A WATERMARKING TECHNIQUE BASED ON ONE-WAY HASH FUNCTIONS

Min-Shiang Hwang[1,0], Chin-Chen Chang, *IEEE Fellow*[2], and Kuo-Feng Hwang[1]

Department of Information Management[1]
Chaoyang University of Technology
Wufeng, Taiwan, R.O.C.
Email: mshwang@mail.cyut.edu.tw

Department of Computer Science and Information Engineering[2]
National Chung Cheng University
Chaiyi, Taiwan, R.O.C.
Email: ccc@cs.ccu.edu.tw

Abstract

Digital watermarking techniques have been proposed for the copyright protection of digital images recently. A digital watermarking technique is a technique for embedding invisible watermarks in a digital image. The watermarks must be designed to be unrecognizable by unauthorized people and to be identified by the legal copyright owner of the image. In this paper, we proposed a new copyright watermarking scheme. Our scheme is based on one-way hash functions, which are widely used in cryptosystems. The main goal of our method is to design a secure watermarking scheme.

KeyWords: Digital Watermarks, Intellectual Property, Copyright, Cryptography.

1 INTRODUCTION

Since computer networks allow rapid and convenient communication, they have become the principal media for the distribution of information. Today many applications and services are provided via computer networks. Many commercial vendors and developers have used the internet to deliver media products or transactions for profit. Services such as video on demand, electronic data exchange and online shopping, etc. However, there are two main problems when providing these services via computer networks. One is that these services are vulnerable to relatively easy access [23] by illegal users. Without appropriate protection, these services are susceptible to unauthorized access [2]. Many schemes based on cryptographic techniques have been proposed for solving this problem [9, 14].

The other problem is that these services are easy to duplicate or redistribute. Without appropriate validation, these services are susceptible to unauthorized use [4]. Copyright protection and validation for authorized use of online services are very important research topics [4, 5, 6]. Since images are easily reproduced by an authorized user from previously secured services, the use of cryptosystems does not completely solve this problem. The idea of using an indelible digital watermark to solve this problem has stimulated much interest in the electronic publishing and printing industries [21].

Digital watermarking techniques have been proposed for copyright protection of digital images recently. A digital watermarking technique is a technique that embeds an invisible watermarks into a digital image. The watermarks must be designed to be unrecognizable by unauthorized people and easily identified by the legal copyright owner of the image. In this paper, we proposed a new copyright watermarking scheme. Our scheme is based on one-way hashing functions, which are widely used in cryptosystems. The main goal of our method is to design a secure watermarking system.

In order to develop a practical digital watermarking scheme. The digital watermarking technique should satisfy the following requirements.

1. The difference between the original image and the embedded watermarking image should be

[0]Responsible for correspondence.

Contributed Paper

Manuscript received January 28, 1999

perceptually invisible.

2. The watermark must be undetectable by an unauthorized user.

3. The detection of the watermark should not be correlated with the original image.

4. The watermark should utilize robust image processing which preserves the desired quality of the image.

5. As in information security techniques, the details of the digital watermark algorithms must be publishable to every one. The owner of the intellectual property image is the only one who holds the private secret key.

Many watermarking techniques have been proposed for the copyright protection of digital images [6, 11, 12, 17, 19, 24, 26]. These techniques are classified in two main principles involved in designing a digital watermark. The first principle is that the watermark be embedded in the frequency domain [17, 19, 24, 26]. A small subset of the frequency spectrum of a particular block is modified. The watermark is embedded in the least significant DCT coefficients [25]. The second principle is that the watermark be embedded in the spatial domain [6, 11, 12, 17]. A pseudo-unrandom set of pixels is selected and the least significant bits of their intensity levels are modified. This method is faster and more reliable than the frequency domain method [18].

Both the principles of embedding watermarks in the frequency and spatial domains, are not immune to significant information attacks. An unauthorized user can simply remove the embedded watermark from the image by confusing the least significant information. Since the least significant information does not affect the quality of the original image, an unauthorized user can freely use the image. In this paper, we propose a new watermark scheme, which is based on one-way hash functions. Our scheme is immune to this attack.

