# Watermarking Scheme Based on Wavelet Transformation and Visual Cryptography

Young-Chang Hou, Shih-Chieh Wei, Hsin-Ju Liu, and A-Yu Tseng

***Abstract*—Based on the principles of the visual cryptography and the law of large numbers, the unexpanded shares are generated during the processes of embedding and verifying the hidden watermark. The watermark embedding is done in the frequency domain, which can be decoded by the human visual system (HVS) without the necessity of any complicated computation and the help of the original image. Experimental results indicated that our method had a good robustness on darkening, lightening, blurring, sharpening, noise, distorting, jitter, joint photographic experts group (JPEG) compression, and crop attacks.**

***Index Terms*—Copyright protection, digital watermarking, law of large numbers, visual cryptography, wavelet transformation.**

## 1. Introduction

Thanks to the incoming digital age and rapid development of the 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. But in another aspect, without proper protection of information from being stolen and tampered, the property owner can do nothing to deal with these attacks. Nowadays, numbers of mechanisms used to protect the intellectual property rights (IPR) have been proposed and the digital watermarking technology is one of them.

The so-called digital watermarking refers to using the characteristics that human eye can not notice the subtle changes of embedding a set of digital signals into a digital image. When it is necessary to verify the ownership of the data, the embedded signals can then be extracted from the image. This set of digital signals is named as “watermark”.

The watermarking technology can be classified into different kinds of categories[1] according to the attributes of watermark visibility, resistance against attacks, embedding methods, and extraction methods. In visibility, it can be divided into two types: visible and invisible; by resistance to attacks, it can be classified into three types: robust, fragile, and semi-fragile; by different watermark extraction methods, it can be classified into three groups: blind, non-blind, and semi-blind; and by embedding methods, it can be divided into the spatial domain and frequency domain.

The concept of visual cryptography was originally proposed by Naor and Shamir[2], which is a mechanism for protecting information. The secret image is decomposed into multiple haphazard sharing images (shares). To decrypt, we can simply superimpose these sharing images and take advantage of the human visual system to complete the decryption process, without any need of complex computation.

Since visual cryptography was proposed, several related works[3]–[14] were presented thereafter. Some of them applied the concept of visual cryptography to the field of watermarking[3],[5],[8]–[10],[12]. Hou[3] employed the highest bit-plane of the secret image to produce the share images needed in the visual cryptography. But the drawbacks are that the share images’ size is twice as big as the secret one, and there may be misinterpretation if some images are very similar to the secret one. Hsu and Hou[10] produced share images by comparing 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 the share images and restored image are expanded to four times the size of the original one. Hou and Huang[8] improved Hsu and Hou’s shortcomings. They used the statistical characteristics of the law of large numbers to produce non-expanded share images through comparing randomly selected pixel pairs. However, when the image is attacked, employing single pixel value is more vulnerable than that engaging the sample mean of a plurality of pixels. This will lead to more errors when retrieving the watermark from the attacked image.

The aforementioned methods are based on the spatial

Manuscript received May 17, 2013; revised June 30, 2013. This work was supported by the National Science Council under Grant No. NSC101-2221-E-032-047.

S.-C. Wei is with the Department of Information Management, Tamkang University, New Taipei City (Corresponding author e-mail: seke@mail.im.tku.edu.tw).

Y.-C. Hou, H.-J. Liu and A.-Y. Tseng are with the Department of Information Management, Tamkang University, New Taipei City (e-mail: ychou@mail.im.tku.edu.tw, meteor.s212@gmail.com; vega5633@yahoo.com.tw).

A-Y. Tseng is also with the Computer Center, National Open University, New Taipei City.

