Received December 30, 2017, accepted February 9, 2018, date of publication March 13, 2018, date of current version April 4, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2811722

Secret Image Sharing Based on Encrypted Pixels

ZHILI ZHOU[1], CHING-NUNG YANG[2], (Senior Member, IEEE), YI CAO[1], AND XINGMING SUN[1], (Senior Member)

[1]Jiangsu Engineering Center of Network Monitoring, School of Computer and Software, NanJing University of Information Science and Technology, Nanjing 210044 China

[2]Department of Computer Science and Information Engineering, National Dong Hwa University, Hualien County 97401, Taiwan

Corresponding author: Ching-Nung Yang (cnyang@gms.ndhu.edu.tw)

This work was supported in part by the Ministry of Science and Technology under Grant MOST 105-2221-E-259-015-MY2, in part by the National Natural Science Foundation of China under Grant 61602253, Grant U1536206, Grant U1405254, Grant 61772283, Grant 61672294, Grant 61572258, and Grant 61502242, in part by Jiangsu Natural Science Foundation under Grant BK20150925 and Grant BK20151530, in part by the Priority Academic Program Development of Jiangsu Higher Education Institutions fund, and in part by Collaborative Innovation Center of Atmospheric Environment and Equipment Technology Fund, China.

ABSTRACT The well-known Thien and Lin's (k, n) secret image sharing (SIS) scheme and its extended versions are threshold schemes, in which a secret image is shared among n shadow images and it can be recovered from any k shadow images. To reduce the size of shadow image, in those schemes, secret image pixels are embedded in all coefficients of $(k-1)$-degree polynomial to generate the shadows. Also, the secret pixels are permuted before the sharing to address the residual-image problem on shadow images. Due to the above two approaches, partial secret information can be exposed from $(k-1)$ shadow images, and thus the threshold properties of those schemes will be compromised. To overcome this weakness, we propose a novel (k, n)-SIS scheme based on encrypted pixels, whose shadow image size is slightly larger than that of Thien and Lin's scheme. By slightly modifying the secret image, we also propose a modified (k, n)-SIS scheme with the same shadow size of Thien and Lin's scheme.

INDEX TERMS Encryption, permutation, secret sharing, secret image sharing, visual cryptography.

I. INTRODUCTION

To protect and communicate the secret image data, a variety of techniques such as image steganography [1], copy detection [2], [3], and encryption [4] have been widely researched. Different from these techniques, a secret sharing scheme shares a secret among n shadow images in such a way that the secret can be recovered from any k shadows but no information can be obtained from $k-1$ or fewer shadows [5]. In 1979, Shamir [5] proposed a (k, n) secret sharing, where $k \leq n$, to hide a secret data in the constant term of a $(k-1)$-degree polynomial to generate the shadows. Thien and Lin [6] firstly extended Shamir's (k, n) secret sharing to (k, n) secret image sharing (SIS) scheme for dealing with images. To reduce the shadow size, instead of using only one coefficient, Thien and Lin's (k, n)-SIS scheme uses all coefficients $(a_0, a_1, \ldots, a_{k-1})$ of a $(k-1)$-degree polynomial $f(x) = (a_0 + a_1x + \ldots + a_{k-1}x^{k-1})$ over $GF(251)$ (or $GF(2^8)$) to embed secret pixels, so that the shadow size is reduced to $1/k$ times of secret image size. By using $i \in [1, n]$, the dealer can generate n shadow pixels as $f(i)$. After repeating the above procedure for every k pixels, n shadows are created. Any k shadows can jointly reconstruct the secret image via Lagrange interpolation, but $(k-1)$ or fewer shadows cannot. Thus, the (k, n)-SIS scheme can be regarded as a threshold scheme.

Afterwards, various SIS schemes were accordingly proposed. Noise-like shadows are suspected by censorships, and thus some (k, n)-SIS schemes were proposed using steganography and authentication so that the shadows reveal meaningful image and meanwhile have the tamper detection capability [7]–[10]. For some applications, a part of privileged participants may have shadows more important than others. Several SIS schemes [11], [12] are designed to provide shadows with different importance. The above SIS schemes recover either the entire image or nothing. A new scalable SIS scheme with the scalability that the information amount of reconstructed image is proportional to the number of involved shadows was introduced in [13] and [14]. Since all of those SIS schemes are based on Thien and Lin's (k, n)-SIS scheme, they can be regarded as its extended versions.

