Secret image sharing with capability of share data reduction

Chang-Chou Lin
Wen-Hsiang Tsai
National Chiao Tung University
Department of Computer and Information Science
Hsinchu, Taiwan 300
E-mail: gis85529@cis.nctu.edu.tw

Abstract. A novel approach to secret image sharing based on a (k,n)-threshold scheme with the additional capability of share data reduction is proposed. A secret image is first transformed into the frequency domain using the discrete cosine transform (DCT), which is applied in most compression schemes. Then all the DCT coefficients except the first 10 lower frequency ones are discarded. And the values of the 2nd through the 10th coefficients are disarranged in such a way that they cannot be recovered without the first coefficient and that the inverse DCT of them cannot reveal the details of the original image. Finally, the first coefficient is encoded into a number of shares for a group of secret-sharing participants and the remaining nine manipulated coefficients are allowed to be accessible to the public. The overall effect of this scheme is achievement of effective secret sharing with good reduction of share data. The scheme is thus suitable for certain application environments, such as the uses of mobile or handheld devices, where only a small amount of network traffic for shared transmission and a small amount of space for data storage are allowed. Good experimental results proving the feasibility of the proposed approach are also included. [DOI: 10.1117/1.1588661]

Subject terms: secret image sharing; data hiding; share data reduction; visual cryptography; image compression; discrete cosine transform.

Paper 020511 received Nov. 26, 2002; revised manuscript received Jan. 16, 2003; accepted for publication Feb. 14, 2003.

1 Introduction

Because of the ease of digital duplication and tampering, data security becomes an important issue nowadays. Private-key and public-key systems are two well-known cryptosystems.[1–4] They enable secret data to be kept securely in such a way that an opponent cannot understand what the secret data mean. The secret, which is called plaintext, is first encrypted, using a predetermined key, and the resulting ciphertext is kept by the secret owner. The opponent, who wants to invade, just sees the manipulated ciphertext that is meaningless in semantics but the assigned receiver, who knows the encryption key, can decrypt the ciphertext and reconstruct the plaintext to understand what it means. The data encryption standard (DES) and Rivest, Shamir, Adleman (RSA) are two representative methods.

Other than cryptography, data hiding provides another way to keep data secure. A method of this kind can be employed to embed imperceptibly secret information in a preselected meaningful image, called a camouflage image, to avoid attacks from invaders. Many techniques can be used to make changes in the original image invisible. Unlike utilizing a particular cipher algorithm to protect secret information from illicit access, the purpose of hiding secret data behind a camouflage image is to make an invader unaware of the existence of the secret. Numerous schemes have been developed to achieve the goal of data hiding.[5–8]

On the other hand, a mechanism is desirable for situations where permission to access the secret depends not on one person but on a group of people. The study of such a topic is secret sharing, and it has many real-world applications. For example, it might be necessary in a company for three managers to share a digital document, and only when all or two of the three managers appear with mutual agreement can they work together to see the document through a digital access scheme. The idea here is like the case in a bank when a vault can be opened only by more than one teller in charge of the vault, or like the case in a story that a treasure map was torn into three pieces of which two or more may be combined together to give a clue for accessing the treasure. This concept of secret sharing provides a good solution to the requirements of both security protection and access flexibility. Security can be achieved through the ownership of the secret held together by a group of people. And no need of participation of all the group members in the secret access process avoids the impossibility of secret reconstruction due to the absence of a certain member. This is indeed an advantage of secret sharing, which is not found in other cryptosystems.

A well-known technique for secret sharing is the cryptography method proposed by Shamir.[9] The method, called (k,n)-threshold secret sharing, was designed to encode a secret data set into n shares and distribute them to n participants, where only when any k or more of the shares are collected can be secret data be recovered. After the scheme was proposed, many related topics have been studied.[10–12] However, the resulting methods are suitable for only a few

 0091-3286/2003/$15.00

types of digital data, such as a text file, a password, an encryption/decryption key, etc.

