Efficient Searching Strategy for Secret Image Sharing with Meaningful Shadows

Chin-Chen Chang, Ngoc-Tu Huynh, and Ting-Feng Chung

***Abstract*—In this paper, we propose a new visual secret sharing scheme which is suitable for grayscale images. The proposed scheme achieves the following objectives. First, it satisfies four general criteria of visual secret sharing systems: security, accuracy, small shadow size and low computation cost. Second, the scheme can successfully reconstruct the secret image exactly. Finally, the decoding cost of our proposed scheme is much less than that required by other previously proposed schemes. Therefore, our proposed scheme is suitable for real-time applications.**

***Index Terms*—Secret sharing, Sudoku, meaningful, searching.**

I. Introduction

Secret sharing has been attracted attention in the past decades. Different from conventional protecting data mechanisms such as data encryptions, data hiding, etc., secret sharing shares data into several parts which are kept by a group of participants to avoid losing data accidently or intentionally. The concept of secret sharing, or called visual cryptography, was proposed independently by Shamir and Blakley in 1979 [1], [2]. Inspired by Shamir's [1] and Blakley's [2] (*t*, *n*) threshold schemes, many scholars began focusing on the study of secret sharing. However, the major drawback with these schemes is that their secret data are integers or texts instead of images. In 1995, Naor and Shamir [3] extended it to secret image sharing to apply to images. In [3], dealer shares secret image into n noise-like images and distributed to *n* predefined participants. Each noise-like image does not contain any information of the original secret image and is considered to be a shadow or share. The secret image can be reconstructed if any *t* or more shadows are collected. If the number of collected shadows is less than *t*, information about the secret image cannot be derived. This is considered as an efficient way to share a secret. Unfortunately, the scheme is only suitable for binary image and also suffers from a pixel expansion problem.

Many VSS schemes have been proposed in the past decades. Originally, there are two ways to construct shares: constructing by using polynomial function [4]-[6] and constructing by random grids [7]-[9]. In 2008, Chang *et al.* [11] first proposed a Sudoku-table-based (STB) scheme for data hiding approach, in which the reference table is generated by a Sudoku table. In this scheme, a digit in the 9-ary notational system is embedded into a pixel pair. The usage of the Sudoku table simplifies the reference table that has to be pre-shared by the communication entities. Kieu *et al.* [12] took this idea a little further when they proposed a Sudoku-table-based wet paper (STB-WP) hiding scheme that has even higher security than the original model. Hong et al. [13] found that the original STB scheme does not always find the minimal distortion for the pixel pairs, therefore, they proposed a minimal Euclidean distance and Sudoku-table-based (MED-STB) scheme, which extends the searching area in the reference table and finds the minimal distortion by comparing the Euclidean distances of all the candidates.

There are four general criteria which are observed to evaluate secret sharing techniques such as security, accuracy, computational complexity, and shadow size, also called pixel expansion. In this paper, we aim to propose a secret image sharing scheme, which can satisfy these criteria with high security, low computational complexity and prevent pixel expansion problem. Especially, to reconstruct the cover image during revealing the original secret image, we will exploit Sudoku puzzle to share secret image. Sudoku is a logic-based number placement puzzle [11], [14]-[16]. Sudoku is a 9×9 matrix which contains nine 3×3 sub-blocks, each contains different digits from 1 to 9. In addition, each row and each column of a Sudoku grid also contain different digits from 1 to 9. In general, the Sudoku puzzle which is exploited in our scheme is computed as a modification to the host image. Shadows are generated by encoding the host image, called host coefficient, and the secret image such that $m = f(c, s)$, where c is the host coefficient, s is the secret pixel and m is the modification. Thank to this strategy, the shadows constructed by our proposed scheme are meaningful with high quality and there are no pixel expansion problem occurred.

The rest of this paper is organized as follows. Section II introduces the related work in this field, and Section III is the proposed Sudoku-table-based secret image sharing scheme. The analysis of the proposed scheme and the experimental results are then presented in Section IV, and Section V presents our final conclusions.

II. Proposed Scheme

A. Share Construction Algorithm

Input: Grayscale Secret Image S sized $H \times M$, $\{S_i | i = 1, 2, \ldots,$

Manuscript received April 5, 2014; revised May 29, 2014.