Note that, if we directly apply secret sharing on a secret image, some residual information of this image will be left on because of the relationships among neighbor pixels. Fig. 1 shows the residual image effect. To avoid this problem, all of the above (k, n)-SIS schemes use a key to permute the pixels of the secret image before the secret sharing.

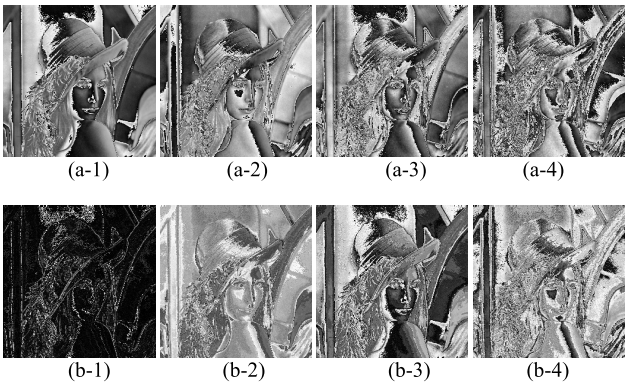


FIGURE 1. Four shadows with image IDs 1, 2, 3 and 4 of (2, 4)-SIS scheme over finite fields: (a) *GF* (251) (b) *GF* (2^8).

However, since all coefficients are used in those (k, n)-SIS schemes, a part of permutated pixels may be directly obtained from less than k shadows, which will be shown in the next section. Moreover, Jolfaei *et al.* [15] proved that permutation-only ciphers are insecure and correct permutation mapping can be recovered completely by a chosen-plaintext attack. Therefore, some partial secret pixels could be exposed from $(k-1)$ shadows, which will compromise the threshold properties of those (k, n)-SIS schemes.

To overcome the above weakness, we use encryption rather than simple permutation, and propose a (k, n)-SIS scheme based on encrypted pixels, in which the shadow size is the $1/k$ size of a secret image plus a short piece of key length. In addition, a modified secure (k, n)-SIS scheme is proposed to achieve the same shadow size as Thien and Lin' scheme.

II. THE PROBLEM OF THE EXISTING SIS SCHEMES

Shamir's scheme only uses one coefficient of a $(k-1)$-degree polynomial for embedding secret, and thus it has perfect security [5]. Different from Shamir's scheme, Thein and Lin's (k, n)-SIS scheme and its extended versions use all coefficients of a $(k-1)$-degree polynomial for embedding secret pixels to reduce the shadow size. To avoid residual image effect, all of those existing (k, n)-SIS schemes which are mentioned above permute the pixels of a secret image before the secret sharing. Consequently, partial secret pixels can be reconstructed from less than k shadows, and thus the threshold properties of those (k, n)-SIS schemes will be compromised. That can be illustrated by the following examples.

Suppose that we embed three permutated secret pixels (a_0, a_1, a_2) in the following polynomial of degree 2 over the finite field $GF(251)$.

$$f(x) = a_0 + a_1 x + a_2 x^2 \tag{1}$$

Also, suppose that the i-th shadow is given by $S_i = f(i)$. Then, after a simple calculation by S_1 and S_{250}, we obtain

$$a_1 = 126S_1 + 125S_{250} \tag{2}$$

By the same argument, for $(4, n)$-SIS scheme based on $a_0 + a_1 x + a_2 x^2 + a_3 x^3$, we can derive a_1 in Eq. (3-1) by S_7, S_8 and S_{13}. Consider another case that we can obtain a_2 in Eq. (3-2) by S_3, S_4 and S_{244}.

$$\begin{cases} a_1 = 122S_7 + 4S_8 + 125S_{13} & (3\text{-}1) \\ a_2 = 25S_3 + 137S_4 + 89S_{244} & (3\text{-}2) \end{cases}$$

Eqs. (2) and (3) imply that those existing (k, n)-SIS schemes are not always strong enough. We can recover the partial permutated pixels from $(k-1)$ shadows. Note that, if the permutation is not secure enough, one can recover some original pixels of the secret image. Generally, the image pixels are permuted using a permutation matrix that is built by a pseudo-random number generator. In fact, the cryptanalysis demonstrated that such permutation-only image ciphers are insecure against ciphertext-only attacks and/or known/chosen plaintext attacks. Jolfaei *et al.* [15] showed that the correct permutation mapping can be recovered completely by a chosen-plaintext attack. For an image with the size of $(M \times N)$ and with L different color intensities, the number of required chosen plain-images to break the permutation-only image cipher is $\lceil \mathrm{Log}_L(MN) \rceil$. The complexity indicates that this attack is computational feasible in a polynomial time.