The rest of this paper is organized as follows. Section 2 introduces a one-way hash function, which is applied to our scheme for embedding the watermark in the original image. We propose a new watermarking scheme in Section 3. The security analyses and empirical tests of the proposed watermarking technique are presented and discussed in Sections 4 and 5. Finally, Section 6 concludes this paper.

2 A ONE-WAY HASH FUNCTION AND RABIN'S SCHEME

Since our scheme is based on one-way hash functions, we will describe the concept of one-way hash functions in this section. This is a family of functions $f : x \rightarrow y$ with the following properties [13, 15]:

1. The functions f's are easily computed, and randomly picking a member of the function, f, is also relatively simple.

2. The functions are computationally difficult to invert. In the other words, it is computationally infeasible, given a string x, to compute another string $x \neq x'$, that satisfies $f(x) = f(x')$ for a randomly chosen f.

3. The functions can be applied to any argument of any size.

4. The functions produce a fixed size output.

During the last decade, the one-way hash function has been used in many cryptographic applications. For instance, they have found applications for safeguarding cryptographic keys [8], access control in a hierarchy [1, 22], key management in a group-oriented scheme [7], for user authentication scheme [3], and other functions [10].

Merkle [13] showed that a good cryptosystem can be used to implement a one-way hash function. A conventional approach involves encrypting a fixed constant, c, using x as the key, i.e., $f(x) = E_x(c)$. A commercial product, DES [16], is the best known and most widely used encryption function. Generating one-way functions is secure if DES is random [13]. Public key cryptographic systems (i.e., the RSA scheme) are also based on one-way functions.

In this paper, we apply Rabin's scheme [20] and a simple modulo operation as an example of one-way hash functions. The security of Rabin's scheme is based on the difficulty in finding a composite square roots modulo. The difficulty is equivalent to factoring. We briefly introduce Rabin's scheme as follows.

To encrypt a message M:
Simply compute $C = M^2 \bmod n$, where $n = pq$, both p and q are primes and congruent to 3 mod 4.

To decrypt a message M:
By the Chinese remainder theorem, we can obtain

$$M_1 = C^{(p+1)/4} \bmod n, \quad (1)$$

$$M_2 = p - C^{(p+1)/4} \bmod n, \quad (2)$$

$$M_3 = C^{(q+1)/4} \bmod n, \quad (3)$$

$$M_4 = q - C^{(q+1)/4} \bmod n. \quad (4)$$

Among M_1, M_2, M_3, and M_4, one of them equals to the message M.

In our scheme, we calculate a position for an original image using Rabin's scheme and a modulo operation. We insert the bit of a watermark to the position of the image. Since the positions are random numbers, an illegal user is difficult to derive the watermark and it's embedded positions.

3 OUR SCHEME

In this section, we propose a new copyright watermarking scheme. The scheme is based on one-way hash functions, which are widely used in cryptosystems. The main goal of our method is to design a high security watermarking system. Generally speaking, a digital image can be expressed as a matrix of size $m_x \times m_y \times m_z$. Here, $m_x \times m_y$ is the size of an image while m_z is the size of a pixel in gray level or in the three intensity levels of red, green, or blue color.

The new watermarking scheme consists of the following two basic phases: embedding the watermark and deriving the watermark. In the embedding watermark phase, we first calculate a position for the image using one-way hash functions. Next, we insert the bit of a watermark to the position of the image in sequence. Similarly, in the deriving watermark phase, we also calculate the position of an image by using the way that in the embedding watermark phase uses. Next the bit in the position of the image is retrieved.

We assume that the owner of the original image has a private key K with 512 bits in length. Let ID_i denote the identification of the original image. The detailed procedures of our watermarking scheme in the embedding watermark phase are given as follows.