C. C. Chang was with the Department of Computer Science and Information Engineering, Asia University, No. 500, Lioufeng Rd., Wufeng, Taichung, 41354, Taiwan. He is now with the Department of Information Engineering and Computer Science, Feng Chia University, No. 100, Wenhwa Rd., Seatwen, Taichung, 40724, Taiwan (corresponding author; e-mail: alan3c@gmail.com; tel.:+886-4-24517250 ext. 3790).

N. T. Huynh and T. F. Chung were with the Department of Information Engineering and Computer Science, Feng Chia University, No. 100, Wenhwa Rd., Seatwen, Taichung, 40724, Taiwan (e-mail: ngoctu84vn@gmail.com, carter629629@gmail.com).

$H \times W$}, and

Cover Image O sized $H \times M$

Output: Two shares S^1 and S^2 sized $H \times W$

Algorithm:

Step 1: Generate the Sudoku matrix sized 256 ×256.

Step 2: Convert each pixel of secret image into a group of digits in base-9 numeral system. After converting, value of the first digit is from 1 to 3 because the highest value of a grayscale image is 255, we have $255_{10} = 313_9$. Therefore, the highest value of digits is 3. If the result of converting step is two digits, we shall add a bit 0 to get a group of three digits. Now, our digit group includes three digits d_1, d_2, d_3.

Step 3: Read the next pixel pair (O_i, O_{i+1}) from cover image O according to the user-defined pairing rule and map them to the reference matrix to get the modification m.

Step 4: In order to construct shares, dealer checks the first bit d1 in the group. The reference matrix is divided into four directions as Fig. 1.

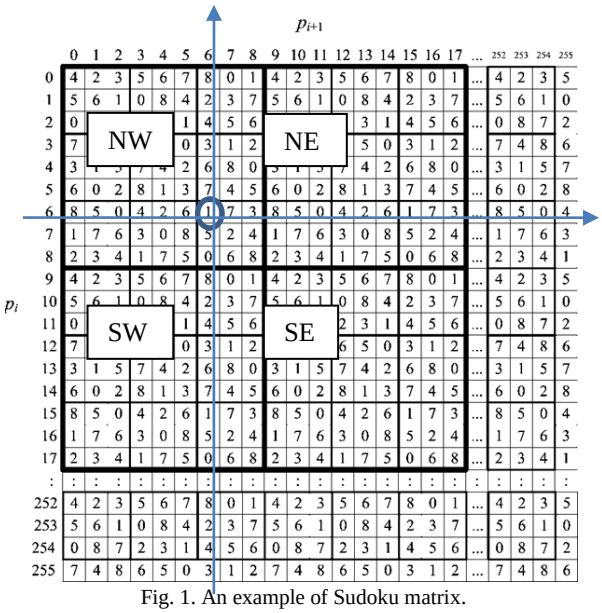


Fig. 1. An example of Sudoku matrix.

Based on the value of the digit d_1, we have four cases to be considered:

Case 1: $d_1 = 0$

Dealer searches for mapping value in the NW region of the table.

- To create share S^1, dealer searches along the horizontal to find the mapping value of d_2.
- To create share S^2, dealer searches along the vertical line to find the mapping value of d_3.

Case 2: $d_1 = 1$

Dealer searches for mapping value in the NE region of the table.

- Share S^1 is created by finding the mapping value d_2 on the horizontal line.
- Share S^2 is generated according to the mapping value d_3 which is found on the vertical line.

Case 3: $d_1 = 2$

Dealer searches for mapping value in the SE region of the table.

- Generates S^1 and S^2 by the same way as Case 2.

Case 4: $d_1 = 3$

Dealer searches for mapping value in the SW region of the table.

- The share S^1 and S^2 are constructed by the same way as Case 2.

Step 5: Repeat Step 2 to Step 4 until all the pixels are processed and the shares are constructed.

B. Secret Image Revealing and Cover Image Reconstructing Algorithm

Input: Two shares S^1, S^2, sized $H \times W$

Output: Secret Image S, sized $H \times M$, $\{S_i | i = 1, 2, ..., H \times W\}$

Step 1: Generate the Sudoku matrix sized 256 × 256.

Step 2: Read the next pixel pair from collected shares S^1: $\left(S_i^1, S_{i+1}^1\right)$ and S^2: $\left(S_i^2, S_{i+1}^2\right)$ according to the user-defined pairing rule.