Finally, the partial pixels of a secret image will be reconstructed from $k-1$ shadows, and this compromises the threshold properties of those existing (k, n)-SIS scheme. By the above approach, there are one third, a quarter and one fifth pixels of a secret image that can be recovered for $(3, n)$, $(4, n)$ and $(5, n)$ SIS schemes, respectively. For a secret image "Lena", Fig. 2 reveals the reconstructed images of $(3, n)$, $(4, n)$ and $(5, n)$ SIS schemes generated from $(k-1)$ shadows, where black pixels are used for unknowns.

FIGURE 2. Using $(k-1)$ shadows to recover the secret images of (k, n)-SIS scheme with: (a) k=3 (b) k=4 (c) k=5.

III. THE PROPOSED (k, n)-SIS SCHEME

A. DESIGN CONCEPT

As illustrated above, although those existing (k, n)-SIS schemes have the advantage that shadow size is significantly smaller than the secret size, some partial secret pixels could be exposed from $(k-1)$ shadows because (i) all coefficients are used for embedding and (ii) the permutation is not secure enough. As a result, the threshold properties of the existing (k, n)-SIS schemes are compromised.

Therefore, all of those existing SIS schemes are not secure enough. To address the security problem while maintaining the advantage of small shadow size, instead of simply permuting secret image pixels and using the permuted

pixels, we propose a secure (k, n)-SIS scheme based on encrypted pixels. It combines the perfect secret sharing (using one coefficient in polynomial for embedding), the existing secret image sharing (using all coefficients in polynomial for embedding), and encryption.

To make the secret sharing more feasible and practical, without using an extra key distribution protocol, we share the key by the perfect secret sharing again. Finally, our shadow size is the $1/k$ size of a secret image plus a short piece of key (*e.g.*, 128 bits for encryption), which is much smaller compared with the size of secret image.

B. DISTRIBUTION AND RECONSTRUCTION

Next, we describe distribution (the generation of shadows) and reconstruction (the recovery of secret image from any k shadows). Notations and their descriptions are listed in Table 1.

TABLE 1. Notation and description.

Notation	Meaning
I	A secret image I with the size $\|I\|$.
$E_K(\cdot)/D_K(\cdot)$	Encryption/decryption under the key K with the key size $\|K\|$, where the plaintext and ciphertext are 128 bits.
$\hat{I}$	Encrypted image, *i.e.*, $E_K(I)=\hat{I}$ and $D_K(\hat{I})=I$.
$CS_{k,n}(\cdot)$	The secret sharing function that shares every k secret pixels $(a_0, a_1, \ldots, a_{k-1})$ of an image by $f(x)=(a_0+a_1x+\cdots+a_{k-1}x^{k-1})$ over $GF(251)$ (or $GF(2^8)$), and then generates n shadow pixels $(b_0, b_1, \ldots, b_n)$ where $b_i=f(i)$, $i\in[1, n]$. $CS^{-1}{}_{k,n}(\cdot)$ is its reverse function, which can recover the polynomial from any k shadow pixels.
$PS_{k,n}(\cdot)$	A (k, n)-perfect secret sharing that embeds secret into a_0 of $f(x)$ to generate n shares. $PS^{-1}{}_{k,n}(\cdot)$ is its reverse function.
S_i	Image shadows S_i of the proposed (k, n)-SIS scheme, where $1\le i\le n$.

Distribution: In this phase, the dealer shares the secret image among n shadows $\{S_1, S_2, \ldots, S_n\}$, and delivers them to n participants.

(1) The dealer selects a random key K, and encrypts I to obtain $\hat{I}=E_K(I)$.