1. Randomly choose two large prime numbers p and q and compute the parameter $n = p \cdot q$, where p and q are kept secret and n is public. The size of p and q is 256 bits in length.
2. Obtain three secret seeds X, Y, and Z using the following encipher process.

$$X = ID_i^K \bmod n, \quad (5)$$

$$Y = ID_i^{(K^2)} \bmod n, \quad (6)$$

$$Z = ID_i^{(K^4)} \bmod n, \quad (7)$$

   where the size of X, Y, and Z are 512 bits in length.
3. Calculate a position (L_x, L_y, L_z) using the following:

$$L_x = X^2 \bmod n, \quad (8)$$

$$L_y = Y^2 \bmod n, \quad (9)$$

$$L_z = Z^2 \bmod n. \quad (10)$$

   where the size of n, L_x, L_y, and L_z are 512 bits in length.
4. Calculate an embedding position (x, y, z) using the following:

$$x = L_x \bmod m_x, \quad (11)$$

$$y = L_y \bmod m_y, \quad (12)$$

$$z = L_z \bmod m_z, \quad (13)$$

   where $m_x \times m_y$ is the size of the original image; and m_z is the size of a pixel in gray level or in the three intensity levels of red, green, or blue color.
5. Embed a bit of the watermark in the position (x, y, z).
6. Calculate the next position (L_x, L_y, L_z) using the following:

$$L_x = L_x^2 \bmod n, \quad (14)$$

$$L_y = L_y^2 \bmod n, \quad (15)$$

$$L_z = L_z^2 \bmod n. \quad (16)$$

7. Repeat steps 4, 5, 6, until all bits of the watermark have been embedded in the original image.

The retrieving procedures are notably symmetrical to that of the above embedding watermark procedures.

1. Calculate a set of secret seeds X, Y, Z using Equation (5).
2. Calculate a position (L_x, L_y, L_z) by Equation (8).
3. Calculate an embedding position (x, y, z) using Equation (11).
4. Retrieve a bit of the watermark from the position (x, y, z).
5. Calculate the next position (L_x, L_y, L_z) using Equation (14).
6. Repeat Steps 3, 4, and 5, until all bits of the watermark have been retrieved.

There are two problems in the above procedures. The first is that the position (L_x, L_y, L_z) may be chosen repeatedly, i.e., a hashing collision. In this case, the different bits of the watermark will be embedded in the same position. In other words, the previously embedded bits of watermark may be covered by subsequent embedded bits of watermark. Therefore, some bits of the watermark may be lost. We call this is a collision problem.

The second problem is that the position may be chosen in the high bit (the significant bit) of a pixel. In this case, the embedded watermark image could be significantly cloudy. We call this is a resolution problem. We give the solution for these two problems in the following.

To solve the collision problem:
We use a transient table to record all positions calculated by Equation (11). After a position is calculated using Equation (11) in Step 4, the position is checked

with the all positions recorded in the transient table. If the new position exists in the transient table, the process then skips Step 5 in the embedding watermark phase. Otherwise, it records the position in the transient table. This approach will remove the collision problem. The transient table is not stored in a file. It is created during the embedding watermark and the retrieving watermark phase.

To solve the resolution problem:
The most significant bit and the least significant bit are not used in embedded positions for resolution in our scheme. When (x, y, z) is obtained in Step 4 of the embedding watermark phase, we check z's value. If $z = 0$ or $z = 7$, the process then skips Step 5 in the embedding watermark phase. Otherwise, we compare each bit of watermark and the z's bit of the pixel in (x, y) of the original image. If the two bits are the same, nothing more is required. Others, change the z's bit of the pixel in (x, y) of the original image to the bit of the watermark and change the other bits of the pixel such that the difference between the two pixels is minimal. Note that the other bits must not be previously embedded bits of watermark embedded in the above procedure. In this case, we must keep that bit. For example, assume that a pixel is $(p_0p_1p_2p_3p_4p_5p_6p_7)$. p_0 is the most significant bit, and p_7 is the least significant bit. Assume that z is 2, and p_5 is a previously embedded bit of the watermark, which was embedded in the above procedure. We choose an appropriate (u_1, u_3, u_4, u_6) such that the difference between $(p_0p_1p_2p_3p_4p_5p_6p_7)$ and $(p_0u_1w_2u_3u_4p_5u_6p_7)$ is minimal, where w_2 is the bit of watermark to be embedded. After finding (u_1, u_3, u_4, u_6), we use $(p_0u_1w_2u_3u_4p_5u_6p_7)$ instead of $(p_0p_1p_2p_3p_4p_5p_6p_7)$ in the pixel of the original image. This approach minimizes the cloudiness in the embedded watermark image.