Step 3: Map the pixel pair value $\left(S_i^1, S_{i+1}^1\right)$ to the Sudoku table, we can get the digit d_2 and map the pixel pair value $\left(S_i^2, S_{i+1}^2\right)$ to the Sudoku matrix, we get the digit d_3.

Step 4: In Share Construction Algorithm, dealer only finds the mapping value on the vertical and horizontal direction, and their intersection is the element corresponded to the cover pixels pair. Therefore, we can reconstruct the original cover pixels by searching along the vertical direction lined from d_2 and horizontal direction lined from d_3. Their intersection is the element m and the original cover pixel pair is found such that $(I_i, I_{i+1}) = m$.

Step 5: According to position of d_2 and d_3 correlative to the position of m, we can determine the value d_1 based on the following rules:

If d_2 and d_3 are located in the NW region, then $d_1 = 0$.

If d_2 and d_3 are located in the NE region, then $d_1 = 1$.

If d_2 and d_3 are located at the SE corner, then $d_1 = 2$.

If d_2 and d_3 are located at the SW corner, then $d_1 = 3$.

Step 6: Convert three digits $(d_1, d_2, d_3)_9$ to the decimal based numeral system to reveal the original secret pixel.

Step 7: Repeat Step 2 to Step 6 to reveal the original secret image and reconstruct the cover image.

III. Experimental Results

In this section, our experimental results will be shown to illustrate the features of our scheme. We implement our method by using MATLAB 7.10 software running on the Duo Core CPU, and 2GB RAM hardware platform. Ten commonly used grayscale images sized 512 ×512, as shown in Fig. 2 were used as cover images and secret images in our simulations to test the performance of our proposed method in term of security, accuracy, computational complexity, and shadow size.

A. Security Analysis

To ensure that our scheme satisfies the security criterion; that is, it protects a shadow from leaking any information about the original secret image, we generate a set of meaningful shadows with high quality so that it does not gain any suspicion from attacker. The sets of generated shadows are shown in Fig. 3, in which we embed and share the secret

image (i.e. Airplane) using different cover images.

Fig. 3 clearly shows that each shadow is very similar to the original cover image that helps mitigate the suspicions of attackers. Even in cases of doubt, no information can be leaked from it. Therefore, security from the human visual system can be guaranteed. Moreover, to demonstrate the security of our scheme theoretically, we use two general parameters, the number of pixels change rate (*NPCR*) and the unified average changing intensity (*UACI*). *NPCR* considers the percentage of different pixel numbers between the two shadows, S^1 and S^2, while *UACI* is the average intensity of differences between the two shadows.

The *NPCR* value is defined in Equation (1).

$$NPCR(S_1, S_2) = \frac{\sum_{i,j} G(i,j)}{W \times H} \times 100\%, \quad (1)$$

where *W* and *H* are the width and height of shadows S^1 and S^2. $G(i, j)$ is determined as:

$$G(i,j) = \begin{cases} 1, & S_1(i,j) \neq S_2(i,j) \\ 0, & S_1(i,j) = S_2(i,j) \end{cases}. \quad (2)$$

In [17], Kwoka and Tang claimed that a scheme gives optimal results when the *NPCR* value is equal to $(1 - 2^{-l}) \times 100\%$, where l is the number of bits used to represent one pixel of an image. Thus, for a grayscale image shadow, whose pixel contains 8 bits (l = 8), the corresponding expected *NPCR* value is 99.61%.

In contrast, *UACI* is determined by Equation (3):

$$UACI(S_1, S_2) = \frac{1}{W \times H}\left(\frac{\sum_{i,j}|S_1(i,j) - S_2(i,j)|}{2^l - 1}\right) \times 100\%. \quad (3)$$

The expected *UACI* value is $\frac{\sum_{i=1}^{2^l-1} i(i+1)}{2^l \times 2^l \times (2^l - 1)} \times 100\%$.

Consequently, for grayscale images, the *UACI* is around 33%. Table I shows the *NPCR* and *UACI* values that are achievable with our proposed scheme.