Digital Object Identifier: 10.3969/j.issn.1674-862X.2014.01.020

domain. The major problem of these methods is their less robustness after receiving an attack. Therefore, most of the researchers were focused on the frequency domain[5],[9],[12],[15],[16]. The common practice is to exploit different transformation technologies to convert the pixel values of the image in the spatial domain to the amplitude coefficients of the frequency domain. The advantages of frequency domain are not only its better resistance to attacks, but also its distinctiveness of the information importance which are represented by diverse frequencies. We can do different levels of image processes in accordance with the requirements and its importance. Chang *et al*.[5] extracted DC (zero-frequency) coefficients from the original image to produce share images. Hsieh and Huang[9] distributed the sharing blocks by the averages of lower-lower 2 (LL2) coefficients of wavelet transforms and their corresponding positions to produce the share images. Lou *et al*.[12] also used wavelet transforms to extract the coefficients of the middle frequency and low frequency to generate share images. The common defect of the above three works is that the size of the watermark should be much smaller than the size of the protected images, only 1/144, 1/64, and 1/64, respectively. In addition, Chang *et al*.[5] had to calculate the number of white dots in every 3 pixels×3 pixels block when extracting the watermark to restore the color of the watermark, and Hsieh and Huang[9] and Lou *et al*.[12] needed to do the XOR operation on share images, all of which are unable to take advantage of visual cryptography to decrypt the stacked images by using only the human visual system.

This research aims to improve the abovementioned defects. The authors employ a non-expanded scheme and embedded the watermark in frequency domain to produce the share images. When the protected image once encounter an attack, the extracted watermark could still be robust. The process of extracting watermark uses the mechanism of visual cryptography. By superimposing share images, the watermark emerges naturally without the help of any complex arithmetic computation.

## 2. Proposed Sharing Model

Watermark embedding techniques must take the following points into account. Firstly, in the embedding method of the spatial domain, to avoid any clues to be easily found, the quantity and the location of the hidden information are particularly critical. Its utility also decreases for these restrictions. Secondly, in the embedding method of frequency domain, the computation is more complex and therefore requires more calculation processes in watermark embedding and extraction. Thirdly, adding a watermark will modify the information of the original image, which may destroy the visual quality of the image. Fourthly, it often needs to refer to the original image while extracting the watermark. Once the original image cannot be reached, the watermark cannot be extracted. This will lose the flexibility of the ownership verification.

This study combines the probability theory, the law of large numbers, and the transformation to the frequency domain, with the characteristics of the non-expanded visual cryptography, to construct a digital image protection scheme which is used to safeguard the IPR. The concept of visual cryptography is used to produce some half black and half white share images. When the share images are superimposed, the content of the secret image can be revealed naturally. Some other days, when identity authentication is needed, as long as the embedded watermark can be revealed on the stacked image when we superimpose the two share images together, in which one is produced from the controversial image and the other is kept in our hands as an ownership certificate, the purpose of verifying IPR is achieved.

In this study, the basic concept is that every share image processed by the visual cryptography has 50% of black points and 50% of white points on it. From the viewpoint of coding theory, each share image is a combination of a series of 0 and 1. So if we can generate the proper “01” series from the protected digital asset, then we can produce the share image we need. Therefore, the research of combining the visual cryptography and the watermarking technology lies on: how to obtain the “01” series of the share image (master share) through the protected assets, and then combine with the watermark to produce the share image (ownership share) for verifying the ownership.

We find that an image usually can maintain a certain image quality when it is subjected to the attacks of image processing software. That is, after attacks the original image still keeps the same mountains, or the same seas; a red region is still maintained to be red and the green part is also kept to be green. Though every pixel value of the attacked image has been changed a little bit, but most parts of the appearance are almost the same with those before. It is not difficult to find that the grey value distribution of the image pixels, owing to the statistical conservative property, will not be easily changed and then maintains certain regularity.

First of all, we adopt the frequency domain approach to perform a three-level wavelet transform to the protected image. Because each coefficient of the LL3 low-frequency band condenses the values of many surrounding pixels, it retains the most important information of the original image. Next, we compare two pixel values ($x$, $y$) retrieved from the LL3. There are only two cases, ($x\geq y$) or ($x\leq y$) that can occur. According to the theory of the law of large numbers, the probabilities of the occurrences of the cases ($x>y$) and ($x<y$) are equal. As for the case of ($x=y$), half of which, for example, each having an even coordinate is classified into

the ($x>y$) group; the other half, in which each coordinate is odd is classified into the ($x<y$) group. All the results of each comparison look like a chaotic arrangement, but because of the very large number of tests, a 256 pixels× 256 pixels watermark, for example, will be at least executed more than sixty-five thousand trials, the testing result of the presences of case ($x\geq y$) or ($x\leq y$) will be very close to 1/2 of all the number of tests according to the law of large numbers. Whenever appearing the case of ($x\geq y$), we will produce a black point (1) on the master share; while for the case of ($x\leq y$), we produce a white point (0) instead. Thus, we can let the share image have disorderly 1/2 black dots and 1/2 white dots to meet the security requirement of the visual cryptography.