(2) By $CS_{k,n}(\cdot)$ function, we process every k encrypted pixels to share $\hat{I}$ to n fragmented images $\{F_1, F_2, \ldots, F_n\}=CS_{k,n}(\hat{I})$.

(3) By $PS_{k,n}(\cdot)$ function, we share the key K to n sub-shares $\{K_1, K_2, \ldots, K_n\}=PS_{k,n}(K)$.

(4) By concatenating F_i and K_i, we generate n shadows $S_i=(F_i||K_i)$, where $i=1, 2, \ldots, n$.

Reconstruction: In this phase, any k shadows are used to reconstruct the secret image.

(1) Any k shadows are used for reconstruction (w.l.o.g. say $S_1, S_2, \ldots,$ and S_k).

(2) Extract F_i and K_i from S_i, respectively, for $1\le i\le k$.

(3) Recover the encrypted image $\hat{I}=CS^{-1}_{k,n}(F_1, F_2, \ldots, F_k)$.

(4) Recover the key $K=PS^{-1}_{k,n}(K_1, K_2, \ldots, K_k)$.

(5) Via $\hat{I}$ and K, decrypt the secret image $I=D_K(\hat{I})$.

The following theorem shows that the proposed (k, n)-SIS scheme based on encrypted pixels is computationally secure. Here, "computationally secure" means that the security of the proposed SIS scheme is similar to that of computationally infeasible secure encryption/decryption.

Theorem 1: The proposed SIS scheme is a (k, n)-threshold scheme, and is computationally secure. Each shadow has the size $(|I|/k)+|K|$.

Proof: We first prove that our scheme is a (k, n)-threshold scheme, *i.e.*, the secret image can be reconstructed from any k shadows (w.l.o.g. say $S_1, S_2, \ldots, S_k$). From these k shadows, we derive k fragmented images F_1-F_k and sub-keys K_1-K_k, and recover $\hat{I}=CS^{-1}_{k,n}(F_1, F_2, \ldots, F_k)$ and $K=PS^{-1}_{k,n}(K_1, K_2, \ldots, K_k)$. Via $\hat{I}$ and K, the secret image can be decrypted and obtained.

Suppose that the decryption function $D_K(\cdot)$ is computationally infeasible. We also prove our scheme is computationally secure. In other words, we prove that no information about the secret can be recovered from less than k shadows. From Section II, we can only obtain partial encrypted pixels from less than k shadows for some cases ($\because$ $CS(\cdot)$ does not have perfect security). However, we cannot decrypt the secret pixels from those encrypted pixels, because the key K in the computation infeasible function $D_K(\cdot)$ cannot be obtained from less than k shadows ($\because$ $PS(\cdot)$ is a perfect secret sharing scheme). Finally, it is obvious that the shadows size is $|S_i|=|(F_i||K_i)|=|F_i|+|K_i|=(|I|/k)+|K|$.

Fig. 3 shows one shadow of the proposed $(2, n)$-SIS scheme over $GF(2^8)$ using 512×512-pixel Lena as a secret image. The total shadow size is (512×256) pixels plus $|K|=128$ bits (*e.g.*, 128-bit key for AES encryption), which are represented as 16 pixels and are put in the last column of shadow.

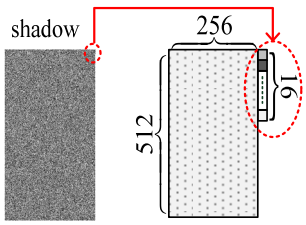


FIGURE 3. The frame structure of a shadow in the proposed (2, *n*)-SIS scheme with 16 pixels in the last column.

Actually, an image with 16 pixels in the last column is not processing-friendly to most image processing tools. Yang *et al.*[16] used an inherent property of image to let the involved k participants easily obtain the permutation key for Thien and Lin's (k, n)-SIS scheme. Their approach is based on the fact that the permutation of pixels does not change histogram. However, our scheme encrypts the image and all the values of pixels are changed. Thus the method in [16] cannot be used for the proposed scheme. To achieve the same shadow size of Thien and Lin's scheme (*i.e.*, $|I|/k$), in next section, we also propose a modified (k, n)-SIS scheme.