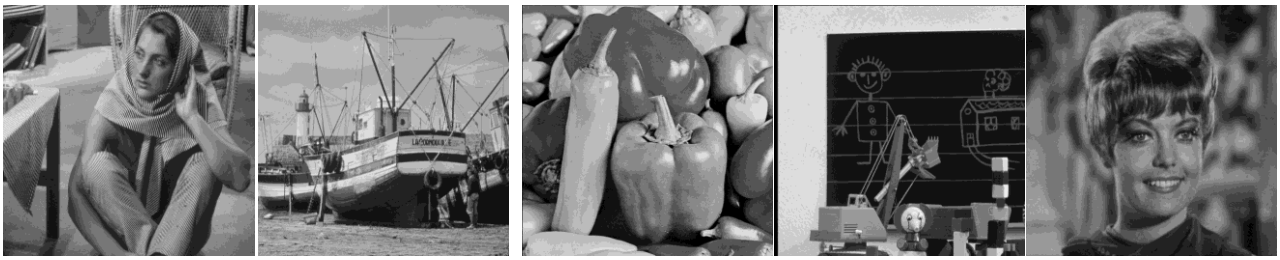
TABLE I: NPCRS AND UACIS FOR THESE SETS OF SHADOWS OF FOUR TEST IMAGES

Image	Shadow 1		Shadow 2	
	NPCR	UACI	NPCR	UACI
Lena	99.9%	33.13%	99.8%	33.30%
Baboon	99.9%	34.68%	99.9%	34.03%
Goldhill	99.7%	32.99%	99.8%	33.01%
Barbara	99.8%	33.17%	99.8%	33.36%

B. Accuracy

To consider the accuracy criterion, we exploited the peak signal-to-noise ratio (*PSNR*) which is the basic parameter for evaluating the quality of reconstructed grayscale and color images. Essentially, a secret sharing scheme is assumed to achieve good visual quality of reconstructed images when the *PSNR* value ranges between 30dB and 40dB.

Lena Baboon Airplane GoldHill House



Barbara Boat Peppers Toys Zelda

Fig. 2. Test Images (cover images and secret image).

$$PSNR = 10 \times \log_{10} \frac{255^2}{MSE}, \quad (4)$$

where *MSE* is the mean square error between the original image and the reconstructed image, and is defined in Equation (5).

$$MSE = \frac{1}{W \times H} \sum_{x=1}^{W} \sum_{y=1}^{H} (C_{xy} - C'_{xy})^2, \quad (5)$$

where $W \times H$ is the image size, C_{xy} and C'_{xy} are the pixel values at position (x, y) of the original grayscale image and the reconstructed grayscale secret image, respectively.

Table II is the quality of shadows constructed by our scheme.

Especially, our scheme can be extended to increase embedding capacity by sharing two secret images at the same time. Fig. 4 shows that even embedding two secrets into cover images, the quality of shadows is still very high.

TABLE II : VISUAL QUALITY OF TWO SHADOWS GENERATED BY SHARING ONE SECRET IMAGE

Cover Image	PSNR	
	Shadow 1	Shadow 2
Lena	39.396	39.166
Baboon	39.378	39.162
Airplane	39.161	39.172
Barb	39.152	39.127
Boat	39.141	39.170
Gold	39.348	39.143
Toy	39.210	39.126
Zelda	39.327	39.150
Home	39.757	39.190

Table III demonstrates visual quality of shadows when we share two secret images. It can be seen that, when our embedding capacity is two times higher, the PSNR of the shadows only decreases 3dB.

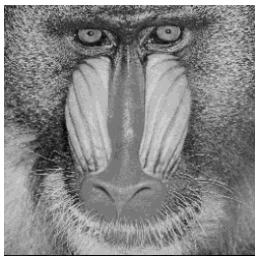
C. Computational Complexity

It is important for a visual secret sharing scheme to be able to share and reveal secret information while maintaining low computational complexity.

Our shares construction phase as well as our revealing algorithm, which are described in detail in Subsections 2.1 and 2.2, demonstrate that the computational cost of the proposed scheme depends on linear searching strategy which has $O(n)$ time complexity. It is the lowest computational cost and thus the least effect on the complexity of the scheme. Table IV lists all the formulas which are used in proposed schemes of Lin et al.'s scheme, El-Latif's scheme and our proposed scheme. It can be seen that our proposed scheme is the simplest scheme which only uses searching strategy.