With the master share and the watermark, following the encryption rules of visual cryptography, we can create another share image (the ownership share), as shown in Fig. 1. The master share can then be discarded, but the ownership share represents the certificate of our identity authentication, and therefore should be properly kept. We can register this ownership share to the certification authority (CA), and then use it to verify our IPR in the future. Because of the less sensitive characteristics of the LL3 coefficients to image attacks, the comparison results of the pixel pairs will not easily be changed. If there are disputes over the ownership of the intellectual property someday, we can simply generate the master share′, which has a really good robustness from the controversial image, and superimpose it onto the registered ownership share. If the stacked image can show the watermark information, the ownership of this asset is proved to be ours. This way achieves the purpose of ownership verification, as shown in Fig. 2.

There are two advantages to apply the visual cryptography to the watermark mechanism. Firstly, the information of the original image remains intact. As the watermark is not actually embedded into the original image, hence the intellectual property will not be damaged. This benefit is particularly suitable for the application areas that original images are not allowed to be modified, such as medical images and satellite images. Secondly, the watermark is easy to be extracted. By simply superimposing the share images on each other, we can take the advantage of the human visual system to extract the watermark. Since it does not need complex mathematical calculations, even in the environment without the computer, it can easily be done.

## 3. Experimental Results and Discussions

In this study, we ran our experiments under the Microsoft Windows XP with service pack 3 on a personal computer with Intel Core 2 Duo processor and 2 GB memory, and we also used Java SE 6.0 SDK as our program development tools. The experimental subject was a 512 pixels×512 pixels grayscale image named “vegetable” (as shown in Fig. 3 (a)). The embedded watermark was a 256 pixels×256 pixels black and white image showing the “Information Management Department of Tamkang University” in Chinese (see Fig. 3.(b)).

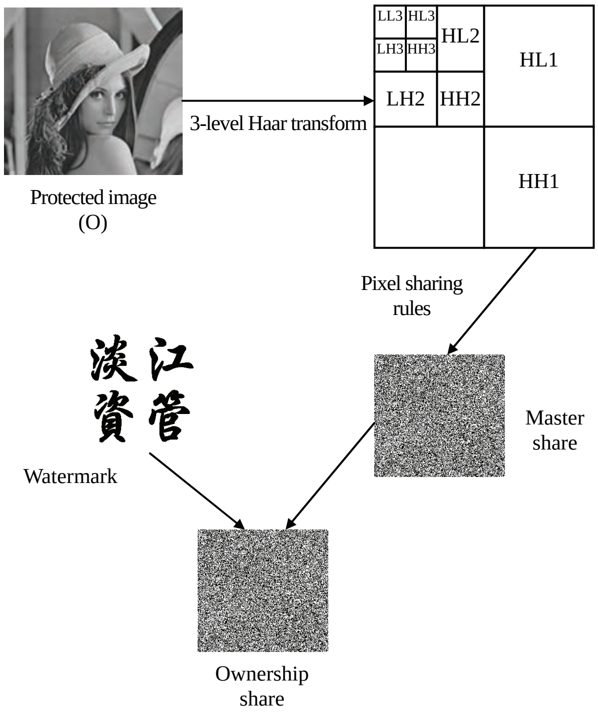


Fig. 1. Watermark embedding process.

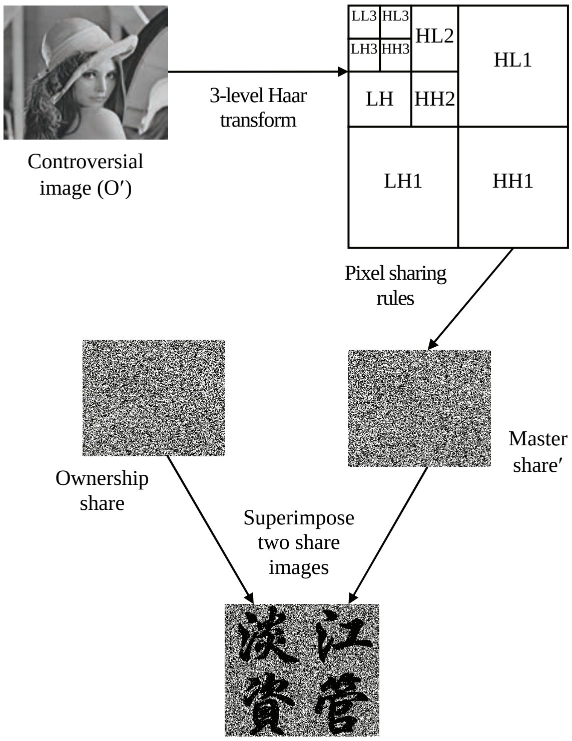
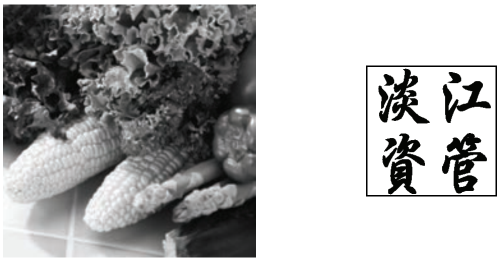