Due to the widespread uses of images, how to share a secret image has attracted wide attention in recent years. Naor and Shamir[13] proposed first the idea of visual cryptography to share secret images. The scheme provides an easy and fast decryption process that includes the steps of xeroxing the shares onto transparencies and stacking them to reveal the shared image for visual inspection. This scheme, which differs from traditional secret sharing, does not require complicated cryptographic mechanisms and computations. Instead, it can be decoded directly by the human visual system. Great expansion of share data sizes and the fact that it deals only with binary images limit the applicability of this scheme. Although an extended scheme for color images[14] was proposed later, it handles images with only a small number of colors and inherits the characteristic of share data size expansion.

In this paper, we propose a scheme that does not manipulate images in the spatial domain as the mentioned visual cryptography does. Instead it transforms images into the frequency domain by the discrete cosine transform (DCT), resulting in a set of transform coefficients. For most natural images, a significant number of the high-frequency coefficients are small in magnitude and can be discarded. Therefore, in this paper we reserve only low-frequency DCT coefficients that keep most visual information in images. This drastically decreases the size of the data that must be shared, and guarantees the quality of the recovered image in the mean time. Furthermore, we randomize the values of all the reserved coefficients except the first one (called the DC value) by a designed transformation. The DC value is taken to be a key for this transformation. It is also used in the back transformation to recover the original coefficients. That is, the critical item for sharing is restricted to be just the DC value, and so the amount of information to be shared and that of the created share data both decrease noticeably. Therefore, the proposed scheme has the capabilities of sharing full-color images as well as reducing the share data size. The former capability extends the application scope of secret image sharing which is still quite limited so far, and the latter makes the proposed scheme more practical for certain applications, where the memory size and network bandwidth are restricted. For example, the scheme is suitable for applications to mobile or handheld devices, where only a small amount of network traffic for shared transmission as well as a small amount of space for data storage are allowed.

The remainder of this paper is organized as follows. Section 2 gives an overview of the proposed approach and describe the proposed process of encryption. Section 3 introduces proposed decryption method. Some experimental results are shown in Sec. 4. For ease of demonstration, we use gray-scale image data as examples. Finally, some conclusions are given in Sec. 5.

2 Proposed Process of Encryption

In the proposed process of image share encryption, first we divide a given secret image into 8×8 blocks and transform each block into the frequency domain by the DCT. We then reserve the first 10 DCT coefficients and discard the remaining ones. This reduces the size of the original secret image without degrading the image quality too much. Of course, if higher image quality is desired, we may keep more than 10 coefficients. Next, we perform a randomization process to change in a random way the values of the reserved DCT coefficients except the first one. The details are described later in this section. Without the help of the first coefficient, the use of the randomized 2nd through 10th coefficients is insufficient to recover the original secret image. So we just keep the first coefficient secret and let the others be public. Accordingly, the amount of shares that should be delivered to users and kept by them is reduced drastically. This saves network bandwidth and storage space requirement for each user. To guarantee the security of the first coefficient, we use the Shamir (k,n)-threshold scheme to share it. In the remainder of this section, we describe the details of the encryption process.

2.1 *Algorithm 1: The Process of Encryption*

The input is an $8b\times8b$ secret image I. The output is n sets of $b\times b$ shares, with each set delivered to a member in a group of n secret sharing participants. The steps are

Step 1. Divide I into $b\times b$ blocks, each with the size of 8×8 pixels.

Step 2. For each block B_i, $i=1,2,...,b\times b$, perform the following steps.

- 2.1 Transform each block into the frequency domain by the DCT.
- 2.2 Reserve the first 10 coefficients and discard the remaining ones.
- 2.3 Use the first coefficient C_1 as a seed into a random number generator f_R to generate a sequence of numbers $R_2, R_3, \ldots,$ and R_{10} in the range of $[0, C_1]$.
- 2.4 Replace respectively the 2nd through the 10th coefficients $C_2, C_3, \ldots, C_{10}$ with the values of $C_2' = R_2 \cdot \cdot C_2$, $C_2' = R_3 \cdot \cdot C_3, \ldots,$ $C_{10}' = R_{10} \cdot \cdot C_{10}$. Call this procedure a randomization process. And keep all C_1' in a public place.
- 2.5 Encrypt the first coefficient C_1 with the Shamir secret sharing scheme into n shares $S_{i1}, S_{i2}, \ldots, S_{in}$.