Secret Image

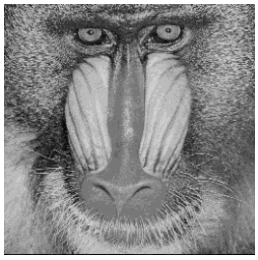
Cover Image



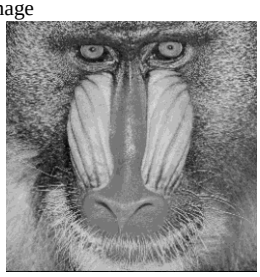
Cover Image

Shadow 1

Shadow 2



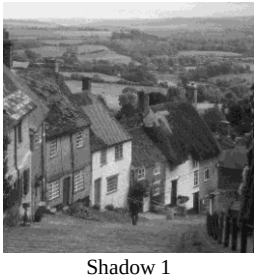
Shadow 1



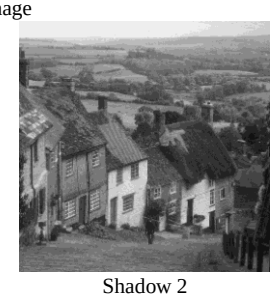
Shadow 2

Cover Image

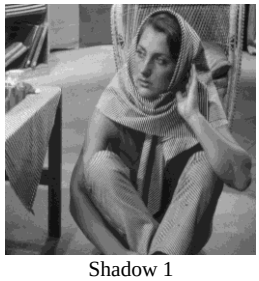
Cover Image



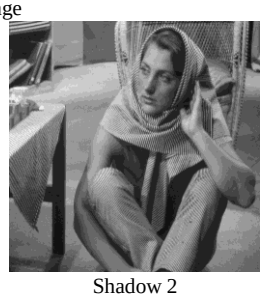
Shadow 1



Shadow 2



Shadow 1



Shadow 2

Fig. 3. One secret image and its shadows with different cover images.

TABLE III: IMAGE QUALITY OF TWO SHADOWS GENERATED BY SHARING TWO SECRET IMAGES

Cover Image	PSNR	
	Shadow 1	Shadow 2
Lena	36.2893	36.1366
Baboon	36.2876	36.1512
Airplane	36.1489	36.1530
Barb	36.1597	36.1269
Boat	36.1421	36.1463
Gold	36.2762	36.1346
Toy	36.1681	36.1092
Zelda	36.2479	36.1488
Home	36.4681	36.1575

D. Pixel Expansion

With our proposed scheme, a pair of cover pixels is used to embed one secret bit and generate two shares, S^1 and S^2, which are the same size as the original cover image. However, we can embed two secret images to increase the embedding capacity of the scheme. Therefore, our proposed scheme does not cause pixel expansion problem.

IV. CONCLUSIONS

This paper proposes a new visual secret sharing scheme that is effective with grayscale images. The proposed scheme can generate a set of shadows with high visual quality. Especially, the scheme can exactly reconstruct the secret image. Our experimental results show that the proposed scheme satisfies the four general essentials of visual secret sharing systems. In addition, the computational complexity of our proposed scheme is much less than other schemes proposed previously. Therefore, our proposed scheme is suitable for real-time applications.

REFERENCES

[1] A. Shamir, "How to share a secret," *Communications of the Association for Computing Machinery*, vol. 22, no. 11, pp. 612-613, 1979.

[2] G. R. Blakley, "Safeguarding cryptographic keys," in *Proc. the National Computer Conference, American Federation of Information Processing Societies*, pp. 313-317, June 1979.

[3] M. Naor and A. Shamir, "Visual cryptography," *Lecture Notes in Computer Science*, vol. 950, pp. 1-12, 1995.

[4] P. Y. Lin, J. S. Lee, and C. C. Chang, "Distortion-free secret image sharing mechanism using modulus operator," *Pattern Recognition*, vol. 42, pp. 886-895, 2009.

[5] P. Y. Lin and C. S. Chan, "Invertible secret sharing with steganography," *Pattern Recognition Letters*, vol. 31, pp. 1887-1893, 2010.

[6] C. Guo, C. C. Chang, and C. Qin, "A hierarchical threshold secret image sharing," *Pattern Recognition Letters*, vol. 33, pp. 83–91, 2012.

[7] A. A. Abd El-Latif, X. Yan, L. Li, N. Yang, J. L. Peng, and X. Niu, "A new meaningful secret sharing scheme based on random grids, error diffusion and chaotic encryption," *Optics and Laser Technology*, vol. 54, pp. 389-400, 2013.