Fig. 2. Watermark verification process.



(a) (b)

Fig. 3. Protected image and watermark: (a) vegetable (512 pixels×512 pixels) and (b) watermark (256 pixels×256 pixels).

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. In order to measure the degree of the destruction that certain attack has done to the original image, the peak signal-to-noise ratio (PSNR) was used to judge the similarity between the attacked image and the original one. The formula is

$$\text{PSNR} = 10 \times \log\left(255^2 / \text{MSE}\right) \tag{1}$$

$$\text{MSE} = \left[1 / \left(M_1 \times M_2\right)\right] \sum_{i=1}^{M_1} \sum_{j=1}^{M_2} \left(c_{i,j} - c'_{i,j}\right)^2 \tag{2}$$

where $c_{i,j}$ represents the gray-level value of a certain pixel in the original image, $c'_{i,j}$ represents the corresponding pixel value in the image which is suffered from an attack, and $M_1$ and $M_2$ represent the length and the width of both images. The higher the value of PSNR is, the less the distortion is. In other words, the lower value of PSNR represents the original image suffers from a more serious attack and is much more different from the original one.

We took normalized correlation (NC) as another indicator to examine the degree of the similarity between the retrieved watermark and the original one. The definition of NC is

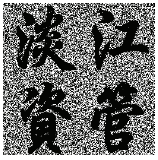
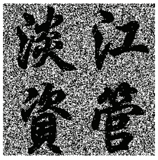
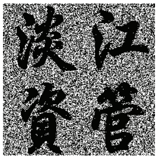
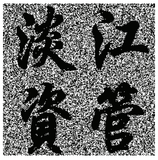
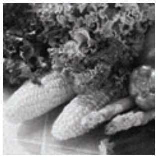
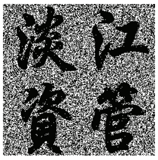
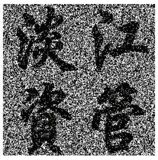
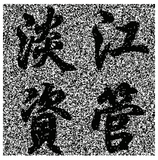
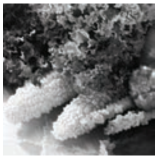
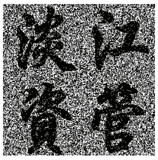
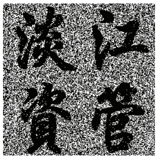
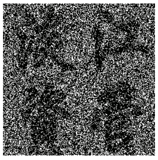
$$\text{NC} = \left[ \frac{\sum_i \sum_j W(i,j) W'(i,j)}{\sum_i \sum_j [W(i,j)]^2} * \frac{\sum_i \sum_j [1 - W(i,j)][1 - W'(i,j)]}{\sum_i \sum_j [1 - W(i,j)]^2} \right]^{1/2} \tag{3}$$

where $W(i, j)$ represents the bit value of a certain pixel in the original watermark, and $W'(i, j)$ represents the corresponding bit value in the retrieved watermark which is taken from the controversial image. The objective of the NC is to calculate the ratio that a black (white respectively) pixel of the original $W$ is also a black (white respectively) one in $W'$. The value of NC must be between 0 and 1. When the value of NC is larger, it represents that the degree of the similarity between $W$ and $W'$ is higher; and when the value of NC is smaller, the degree of similarity is lower.

Generally speaking, if the PSNR value is small and the NC value is large, then they represent that the hidden watermark has a higher resistance to attacks. The results of the experiments are shown in Table 1.