4 SECURITY ANALYSES

To prove the feasibility of our watermarking scheme, we analyzed the degree of security provided in this section. We analyzed the security of our watermarking scheme using the following three cases: position attack, the less significance bits attack, and multiple images attack.

Under the position attack, illegal users are assumed to have obtained the embedded watermark image and the one-way hash function, but do not have the private key K of the owner of the original image. Generally, there are two ways for this information to be taken. One is to directly cryptanalysis the one-way hash function. In other words, if $y = f(x)$ is the one-way hash function used in our scheme. The illegal users must find the inverse function $f^{-1}(\cdot)$ such that $x = f^{-1}(y)$. This function is difficult to find as stated in Section 2. In this paper, we use Rabin's scheme and a simple modulo operation as a one-way hash function. Therefore, the illegal users who want to derive the position of the embedded watermark, must break Rabin's scheme. The security of Rabin's scheme is based on the difficulty of finding the composite square roots modulo. The difficulty is equivalent to factoring. Therefore, the illegal users cannot derive the position of the embedded watermark.

The other method is to directly cryptanalysis the private key K. In this case, the illegal users need to guess the private key K using brute force correctly. Since a private key has 512 bits in our scheme, K has 2^{512} possible combinations. If the illegal users employ a 100 MIPS computer to compute K, the computational load is then $\frac{2^{512}}{100\times10^6\times60\times60\times24\times365} > 10^{140}$ years. This is a very long time. No image can be closed-door after 10^{140} years.

Under the least significant bits attack, the illegal users destroy the least significance bits of the original image without affecting the quality of the image. An unauthorized user can simply remove the embedded watermark from the image by confusing the least significant information. Since the least significant information does not affect the quality of the original image, an unauthorized user can freely use the image. Since the watermark is not always embedded in the least significance bits of the original image in our scheme, destroying the least significance bits of the original image will not destroy the watermark. Our scheme is thus immune to this attack.

Under a multiple images attack, the illegal users are assumed to have obtained many embedded watermark images . If these images are of the same size and use the same private key K, the scheme is not secure. The illegal users can derive the watermark and it's embedded position using the AND logical operation on these images. The watermark must appear in the logical "1" bits. Since the secret seeds are different in all images, the positions of the embedded watermarks are different. Therefore, our scheme is immune from the multiple images attack.

5 EMPIRICAL TESTS

In our experiments, our original image was monochrome, in which each pixel had 256 gray levels. Since 256 equals 2^8, we needed 8 bits to express each pixel. Thus n_z was 8. The watermark was a two level image with a size of 64×64. All of our experiments were performed on an IBM PC using a Pentium 133 CPU.

In our watermarking scheme, there were a few distortions between the original image I_o and the embedded watermark image I_w. To evaluate the quality of the embedded watermark image I_o, we defined the

peak signal-to-noise ratio (PSNR) as follows.

$$PSNR = 10 \log_{10} \frac{255^2}{MSE}(dB). \quad (17)$$

For an $m \times m$ image, the mean-square error (MSE) is defined as follows.

$$MSE = \frac{1}{m^2} \sum_{i=1}^{m} \sum_{j=1}^{m} (\alpha_{[i,j]} - \beta_{[i,j]}), \quad (18)$$

where $\alpha_{[i,j]}$ and $\beta_{[i,j]}$ denote the component values of the pixel [i, j] in the original and the embedded watermark images, respectively. The larger PSNR is, the better the image quality will be. In general, an embedded watermark image is acceptable by human perception if its PSNR is greater than 30 dB.

