some volumetric attacks, from the micro viewpoint, every pixel suffers some kind of modification, but from the macro viewpoint, the attacked image still looks the same as the original, which implies that the white regions will still be bright and the black regions dark. Therefore, if the gray value of pixel A is greater than pixel B, it will remain so most of the time after attacks. On the other hand, some geometric attacks, such as geometric distortion, rescaling and jitter, change the position of pixels A and B in relation to their neighborhood. The comparison results may still remain since the continuity property of the image ensures that the gray values in the neighborhood will usually not differ sharply from each other. These are the reasons why, when we compare the grey value of pixel pairs picked during the authentication phase, the result can still be kept the same as that of the original comparison during the registration phase. Utilizing the conservative property of an image is one of the major advantages of our method. In short, our method demonstrates that even when the image suffers from various attacks it still maintains good robustness.

5. Conclusion. In this paper, a novel copyright protection scheme for digital images based on visual cryptography and the law of large numbers is proposed. The law of large numbers is employed to ensure the generation of the randomly distributed half-black-and-half-white shares, which satisfies the demand of VC for security.

Our method can clearly identify the retrieved watermark even when attacks badly damage the host image due to the fact that most such attacks do not cause significant change to the statistical properties of the original image. The attacked image still looks similar to the original one. Therefore, comparison of the grey value of the pixel pairs picked during the authentication phase shows that the results remain the same as that of the original comparison during the registration phase.

In addition, our method also takes full advantage of the continuity property of color distribution of the host image and proves to have strong robustness to resist jitter attack which is difficult to handle for most existing watermarking techniques. Although from

the micro viewpoint the chosen pixel locations are not the same before and after the jitter attacks, however the continuity of the color distribution of the image makes the value in the neighboring areas similar. Hence, despite the locations before and after the attacks not being the same, as long as the pixels to be compared are picked from neighboring areas, the results will be close to that of the original comparison. With our approach, the master share M' will be similar to the original master share M . The same principle goes for the retrieved watermark.

The other advantages of our method are: (a) registration of the watermark does not affect the original image; (b) the watermark can be retrieved without the need of the original image; (c) the watermark is not limited by the size of the protected image; (d) multiple watermarks can be registered in a single image without damaging the other ones; (e) the unexpanded method solves the problem of larger volume of storage space and transmission time as well.

Acknowledgment. This work is partially supported by the National Science Council of Taiwan under contract NSC-93-2213-E-032-033. The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

REFERENCES

- [1] M. Naor and A. Shamir, Visual cryptography, *Advances in Cryptology-Eurpocrypt'94, Lecture Notes in Computer Science*, vol.950, pp.1-12, 1995.
- [2] C. C. Chang, J. Y. Hsiao and J. C. Yeh, A colour image copyright protection scheme based on visual cryptography and discrete cosine transform, *Imaging Science Journal*, vol.50, no.3, pp.133-140, 2002.
- [3] Y. C. Hou, Copyright protection based on visual cryptography, *Proc. of SCI2002*, Orlando, FL, USA, vol.13, pp.104-109, 2002.
- [4] C. C. Wang, S. C. Tai and C. S. Yu, Repeating image watermarking technique by the visual cryptography, *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol.E83-A, no.8, pp.1598-1598, 2000.
- [5] C. S. Hsu and Y. C. Hou, An image size unconstrained ownership identification scheme for gray-level and color ownership statements based on sampling methods, *Journal of Systems and Software*, vol.79, no.8, pp.1130-1140, 2006.
- [6] H. Luo, F.-X. Yu, S.-C. Chu and Z.-M. Lu, Hiding multiple watermarks in transparencies of visual cryptography, *International Journal of Innovative Computing, Information and Control*, vol.5, no.7, pp.1875-1881, 2009.
- [7] L. Fan, T. Gao and Q. Yang, A novel watermarking scheme for copyright protection based on adaptive joint image feature and visual secret sharing, *International Journal of Innovative Computing, Information and Control*, vol.7, no.7(A), pp.3679-3694, 2011.
- [8] Y. C. Hou and P. M. Chen, An asymmetric watermarking scheme based on visual cryptography, *Proc. of ICSP*, Beijing, China, vol.2, pp.992-995, 2000.
- [9] S. H. Low and N. F. Maxemchuk, Performance comparison of two text marking methods, *IEEE Journal on Selected Areas in Communications*, vol.16, no.4, pp.561-572, 1998.
- [10] I. J. Cox, J. Kilian, T. Leighton and T. Shamoon, Secure spread spectrum watermarking for multimedia, *IEEE Trans. Image Processing*, vol.6, no.12, pp.1673-1687, 1997.
- [11] Y. S. Kim, O. H. Kwon and R. H. Park, Wavelet based watermarking method for digital images using the human visual system, *Electronics Letters*, vol.35, no.6, pp.466-468, 1999.
- [12] R. G. van Schyndel, A. Z. Tirkel and C. F. Osborne, A digital watermark, *Proc. of IEEE Int. Conf. Image Processing*, Austin, TX, vol.2, pp.86-90, 1994.
- [13] S. Katzenbeisser and F. A. P. Petitcolas, *Information Hiding Techniques for Steganography and Digital Watermarking*, Arden House, Inc., Norwood, MA, 2000.