Step 3. For each secret sharing participant P_j, $j=1,2,...,n$, collect as a set W_j all the corresponding $b\times b$ shares $S_{1j}, S_{2j}, \ldots, S_{(b\times b)j}$, with each share S_{ij} from an image block B_i, and deliver W_j to him/her as his/her final secret share.

In step 1, we first divide the secret image into blocks and then perform the DCT to transform each of them into the frequency domain in step 2.1. This process is often done in the image compression field. The leading coefficients, which are often more significant to human vision, represent the magnitudes of lower frequencies. According to this

characteristic, we reserve only the first 10 coefficients and discard the remaining ones in step 2.2. This can reduce the size of the data to be shared, with little sacrifice of the quality of the reversely-transformed images. However, this is not the only step we adopt for share data reduction. After the randomization process in step 2.4 is performed, the image obtained from inversely transforming the modified coefficients will become noise. Consequently, these coefficients need not be shared but may be made public instead. Only when the value of the first coefficient is obtained can the original coefficient values $C_2, C_3, \ldots, C_{10}$ be solved by the following equations:

$$C_i = R_i - C_i' \quad i = 2,3,...,10. \tag{1}$$

In Eq. (1) R_i is obtained by using C_1 as a seed to generate a random number sequence, as is done in step 2.3. It is obvious that C_1 is now the only factor that we need to protect securely in the access control of the secret image. It is so used in step 2.5 by the Shamir (k,n)-threshold scheme to generate n shares for the group of n secret sharing participants. The details of this sharing process are described as follows. Based on a preselected secret integer value y and a preselected threshold k, and by using the following $(k-1)$-degree polynomial

$$F(x) = y + m_1 \times x + m_2 \times x^2 + \cdots + m_{k-1} \times x^{k-1} \mod p, \tag{2}$$

the generation of the n shares proceeds in the following way.

1. Choose y to be the value of C_1 that is to be shared.
2. Select the number k is to be no larger than n.
3. Choose p to be the nearest prime number larger than C_1.
4. Choose $k-1$ integer values $m_1, m_2, \ldots, m_{k-1}$ randomly in the range $[0,p)$.
5. Choose freely for the i'th secret sharing participant a value of x (denoted as x_i), with all x_i distinct from one another.
6. For each chosen x_i, compute a corresponding value of $F(x_i)$ by Eq. (2).
7. Take each pair of $[x_i, F(x_i)]$ as a share.

Here we use modular arithmetic instead of real arithmetic as Shamir did. The set of all integers modulo a prime number p forms a Galois field. In this field, we can reconstruct the polynomial $F(x)$ using an interpolation method in the secret recovery phase, which is described in the next section.

So far, we have accomplished a mechanism that not only shares a secret image but also generates a small amount of share data for each participant. In our proposed scheme, the characteristic that lower frequencies preserve most information based on human vision after an image is transformed into the frequency domain is utilized. So coefficients of higher frequencies can be discarded and the information we must process decreases preliminarily. Moreover, an extra randomization process is applied to manipulate the remaining coefficients and further decreases the amount of information that must be securely dealt with.

Note here that an extra step could be added between steps 2.4 and 2.5 if further data compression is required. That is, we can perform a process called quantization to reduce the amount of data to be kept. Such quantization can be represented by the following formula:

$$C_i'' = \text{round}(C_i'/Q_i), \tag{3}$$

where Q_i is called a quantization factor, round$(\cdot)$ is a rounding function, and C_i'' is the quantized value. The value of Q_i affects the transformed image size and the image quality, and is a trade-off between them.