IV. The MODIFIED (k, n)-SIS SCHEME

A. DESIGN CONCEPT

Consider that the secret image is a gray-level image with 512×512 pixels and the length of encryption key is 128 bits, where $K = (k_1, k_2, \ldots, k_{128})$. The design concept is briefly described as follows. As shown in Fig. 4, we first subdivide a secret image into 128 super blocks SB_i, $1 \le i \le 128$. Then, we divide each super block SB_i into 128 blocks $B_{i,j}$, $1 \le j \le 128$, and thus every block has 16 pixels (*i.e.*, 128 bits). Let the super block and the block in an encrypted image be $\widehat{SB}_i$ and $\widehat{B}_{i,j}$.

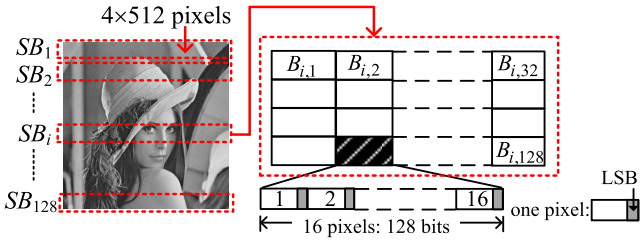


FIGURE 4. Super blocks and blocks in the modified (*k*, *n*)-SIS scheme.

If the XOR-ed result of the bits of all pixels in $\widehat{SB}_i$ is the same as k_i, the super block SB_i is not modified. Otherwise, modify the least significant bit (LSB) in one of 16 pixels in the block $B_{i,j}$, for $1 \le j \le 128$, to test whether the XOR-ed result of all bits in the new $\widehat{SB}_i$ is the same as k_i. There are $128 \times 16 = 2048$ ($\because$ one super block has 128 blocks, and every block has 16 pixels) chances to get the same result, and the successful probability is almost 100% ($\approx 1-(0.5)^{2048}$). Thus, at most, we only need to change one bit in SB_i, which implies that the modified image I' has almost no distortion with a very high PSNR, *i.e.*, $10\log_{10}\left(\frac{255^2}{128/(512\times512)}\right) = 81.24$dB.

B. DISTRIBUTION AND RECONSTRUCTION

Let the operation $\text{XOR}(\widehat{SB}_i) = k_i$, $1 \le i \le 128$, be the XOR-ed result of the bits of all pixels in $\widehat{SB}_i$, and the operation $I' = \text{LSB}(B_{i,j})$ be the modification of the LSB in one of 16 pixels in $B_{i,j}$, for $1 \le j \le b$, to get a modified image I'. Distribution and reconstruction of the modified (k, n)-SIS scheme are described below.

Distribution:

(1) The dealer selects a random key $K = (k_1, k_2, \ldots, k_{128})$ (for simplicity we use $|K| = 128$), and encrypts I to obtain $\hat{I} = E_K(I)$.

(2) Subdivide I and $\hat{I}$ into 128 super blocks SB_i and $\widehat{SB}_i$, $1 \le i \le 128$, respectively, where every super block has b 16-pixel blocks $B_{i,j}$ and $\widehat{B}_{i,j}$, $1 \le i \le b$, respectively (note: the block length is 128 bits; we use XTS-AES mode (IEEE standard 1619-2007), which employs a ciphertext-stealing technique instead of padding, and thus no extra appended bits are required).

(3) For $i = 1$ to 128, do {if $\text{XOR}(\widehat{SB}_i) = k_i$ skip the super block, else {for $j = 1$ to b do {$I' = \text{LSB}(B_{i,j})$; $\hat{B}_{i,j} = E_K(\text{LSB}(B_{i,j}))$; if $\text{XOR}(\widehat{SB}_i) = k_i$ skip the super block}}}.

(4) Encrypt the modified image, *i.e.*, $\widehat{I} = E_K(I')$.

(5) We generate n shadows $\{S_1, S_2, \ldots, S_n\}$ from $CS_{k,n}(\hat{I})$.

Reconstruction:

(1) Any k shadows are used for secret image reconstruction (w.l.o.g. say $S_1, S_2, \ldots,$ and S_k).

(2) Recover the encrypted image $\hat{I} = CS_{k,n}^{-1}(S_1, S_2, \ldots, S_k)$.

(3) Obtain the key K from $k_i = \text{XOR}(\widehat{SB}_i)$, $1 \le i \le 128$.