Figure 1 is our original image in which there is an airplane flying in the sky. Its image size was 512 × 512. To embed a watermark on the original image, we employed a watermark image with a size of 64 × 64. It is shown in Figure 2. The watermark contains a Chinese signature, "ChaoYang University".

Figure 3 is an embedded watermark image in which the watermark in Figure 2 is embedded in the original image in Figure 1. The experimental results showed that the PSNR of this image is 55.56, which is much larger than our acceptable criterion 30 dB.

Figure 4 is another original image in which there is a sweet girl named "Lena". Its image size was 512×512. Figure 5 is an embedded watermark image in which the watermark in Figure 2 is embedded in the original image in Figure 4. The experimental results showed that the PSNR of this image is 55.28. This result is also much larger than our acceptable criterion 30 dB.

From the above experimental results, the embedded watermark image is preserved at the desired quality of the original image.

Figure 6 is an image which the least 3 significant bits of all pixels of the embedded image in Figure 5 are destroyed by an illegal user. The experimental results showed that the PSNR of this image is 36.02. Figure 7 is a watermark which is retrieved from Figure 6.

Figure 8 is an another image which the least 4 significant bits of all pixels of the embedded image in Figure 3 are destroyed by an illegal user. The experimental results showed that the PSNR of this image is 30.73. Figure 9 is a watermark which is retrieved from Figure 8. From the above experimental results, destroying the least significant bits of the embedded image will not destroy the watermark. Our scheme is thus immune to the least significant bits attak.

6 CONCLUSIONS

We have proposed a digital watermarking scheme for copyright protection of digital images. We provided two empirical tests in Section 5. In those tests, we demonstrated that the PSNR of the embedded watermark image was 55.56 and 55.28, respectively. Therefore, the difference between the original image and the embedded watermark image is perceptually invisible in our scheme. Further, the proposed scheme satisfies the requirements stated in Section 1. The characteristics of our scheme can be described as follows.

1. The embedded position of the watermark in our scheme is pseudo-random number using Rabin's scheme and a modulo operation. It is very difficult for an unauthorized user to detect the position. It is equally difficult to break the factoring.

2. The detection of the watermark is performed using a private key K. We need not to store the original image for detecting the watermark.

3. The watermark is embedded in any position of a pixel, but not in the least significant bits in our scheme. Therefore, the embedded watermark is a more robust image process, which preserves the desired image quality better than that of any other scheme.

4. Our scheme is based on one-way hash functions, which are widely used in cryptosystems. The details of digital watermark algorithms can be published to every one. The intellectual property owner of the image is the only one who holds the private secret key.

ACKNOWLEDGEMENTS

Part of this research was supported by the National Science Council, Taiwan, R.O.C., under contract no. NSC88-2213-E-324-001.

References

[1] S. G. Akl and P. D. Taylor, "Cryptographic solution to a problem of access control in a hierarchy," *ACM Transactions on Computer Systems*, vol. 1, no. 3, pp. 239–248, July 1983.

[2] J. B. Borka, "Security in value added networks - security requirements for EDI," *Computer Standard & Interfaces*, vol. 12, pp. 23–33, 1991.

[3] C. C. Chang and T. C. Wu, "Remote password authentication with smart cards," *IEE Proceedings-E*, vol. 138, no. 3, pp. 165–168, May 1991.

[4] I.J. Cox, J. Kilian, F.T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Transactions*

Figure 1. Original image of airplane

Figure 3. Watermarked image of airplane(PSNR=55.56)

Figure 2. Watermark of "ChaoYang University"

Figure 4. Original image of "Lena"

Figure 5. Watermarked image of "Lena"(PSNR=55.28)

Figure 6. Destroyed the least 3 significant bits image from Figure 5.(PSNR=36.02)

Figure 7. Retrieved watermark from Figure 6.

Figure 8. Destroyed the least 4 significant bits image from Figure 5.(PSNR=30.73)

Figure 9. Retrieved watermark from Figure 8.

on Image Processing, vol. 6, no. 12, pp. 1673–1687, Dec. 1997.