3 Proposed Process of Decryption

In this section, we first describe the process of decryption as an algorithm, and then explain the details.

3.1 *Algorithm 2: The Process of Decryption*

The input is the n sets of secret shares held by the n secret sharing participants. The output is an $8b \times 8b$ secret image with $b \times b$ blocks. The steps are

Step 1. Divide the set of secret shares of each participant P_j of the n ones into $b \times b$ shares $S_{1j}, S_{2j}, \ldots, S_{(b\times b)j}$.

Step 2. For each image block B_i of the $b \times b$ ones to be reconstructed, perform the following steps.
- 2.1 Reconstruct the value of C_1 using the interpolation method mentioned in Ref. 9 from the n corresponding shares $S_{i1}, S_{i2}, \ldots, S_{in}$ held by the n participants, respectively.
- 2.2 Use C_1 as a seed into the random number generator f_R identical to that used in the process of encryption to generate a number sequence R_2 through R_{10}.
- 2.3 Acquire C_2' through C_{10}' from the public place where they are kept.
- 2.4 Compute C_2 through C_{10} using Eq. (1), which is called a derandomization process.
- 2.5 Perform the inverse DCT using the coefficient C_1 as well as C_2 through C_{10} obtained from the previous steps to obtain the desired block image B_i in the spatial domain.

Step 3. Combine in order all the block images B_1 through $B_{b\times b}$ obtained in the last step to reconstruct the original secret image.

In the preceding algorithm, we first divide in step 1 the secret share set into $b \times b$ shares, each being obtained from one block in the encryption process. Then we try to recover the block images one by one in step 2. In step 2.1, we recover the value of C_1 of each block. The details[9] are described as follows.

1. Collect at least k secret shares from the n ones to form a system of equations as follows:

$$
\begin{aligned}
F(x_1) &= y + m_1 \times x_1 + m_2 \times x_1^2 + \cdots + m_{k-1} \times x_1^{k-1} \bmod p, \\
F(x_2) &= y + m_1 \times x_2 + m_2 \times x_2^2 + \cdots + m_{k-1} \\
&\quad \times x_2^{k-1} \bmod p, \\
&\vdots \\
F(x_k) &= y + m_1 \times x_k + m_2 \times x_k^2 + \cdots + m_{k-1} \\
&\quad \times x_k^{k-1} \bmod p.
\end{aligned} \tag{4}
$$

2. Use the Lagrange method to solve the k unknowns, $m_1, m_2, \ldots, m_{k-1}$, and y, in the preceding k equations, and reconstruct the $(k-1)$-degree polynomial $F(x)$ described by Eq. (2). Note that the x_i and $F(x_i)$ in Eq. (4) with $1 \leqslant i \leqslant k$ are $2k$ known values collected from the k secret shares.
3. Construct $F(x)$ by the following formula:

$$
\begin{aligned}
F(x) &= F(x_1) \frac{(x-x_2)(x-x_3)\cdots(x-x_k)}{(x_1-x_2)(x_1-x_3)\cdots(x_1-x_k)} \\
&\quad + F(x_2) \frac{(x-x_1)(x-x_3)\cdots(x-x_k)}{(x_2-x_1)(x_2-x_3)\cdots(x_2-x_k)} + \cdots \\
&\quad + F(x_k) \frac{(x-x_1)(x-x_2)\cdots(x-x_{k-1})}{(x_k-x_1)(x_k-x_2)\cdots(x_k-x_{k-1})} \bmod p.
\end{aligned} \tag{5}
$$

4. Take the secret value $C_1 = y$ to be $F(0)$.

Note that according to Shamir,[9] if fewer than k secret shares are collected, the k unknowns cannot be solved and the desired y value cannot be reconstructed. After we get the value of C_1, we use it in step 2.2 as a seed to generate a random number sequence, which includes just the values of R_2 through R_{10} also generated in the encryption process. Then we acquire in step 2.3 the values of C_2' to C_{10}', which are kept publicly and obtain C_2 to C_{10} by the derandomization process of step 2.4. Now, we have all the values of coefficients C_1 to C_{10}, so the inverse DCT can be performed in step 2.5 to get the original image block. Finally, we combine these image blocks in order to reconstruct the original secret image.