(4) Via $\hat{I}$ and K, decrypt the secret image $I' = D_K(\hat{I})$.

In step (3) of distribution phase, the modified I' has the property $\text{XOR}(\widehat{SB}_i) = k_i$, $1 \le i \le 128$, where $\widehat{SB}_i$ is the super block in $\widehat{I} = E_K(I')$; the probability of success of this process is $1-(0.5)^{16\times b}$. For a 512×512-pixel image, when the value of b is 128, the probability is equal to $1-(0.5)^{16\times b} = 1-(0.5)^{2048} \approx 100\%$. For a very small-size image, *e.g.*, 64×32-pixel image, by a certain manner, we can also divide it into 128 super blocks, each of which has 16 blocks. For this case, we have $b = 1$. Thus, the probability is $1-(0.5)^{16} = 99.998\%$, which is still a very high probability to accomplish step (3) of distribution phase. Also, we can choose to modify at most two LSBs in a block. Then, the probability for $b = 1$ will be $1-(0.5)^{\binom{16}{1}+\binom{16}{2}} = 1-(0.5)^{16+120} = 1-(0.5)^{136} \approx 100\%$, and the PSNR of modified image is slightly reduced from 81.24dB to 78.2dB. Although the recovered image is not the original one, the quite high PSNR means that it almost the same as the original one.

Theorem 2: The modified SIS scheme is a (k, n)-threshold scheme, and is computationally secure. Each shadow has the size $|I|/k$.

Proof: As mentioned above, when there are k shadows, we can recover the encrypted image and extract the key from the encrypted image. By using the encrypted image and the key, the modified I', which is almost the same to I, can be recovered. On the other hand, from Section II, because $CS(\cdot)$ does not have perfect security, we can obtain partial encrypted pixels from less than k shadows, *e.g.*, $(k-1)$ shadows. However, it is worth noting that the key cannot be extracted from partial encrypted pixels. Therefore, without the complete key, we cannot obtain any original information of secret image from $(k-1)$ shadows. Therefore, we can conclude that it is a (k, n)-threshold scheme, and is computationally secure.

The modified scheme embeds the key into encrypted image by changing LSB of a small part of pixels in the secret image. The changed secret image has the same size with the original secret image. Thus, the shadow size of this scheme is the same with that of Thien and Lin's scheme, *i.e.*, $|I|/k$.

V. CONCLUSION

Because all coefficients of $(k-1)$-degree polynomial are used for embedding secret image pixels and permutation-only ciphers are insecure, in all of the existing (k, n)-SIS schemes, one may recover some partial secret pixels from $(k-1)$ shadows. Thus, the threshold properties of those schemes

are compromised. In this paper, we address this weakness, and propose a (k, n)-SIS scheme based on encrypted pixels. Moreover, by slightly modifying the secret image, we propose a modified (k, n)-SIS scheme with the same shadow size of Thien and Lin's scheme. Both schemes are proved to be computationally secure.

REFERENCES

[1] Z. L. Zhou, Q. M. J. Wu, C.-N. Yang, X. Sun, and Z. Pan, "Coverless image steganography using histograms of oriented gradients-based hashing algorithm," *J. Internet Technol.*, vol. 18, no. 5, pp. 1177–1184, Sep. 2017.

[2] Z. Zhou, Y. Wang, Q. M. J. Wu, C.-N. Yang, and X. Sun, "Effective and efficient global context verification for image copy detection," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 1, pp. 48–63, Jan. 2017.

[3] Z. Zhou, Q. M. J. Wu, F. Huang, and X. M. Sun, "Fast and accurate near-duplicate image elimination for visual sensor networks," *Int. J. Distrib. Sens. Netw.*, vol. 13, no. 2, pp. 1–12, Feb. 2017, doi: 10.1177/1550147717694172

[4] L. Xiong, Z. Xu, and Y.-Q. Shi, "An integer wavelet transform based scheme for reversible data hiding in encrypted images," *Multidimensional Syst. Signal Process.*, pp. 1–12, May 2017, doi: 10.1007/s11045-017-0497-5

[5] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[6] C.-C. Thien and J.-C. Lin, "Secret image sharing," *Comput. Graph.*, vol. 26, no. 5, pp. 765–770, Oct. 2002.