The experimental results show that, despite a certain degree of destruction caused by the various attacks to the original image, we are still able to clearly recognize the four Chinese words "淡江資管" presented in the retrieved watermark. So when an image encounters any attack, the basic statistical properties of the image will not be changed significantly. Perhaps, from a micro point of view, every pixel value subjects to a varying degree of modification; but in a macroscopic perspective, the original look of the image after attacks can still be recognized, i.e., the original black is still blacker and the original white is still whiter.

Table 1: Experimental results of different attacks

| Attacked image | Reconstructed watermark | Attacked image | Reconstructed watermark |
|---|---|---|---|
| |  | |  |
| JPEG: JPEG compression at a 5% ratio | | Sharpening: Sharpen the edges | |
| PSNR=27.63 dB | NC=0.995 | PSNR=22.74 dB | NC=0. 987 |
| |  | |  |
| Lightening: 20% brighter | | Darkening: 20% darker | |
| PSNR=25.73 dB | NC=0.993 | PSNR=26.60 dB | NC=0.996 |
|  |  | |  |
| Noising: Add 20% Gaussian noise | | Cropping: Cut off the upper left corner (1/3×1/3) | |
| PSNR=21.69 dB | NC=0.990 | PSNR=12.64 dB | NC=0.930 |
| |  |  |  |
| Blurring | | Geometric distortion: Distortion of a ripple effect | |
| PSNR=18.05 dB | NC=0.976 | PSNR=14.76 dB | NC=0.953 |
| |  | |  |
| Rescaling: Reduce to 1/2 of the original size first, and then zoom back to the original size | | Jitter: Cut off a 16-pixel wide column from the leftmost of the picture, and then append it to the rightmost side | |
| PSNR=34.76 dB | NC=0.980 | PSNR=9.73 dB | NC=0.821 |

Since the data of the low frequency LL3 region are the condensed results of the surrounding pixel values, these values are more representative for their neighboring pixels and are not easy to be greatly modified. So, when the values of the pixel pairs are compared, the same results as those of the original can almost be kept, which ensures a better robustness. This is the reason that the general lightening and darkening attacks have almost no effect in our method and will not alter the extracted watermark at all. The proposed method can also retain a good resistance to a higher compression ratio of the JPEG compression attack. Not only the image that looks only a little different from the original image have a high NC value, but also the image that encounters a severer attack (smaller PSNR) also keeps a high NC value and the reconstructed watermark can still be clearly identified. This also proves that the watermark produced by the characteristics of the statistical properties has a very good resistance to attacks and can meet the requirements of the unambiguity and robustness of the digital watermark.

## 4. Conclusions

This study takes advantages 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 Haar wavelet transform, the wavelet transform coefficients of the LL3 are used as the population. Since these coefficients concentrate the pixel information of the original image, they can reduce the variations of single pixel and make the comparison results more stable. So even when the protected images are attacked, the comparison results of pixels are not easily to be changed, that is, the master share′ and the master share are quite consistent. Therefore, the NC value of the superimposed watermark can still be maintained at 95% or more, which reveals that our approach has a good resistance to attacks. The advantages of the proposed image ownership protection method include: 1) The watermark embedding scheme does not affect the contents of the original image; 2) The watermark extracting scheme does not need the assistance of the original image; 3) The watermark's size is not restricted to the size of the protected image; 4) Additionally, the non-expanded approach also solves the larger volume problem of the share image.

## References

[1] S.-J. Lee and S.-H. Jung, "A survey of watermarking techniques applied to multimedia," in *Proc. of IEEE Int. Symposium on Industrial Electronics*, Pusan, 2001, pp. 272–277.

[2] M. Noar and A. Shamir, "Visual cryptography," in *Advances in Cryptology: Eurpocrypt'94*, Berlin: Springer-Verlag, 1995, pp.1–12.

[3] Y.-C. Hou, "Copyright protection based on visual cryptography," in *Proc. of Systemics, Cybernetics and Informatics 2002*, Orlando, 2002, pp. 104–109.

[4] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Extended schemes for visual cryptography," *Theoretical Computer Science*, doi: 10.1.1.40.523.

[5] C.-C. Chang, J.-Y. Hsiao, and J.-C. Yeh, "A colour image copyright protection scheme based on visual cryptography and discrete cosine transform," *The Imaging Science Journal*, vol. 50, no. 3, pp. 133–140, 2002.