Note that if quantization was executed in the encryption process, a corresponding restoration action should be taken between steps 2.3 and 2.4 in the decryption process, which is described as

$$
C_i^* = C_i'' \times Q_i, \tag{6}
$$

where Q_i is the quantization factor in Eq. (3), C_i'' is the quantized value obtained in the encryption process, and C_i^* is the restored value which is used as a substitution of C_i' in the following steps of the decryption process.

4 Experimental Results

In this section, some experimental results are shown to prove the feasibility of the proposed scheme. For ease of demonstration, we use gray-level images to evaluate our scheme. But it is intuitively easy to extend our scheme for full-color images by just applying the operations we introduce in the last two sections on all of the color channels. We show as an example the effect of our secret sharing scheme for the (2,3)-threshold case here by some experimental results.

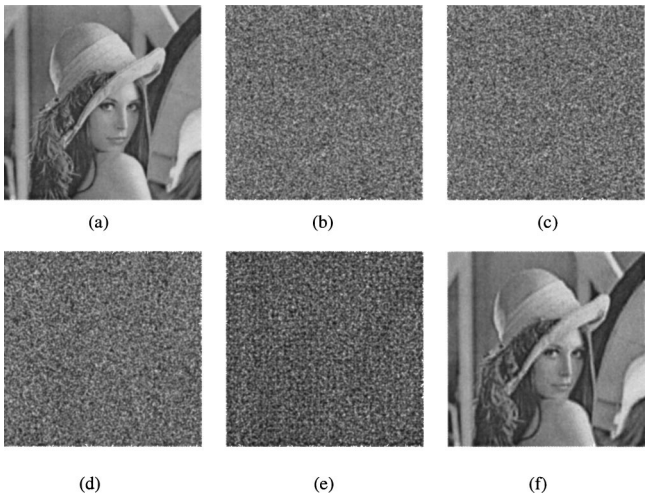

Fig. 1 Experimental result: (a) the secret image, (b) the secret share set of participant 1, (c) the secret share set of participant 2, (d) the secret share set of participant 3, (e) the image recovered by data combining a guess of the first coefficient and the randomized 2nd through 10th coefficients of each block, and (f) the image recovered by data combining a correct recovery of the first 10 coefficients of each block.

We first take an image, as shown in Fig. 1(a), as the secret image. After we performed the DCT for each block, we reserved only the first 10 coefficients. Next, we randomized the values of the 2nd through the 10th coefficients of each image block and made them public. After that, we created shares from the first coefficient of each block image using the Shamir method. Combining the share of each block, we acquired the secret share sets. We express the three secret share sets in the form of images in Figs. 1(b) through 1(d), which look meaningless. Without obtaining enough secret share sets to recover the protected first DCT coefficients, invaders can just guess the values of the first DCT coefficients and then combine the randomized 2nd through 10th coefficients to recover the original image. The result of such an attempt is shown in Fig. 1(e). We can observe from the figure that most information of the original secret image is lost. On the contrary, with enough share sets collected to recover the correct first DCT coefficient of each image block, the 2nd through 10th coefficients were decrypted correctly, and the recovered image is shown in Fig. 1(f). Next, we inspect the sharing effect resulting from performing the additional quantization operation. An experimental example is shown in Fig. 2, in which Figs. 2(a) through 2(f) are all similar to the corresponding ones in Fig. 1. From these results, we can see that the quantization step does not cause visually perceptible changes in the resulting images.