[7] C.-C. Lin and W.-H. Tsai, "Secret image sharing with steganography and authentication," *J. Syst. Softw.*, vol. 73, no. 3, pp. 405–414, Nov./Dec. 2004.

[8] C.-N. Yang, T.-S. Chen, K. H. Yu, and C.-C. Wang, "Improvements of image sharing with steganography and authentication," *J. Syst. Softw.*, vol. 80, no. 7, pp. 1070–1076, Jul. 2007.

[9] C.-C. Chang, Y.-P. Hsieh, and C.-H. Lin, "Sharing secrets in stego images with authentication," *Pattern Recognit.*, vol. 41, pp. 3130–3137, Oct. 2008.

[10] C.-N. Yang, J.-F. Ouyang, and L. Harn, "Steganography and authentication in image sharing without parity bits," *Opt. Commun.*, vol. 285, no. 7, pp. 1725–1735, Apr. 2012.

[11] S.-J. Lin, L. S.-T. Chen, and J.-C. Lin, "Fast-weighted secret image sharing," *Opt. Eng.*, vol. 48, no. 7, pp. 077008-1–077008-7, Jul. 2009.

[12] C.-N. Yang, P. Li, C.-C. Wu, and S.-R. Cai, "Reducing shadow size in essential secret image sharing by conjunctive hierarchical approach," *Signal Process. Image Commun.*, vol. 31, pp. 1–9, Feb. 2015.

[13] Y.-Y. Lin and R.-Z. Wang, "Scalable secret image sharing with smaller shadow images," *IEEE Signal Process Lett.*, vol. 17, no. 3, pp. 316–319, Mar. 2010.

[14] C.-N. Yang and Y.-Y. Chu, "A general *(k, n)* scalable secret image sharing scheme with the smooth scalability," *J. Syst. Softw.*, vol. 84, no. 10, pp. 1726–1733, Oct. 2011.

[15] A. Jolfaei, X.-W. Wu, and V. Muthukkumarasamy, "On the security of permutation-only image encryption schemes," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 2, pp. 235–246, Feb. 2016.

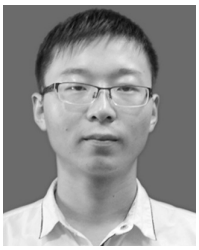
[16] C.-N. Yang, W.-J. Chang, S.-R. Cai, and C.-Y. Lin, "Secret image sharing without keeping permutation key," in *Proc. Int. Conf. Commun. Technol.*, 2014, pp. 410–416.

ZHILI ZHOU received the B.S. degree in communication engineering from Hubei University in 2007 and the M.S. and Ph.D. degrees in computer application from the School of Information Science and Engineering, Hunan University, in 2010 and 2014, respectively.

He is an Associate Professor with the School of Computer and Software, Nanjing University of Information Science and Technology, China. He is currently a Post-Doctoral Fellow with the Department of Electrical and Computer Engineering, University of Windsor, Canada. His current research interests include near-duplicate image/video retrieval, image search, image/video copy detection, coverless information hiding, digital forensics, and image processing.

CHING-NUNG YANG received the B.S. and M.S. degrees in telecommunication engineering from National Chiao Tung University, Hsinchu, Taiwan, in 1983, and 1985, respectively, and the Ph.D. degree in electrical engineering from National Cheng Kung University, Tainan, Taiwan, in 1997.

He is currently a Full Professor with the Department of Computer Science and Information Engineering, National Dong Hwa University, Hualien, Taiwan. His research interests include coding theory, information security, and cryptography.



YI CAO received the B.E. degree from the Nanjing University of Information Science and Technology, China, in 2016. He is currently pursuign the M.S. degree with the Nanjing University of Information Science and Technology, China. His research interests include network and information security.

XINGMING SUN received the B.S. degree in mathematics from Hunan Normal University, China, in 1984, the M.S. degree in computing science from the Dalian University of Science and Technology, China, in 1988, and the Ph.D. degree in computing science from Fudan University, China, in 2001. He is currently a Professor with the College of Computer and Software, Nanjing University of Information Science and Technology, China. In 2006, he visited University College London, U.K., he was a Visiting Professor with the University of Warwick, U.K., from 2008 to 2010. His research interests include network and information security, database security, and natural language processing.