[8] X. T. Wu and W. Sun, "Improving the visual quality of random grid-based visual secret sharing," *Signal Processing*, vol. 93, pp. 977-995, 2013.

[9] X. T. Wu, T. Liu, and W. Sun, "Improving the visual quality of random grid-based visual secret sharing via error diffusion," *Journal of Visual Communication and Image Representation*, vol. 24, no. 5, pp. 552-566, July 2013.

[10] K. L. Chung and S. T. Wu, "Inverse Halftoning algorithm using edge-based lookup table approach," *IEEE Trans. on Image Processing*, vol. 14, no. 10, pp. 1583-1589, Oct. 2005.

[11] C. C. Chang, Y. C. Chou, and T. D. Kieu, "An information hiding scheme using Sudoku," in *Proc. The Third International Conference on Innovative Computing, Information and Control (ICICIC 2008)*, Dalian, China, pp. 17-21, June 2008.

[12] T. D. Kieu, Z. H. Wang, C. C. Chang, and M. C. Li, "A Sudoku Based wet paper hiding scheme," *International Journal of Smart Home*, vol. 3, no. 2, April 2009.

[13] W. Hong, T. S. Chen, and C. W. Shiu, "A minimal Euclidean distance searching technique for Sudoku steganography," in *Proc. the 2008 International Symposium on Information Science and Engineering, ISISE '08*, 2008.

[14] C. C. Chang, P. Y. Lin, Z. H. Wang, and M. C. Li, "A Sudoku-based secret image sharing scheme with reversibility," *Journal of Communications*, vol. 5, no. 1, pp. 5-12, January 2010.

[15] Y. C. Chou, C. H. Lin, P. C. Li, and Y. C. Li, "A (2, 3) Threshold secret sharing scheme using sudoku," *The Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)*, pp. 43-46, 2010.

[16] Z. H. Wang, C. Guo, and C. C. Chang, "A novel (*n*, *n*) secret image sharing scheme based on Sudoku," *Journal of Electronic Science and Technology*, vol. 11, no. 1, pp. 44-50, 2013.

[17] H. S. Kwoka and W. K. S. Tang, "A fast image encryption system based on chaotic maps with finite precision representation," *Chaos, Solitons and Fractals*, vol. 32, no. 4, pp. 1518-1529, May 2007.

Chin-Chen Chang received the B.S. degree in science in applied mathematics and M.S. degree in science in computer and decision sciences. Both were awarded in National Tsing Hua University, Taiwan. He received his Ph.D. degree in computer engineering from National Chiao Tung University, Taiwan.

His current title is chair professor in the Department of Information Engineering and Computer Science, Feng Chia University, from Feb. 2005. He is currently a fellow of IEEE and a fellow of IEE, UK. His current research interests include database design, computer cryptography, image compression and data structures.

Since his early years of career development, he consecutively won Outstanding Talent in Information Sciences of the R. O. C., AceR Dragon Award of the Ten Most Outstanding Talents, Outstanding Scholar Award of the R. O. C., Outstanding Engineering Professor Award of the R. O. C., Distinguished Research Awards of National Science Council of the R. O. C., Top Fifteen Scholars in Systems and Software Engineering of the Journal of Systems and Software, and so on. On numerous occasions, he was invited to serve as a visiting professor, chair professor, honorary professor, honorary director, honorary chairman, distinguished alumnus, Distinguished researcher, research fellow by universities and research institutes.

Ngoc-Tu Huynh received the BS degree in mathematics — informatics in 2006 from Danang University, Vietnam, and the MS degree in information engineering and computer science in 2010 from Feng Chia University. Since 2006, she has been a lecturer of Department of Computer Science, College of Information Technology, Danang University, Vietnam. She is currently pursuing her Ph.D in information engineering and computer science, Feng Chia University, Taichung, Taiwan. Her research interests include visual cryptography, watermarking, steganography and image processing.

Ting-Feng Chung was born in Kaohsiung, Taiwan, in 1990. He received the B.S. degree in applied informatics and multimedia from Asia University, Taichung, Taiwan, in 2012. He is currently working toward the M.S. degree in information engineering and computer science from Feng Chia University, Taichung, Taiwan. His research interests include Steganography and image processing