5 Security Analysis

In this section, we analyze the effectiveness of our proposed scheme for security protection. From Eq. (4), we know that the first coefficient value C_1 can be recon-

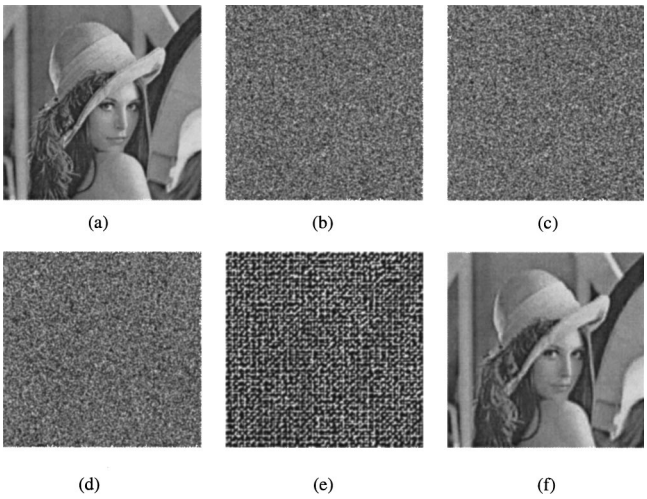

Fig. 2 Another experimental result achieved by performing the additional quantization step: (a) the secret image, (b) the secret share set of participant 1, (c) the secret share set of participant 2, (d) the secret share set of participant 3, (e) the image recovered by data combining a guess of the first coefficient and the randomized second through tenth coefficients of each block, and (f) the image recovered by data combining a correct recovery of the first 10 coefficients of each block.

structed only if k or more shares can be collected. Without getting enough shares, the possibility of guessing the right value of C_1 for a certain image block is only $1/p$, where p is the prime number used in the modular arithmetic involved in the Shamir scheme described by Eq. (2) previously. The reason is that we choose p to be the nearest prime number larger than C_1, that is, C_1 falls in the range of $[0,p)$. Furthermore, in our decryption process, only the right C_1 can be used to deduce the other coefficients correctly. Therefore, the possibility of correct secret image recovery by guessing is $(1/p)^{b\times b}$, assuming that each image has $b\times b$ blocks. Note here that the choice of the value of p is a trade-off between the size of required storage and the degree of security. A larger p requires more storage space for the shares because the magnitudes of the share data will become larger. On the other hand, a larger p will reduce the possibility of correct secret image recovery by guessing according to the preceding probability of correct guesses.

6 Conclusions

A new scheme for secret image sharing based on the Shamir method[9] with the additional capability of share data reduction was proposed. The scheme can be employed to avoid the usual case that a set of secret images is held by only one person without extra copies, and thus prevent the secret data from being lost incidentally or modified intentionally. The proposed scheme provides high security to encrypt a given secret image into shares, which are noisy and leak no information about the secret image. In addition, the capability of share data reduction drastically extends the applicability of the proposed method. The amount of the created share data, which must saved or delivered, is smaller than that of the original secret image. This merit is especially advantageous to applications of portable devices with limited communication channel capacities and storage spaces. The proposed scheme can handle full-color images, and the quality of the recovery result is satisfactory. It is thus suitable for applications where high security and efficiency are required. Finally, although our proposed scheme is based on the use of the coefficients of DCT-based image compression for ease of demonstration, it is easy to extend our scheme to meet the requirements of other compression standards, such as JPEG, MPEG, and the wavelet transform, each of which yields certain types of transform coefficients for use in our scheme.

Acknowledgment

This work was supported by the MOE Program for Promoting Academic Excellence of Universities under the Grant No. 89-1-FA04-1-4.