[6] Y.-C. Hou, "Visual cryptography for color images," *Pattern Recognition*, vol. 36, no. 7, pp. 1619–1629, 2003.

[7] Y.-C. Hou and Z.-Y. Quan, "Progressive visual cryptography with unexpanded shares," *IEEE Trans. on Circuits and Systems for Video Technology*, vol. 21, no. 11, pp. 1760–1764, 2011.

[8] Y.-C. Hou and P.-H. Huang, "An ownership protection scheme based on visual cryptography and the law of large numbers," *Int. Journal of Innovative Computing, Information and Control*, vol. 8, no. 6, pp. 4147–4156, 2012.

[9] S.-L. Hsieh and B.-Y. Huang, "A copyright protection scheme for gray-level image based on secret sharing and wavelet transformation," in *Proc. of Int. Computer Symposium*, Taipei, 2004, pp. 661–666.

[10] C.-S. Hsu and Y.-C. Hou, "Copyright protection scheme for digital images using visual cryptography and sampling methods," *Optical Engineering*, vol. 44, no. 7, 2005, doi: 10.1117/1.1951647.

[11] R. Ito, H. Kuwakado, and H. Tanaka, "Image size invariant visual cryptography," *IEICE Trans. on Fundamentals of Electronics, Communications and Computer Science*, vol. E82-A, no. 10, pp. 2172–2177, 1999.

[12] D.-C. Lou, H.-K. Tso, and J.-L. Liu, "A copyright protection scheme for digital images using visual cryptography technique," *Computer Standards & Interfaces*, vol. 29, no. 1, pp. 125–131, 2007.

[13] S. J. Shyu, "Image encryption by random grids," *Pattern Recognition*, vol. 40, no. 3, pp. 1014–1031, 2007.

[14] S.-F. Tu and Y.-C. Hou, "On the design of visual cryptographic methods with smooth-looking decoded images of invariant size for gray level images," *Imaging Science Journal*, vol. 55, no. 2, pp. 90–101, 2007.

[15] S. Joo, Y. Suh, J. Shin, H. Kikuchi, and S. J. Cho, "A new robust watermark embedding into wavelet DC components," *ETRI Journal*, vol. 24, no. 5, pp. 401–404, 2002.

[16] Y. Wang, J. F. Doherty, and R. E. Van Dyck, "A wavelet-based watermarking algorithm for ownership verification of digital images," *IEEE Trans. on Image Processing*, vol. 11, no. 2, pp. 77–88, 2002.

**Young-Chang Hou** received his B.S. degree in atmospheric physics from National Central University, Taiwan in 1972, his M.S. degree in computer applications from Asian Institute of Technology, Bangkok, Thailand in 1983, and his Ph.D. degree in computer science and information engineering from National Chiao-Tung

University, Taiwan in 1990. From 1976 to 1987, he was a senior engineer with Air Navigation and Weather Services, Civil Aeronautical Administration, Taiwan, where his work focused on the automation of weather services. From 1987 to 2004, he was on the faculty at the Department of Information Management, National Central University. Currently, he is a professor with the Department of Information Management, Tamkang University, Taiwan. His research interests include digital watermarking, information hiding, fuzzy logic, genetic algorithms, and visual cryptography.

**Shih-Chieh Wei** received his B.E. degree in electrical engineering from National Taiwan University, Taiwan in 1988, his M.S. degree in computer science from National TsingHua University, Taiwan in 1990, and his Ph.D. degree in systems engineering from Osaka University, Japan in 1998. He is currently an assistant professor with the Department of Information Management, Tamkang University, Taiwan. His research interests include information security, information retrieval, and GPU-based high performance computing.

**Hsin-Ju Liu** received her B.S. degree in administration management from Ming Chuan University, Taiwan in 2007, her M.S. degree in information management from Tamkang University, Taiwan in 2010. Her research interests include digital image processing, digital watermarking, and visual cryptography.

**A-Yu Tseng** received her B.S. degree in computer science in 1990, her M.S. degree in information management in 2008, both from Chinese Culture University, Taiwan. Now she is pursuing the Ph.D. degree with the Department of Information Management, Tamkang University, Taiwan. Her research interests include evaluation, design, and analysis of information systems, visual cryptography, image processing, and secret sharing.