[5] I. J. Cox and Jean-Paul M.G. Linnartz, "Some general methods for tampering with watermarks," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, pp. 587–593, 1998.

[6] S. Craver, N. Memon, B. L. Yeo, and M. M. Yeung, "Resolving rightful ownerships with invisible watermarking techniques: Limitations, attacks, and implications," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, pp. 573–586, 1998.

[7] D. E.R. Denning, H. Meijer, and F. B. Schneider, "More on master keys for group sharing," *Information Processing Letters*, vol. 13, no. 3, pp. 125–126, 1981.

[8] E. Gudes, "The design of a cryptography based secure file system," *IEEE Transactions on Software Engineering*, vol. SE-6, no. 5, pp. 411–420, 1980.

[9] R. Housley, "Electronic messaging security: A comparison of three approaches," in *Proceedings of the Fifth Annual Computer Security Applications Conference*, 1990, pp. 29.

[10] I. Ingemarsson, D. T. Tang, and C. K. Wong, "A conference key distribution system," *IEEE Transactions on Information Theory*, vol. IT-28, no. 5, pp. 714–720, Sep. 1982.

[11] M. Kutter, F. Jordan, and F. Bossen, "Digital watermarking of color images using amplitude modulation," *Journal of Electronic Imaging*, vol. 7, no. 2, pp. 326–332, 1998.

[12] 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.

[13] R. C. Merkle, "One-way hash functions and DES," in *Advances in Cryptology, CRYPTO'89*, Lecture Notes in Computer Science, vol. 435, 1989, pp. 428–446.

[14] C. J. Mitchell, "Authenticating multicast internet electronic mail messages using a bidirectional MAC is insecure," *IEEE Transactions on Computers*, vol. 41, no. 4, pp. 505–507, 1992.

[15] M. Naor and M. Yung, "Universal one-way hash functions and their cryptographic applications," in *Proc. of the 21st STOC*, 1989, pp. 33–43.

[16] National Bureau of Standard, *Data Encryption Standard*. FIPS, NBS, 1977.

[17] R. Ohbuchi, H. Masuda, and M. Aono, "Watermarking three-dimensional polygoal models through geometric and topological modifications," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, pp. 551–560, 1998.

[18] I. Pitas and T. H. Kaskalis, "Applying signatures on digital images," in *IEEE International Conference on Nonlinear Image and Signal Processing*, 1995, pp. 460–463.

[19] C. I. Podilchuk and W. Zeng, "Image-adaptive watermarking using visual models," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, pp. 525–539, 1998.

[20] M. O. Rabin, "Digitalized signatures and public-key functions as intractable as factorization," Technical Report MIT/LCS/TR-212, Laboratory for Computer Science, Massachusetts Institute of Technology, Cambridge, Mass., Jan. 1979.

[21] J.J.K. O Ruanaidh, W.J. Dowling, and F.M. Boland, "Watermarking digital images for copyright protection," *IEE Proceedings on Visual Image Signal Process*, vol. 143, no. 4, pp. 250–256, 1996.

[22] R. S. Sandhu, "Cryptographic implementation of a tree hierarchy for access control," *Information Processing Letters*, vol. 27, pp. 95–98, 1988.

[23] B. Schneier, *Applied Cryptography*, John Wiley & Sons, New York, 1994.

[24] M. D. Swanson, B. Zhu, and A. H. Tewfik, "Multiresolution scene-based video watermarking using perceptual models," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, pp. 540–550, 1998.

[25] G. K. Wallace, "The JPEG still picture compression standard," *Communications of the ACM*, vol. 34, no. 4, pp. 31–44, 1991.

[26] K. K. Wong, C. H. Tse, K. S. Ng, T. H. Lee, and L. M. Cheng, "Adaptive water marking," *IEEE Transactions on Consumer Electronics*, vol. 43, no. 4, pp. 1003–1009, 1997.