References

1. ''Data Encryption Standard (DES),'' National Bureau of Standards FIPS Publication 46 (1977).
2. M. Matsui, ''Linear cryptanalysis method for DES cipher,'' in *Advances in Cryptology—EUROCRYPT'93*, Vol. 765 of Lecture Notes in Computer Science, pp. 386–397 (1994).
3. R. L. Rivest, A. Shamir, and L. Adleman, ''A method for obtaining digital signatures and public key cryptosystems,'' *Commun. Assoc. Comput. Mach.* **21**, 120–126 (1978).
4. A. Salomaa, *Public Key Cryptography*, Springer-Verlag (1990).
5. W. Bender, D. Gruhl, N. Morimoto, and A. Lu, ''Techniques for data hiding,'' *IBM Syst. J.* **35**(3–4), 313–336 (1996).
6. D. C. Wu and W. H. Tsai, ''Data hiding in images via multiple-based number conversion and lossy compression,'' *IEEE Trans. Consum. Electron.* **44**(4), 1406–1412 (1998).
7. E. Adelson, ''Digital signal encoding and decoding apparatus,'' U.S. Patent, No. 4,939,515 (1990).
8. D. C. Wu and W. H. Tsai, ''Embedding of any type of data in images based on a human visual model and multiple-based number conversion,'' *Pattern Recogn. Lett.* **20**, 1511–1517 (1999).
9. A. Shamir, ''How to share a secret,'' *Commun. Assoc. Comput. Mach.* **22**(11), 612–613 (1979).
10. D. R. Stinson, ''An explication of secret sharing schemes,'' *Design. Codes Cryptograph.* **2**, 357–390 (1992).
11. H. M. Sun and S. P. Shieh, ''Construction of dynamic threshold schemes,'' *Electron. Lett.* **30**(24), 2023–2024 (1994).
12. C. C. Chang and H. C. Lee, ''A new generalized group-oriented cryptoscheme without trusted centers,'' *IEEE J. Sel. Areas Commun.* **11**(5), 725–729 (1993).
13. M. Naor and A. Shamir, ''Visual cryptography,'' in *Advances in Cryptology—EUROCRYPT'94*, Vol. 950 of Lecture Notes in Computer Science, pp. 1–12 (1995).
14. E. R. Verheul and H. C. A. van Tilborg, ''Construction and properties of k out of n visual secret sharing schemes,'' *Design. Code Cryptograph.* **11**, 179–196 (1997).

Chang-Chang Lin received his BS degree from the Department of Computer Science, National Tsing Hua University, in 1996. Since August 1996 he has been a research assistant with the Computer Vision Laboratory of the Department of Computer and Information Science, National Chiao Tung University, where he is currently working toward his PhD degree. His recent research interests include visual secret sharing, pattern recognition, watermarking, and image hiding.

Wen-Hsiang Tsai received his BS degree in electrical engineering from National Taiwan University, Taipei, in 1973, his MS degree in electrical engineering (with major in computer science) from Brown University, Providence, Rhode Island, in 1977, and his PhD degree in electrical engineering (with major in computer engineering) from Purdue University, West Lafayette, Indiana, in 1979. In 1979 Dr. Tsai joined the faculty of National Chiao Tung University, Hsinchu, Taiwan, where he is currently a professor in the Department of Computer and Information Science and the vice president of the university. Professor Tsai has been an associate professor with the Department of Computer Engineering (now the Department of Computer Science and Information Engineering) and the acting director of the Institute of Computer Engineering. In 1984, he joined the Department of Computer and Information Science and headed the department from 1984 through 1988. He was also the associate

director of the Microelectronics and Information System Research Center from 1984 through 1987, the dean of general affairs from 1995 to 1996, and the dean of academic affairs of from 1999 to 2001. He has chaired the Chinese Image Processing and Pattern Recognition Society at Taiwan from 1999 to 2000. Professor Tsai has served as a Consultant to several major research institutions in Taiwan, has been coordinator of computer science with the National Science Council and a member of the Counselor Committee of the Institute of Information Science of Academia Sinica in Taipei. He has been the editor of several academic journals and was the editor-in-chief of *Journal of Information Science and Engineering* from 1998 to 2000. His research interests include image processing, pattern recognition, computer vision, virtual reality, and information copyright and security protection. He has published 107 journal papers and 150 conference papers and holds granted 6 Taiwanese or U.S. patents. Dr. Tsai is a senior member of the IEEE and a member of the Chinese Image Processing and Pattern Recognition Society, the Medical Engineering Society of the Republic of China, and the International Chinese Computer Society.