Min-Shiang Hwang received the B.S. in Electronic Engineering from National Taipei Institute of Technology, Taipei, Taiwan, Republic of China, in 1980; the M.S. in Industrial Engineering from National Tsing Hua University, Taiwan, in 1988; and the Ph.D. in Computer and Information Science from National Chiao Tung University, Taiwan,

in 1995. He also studied Applied Mathematics at National Cheng Kung University, Taiwan, from 1984-1986. Dr. Hwang passed the National Higher Examination in field "Electronic Engineer" in 1988. He also passed the National Telecommunication Special Examination in field "Information Engineering", qualified as advanced technician the first class in 1990. From 1988 to 1991, he was the leader of the Computer Center at Telecommunication Laboratories (TL), Ministry of Transportation and Communications, ROC. He was also a project leader for research in computer security at TL in July 1990. He is currently an Associate Professor in Department of Information Management, Chaoyang University of Technology, Taiwan, ROC. He is a member of IEEE, ACM, and Chinese Information Security Association. Dr. Hwang's current research interests include database and data security, cryptography, image compression, and mobile communications.

Chin-Chen Chang was born in Taichung, Taiwan, Republic of China, on November 12, 1954. He received his B.S. degree in applied mathematics in 1977 and his M.S. degree in computer and decision sciences in 1979 from the National Tsing Hua University, Hsinchu, Taiwan. He received his Ph.D. in Computer engineering in 1982 from National Chiao Tung University, Hsinchu, Taiwan. During the academic years 1980-83, he was on the faculty at the Department of Computer Engineering at National Chiao Tung University. From 1983-1989, he was on the faulty at the Institute of Applied Mathematics, National Chung Hsing University, Taichung, Taiwan. From August 1989 to July 1992, he was the head and professor of the Institute of Computer Science and Information Engineering at National Chung Cheng University, Chiayi, Taiwan. From August 1992 to July 1995, he was the dean of the College of Engineering at the same university. Since August 1995, he has been the dean of Academic Affairs at National Chung Cheng University. In addition, he was served as a consultant to several research institutes and government departments. His current research interests include database design, computer cryptography, coding theory, and data structures. Dr. Chang is the associate editor of Computer Quarterly, Journal of Computers, Journal of the Chinese Institute of Engineers, Journal of Electrical Engineering, International Journal on Policy and Information, Journal of Information and Management Science, Journal of Information Science and Engineering, and is the regional editor of Information Sciences Applications and Editor-in-Chief of Journal of Information and Education. He was elected as an outstanding youth of the Republic of China in 1984. In the same year, he was also elected as an Outstanding Talent in Information Science of the Republic of China. He obtained the 1986-1987, 1988-1989, 1990-1991, 1992-1994, 1995-1996 Distinguished Research Awards of the National Science Council of the Republic of China. He also obtained from the Chung-Shan Academic Foundation of the Republic of China the 1987 Chung-Shan Academic Publication Award. He was the winner of the 1990, 1991, and 1992 AceR Long Term Award for Outstanding M.S. Thesis Supervision, the 1991 AceR Long Term Award for Outstanding Ph.D. Dissertation Study Supervision. He was the winner of the Best Paper Award at the Second International Conference on CISNA sponsored by the British Council. He was also the winner of the 1992 Outstanding Teaching Materials Award of the Ministry of Education of the Republic of China. Dr. Chang has published more than one hundred papers in well-known journals and ten books in the fields of Databases Design, Data Structures, Information Security and Cryptography in Chinese. Dr. Chang is a senior member of the IEEE, and a member of the Chinese Language Computer Society, the Chinese Institute of Engineers of the Republic of China, the International Association for Cryptologic Research, the Computer Society of the Republic of China, and the Phi Tau Phi Society of the Republic of China and he is also the Chairman of the Executive Committee in the Information Security Society of the Republic of China.

Kuo-Feng Hwang received the B.S. in Construction Engineering from National Lien-Ho College of Technology and Commerce, Taiwan, Republic of China, in 1991. He is currently pursuing his master degree in Information Management at Chaoyang University of Technology. His research interests include cryptography, image Processing, and Information Management.