Journal of Information Hiding and Multimedia Signal Processing ©2013 ISSN 2073-4212
Ubiquitous International Volume **4**, Number **4**, October **2013**

On the feasibility and security of image secret sharing scheme to identify cheaters

Qian Kong, Peng Li and Yanpeng Ma

Department of Mathematics and Physics
North China Electric Power University
Baoding, Hebei, 071003 China
qiankongkong@126.com; lphit@163.com; yanpengma@163.com

Receied September, 2012; revised April, 2013

Abstract. *Zhao et al. [A new image secret sharing scheme to identify cheaters, Computer Standards & Interfaces, vol.*31*, no.*1*, pp.*252 − 257*, 2009] proposed a (t, n) threshold image secret sharing scheme to identify cheaters. The scheme is based on Thien-Lin scheme and the intractability of discrete logarithm. It allows honest participants to identify cheaters, and each participant only needs to save her/his own secret shadow. Unfortunately, their scheme has a serious feasibility problem, and is insecure for image sharing. In this paper, the feasibility and security of the scheme are analyzed. It is proved that the scheme may be infeasible with probability* $1 - 251!/(251^n(251-n)!)$*. This probability increases with larger value of n, and reaches* 96.26% *when n is equal to* 40*. We also prove that the scheme is easy to crack when it is suffered from a brute force attack, especially when t is a small integer. The main weaknesses of feasibility and security are proved and shown by theoretical analysis and some experiments.*
Keywords: Image secret sharing; verification; infeasible probability; brute force attack

1. **Introduction.** The effective and secure protections of secret information are primary concerns in commercial, medical and military systems. Many image-protection techniques, such as encryption [1-3] and steganography [4,5], have been proposed to increase the security of secret images. However, a common weakness of these techniques is that the entire secret image is maintained in a single information-carrier. For example, the secret image cannot be recovered if the encrypted content is lost or modified during the transmission. To solve this security problem, secret image sharing method might be one of the possible solutions. It works by sharing a secret image among a set of participants. Only certain subsets of participants can cooperate to reconstruct the secret image.

The concept of the (t, n) threshold secret sharing scheme was introduced independently by Shamir [6] and Blakley [7] in 1979. The secret data is first encoded into n shares. In the revealing process, any t ($t \leq n$) or more shares can be collected to reconstruct the secret. However, any $t-1$ or fewer shares can get no information about the secret. In 1994, Naor and Shamir [8] proposed (t, n) threshold visual cryptography for image secret sharing, which is based on the human visual system. In a (t, n) threshold visual cryptography scheme, a binary secret image is encrypted into n shares printed on transparencies. Each transparency only has black pixels and transparent pixels. Superimposing any t transparencies makes the secret image recognizable by human eyes. Many image secret sharing schemes [9-11] have been proposed based on visual cryptography for different application. However, in these schemes, these schemes have disadvantages of size expansion

and low contrast of the revealed secret image. Thien and Lin [12] proposed a new image secret sharing method. The essential idea is to use a $(t-1)$ degree polynomial to construct n shadow images. The scheme has the property of small size of shadow images. Many researchers proposed secret sharing schemes based on polynomial [13-14]. Unfortunately, these image secret sharing schemes do not have the property of verification. The schemes face the problem of cheating by participants. There were some other image secret sharing schemes for improving security and efficiency [15-17].

In [18], Zhao et al. proposed an image secret sharing scheme to identify cheaters, called ZZDZ scheme. ZZDZ scheme is based on Thien-Lin scheme and the intractability of discrete logarithm. It is claimed that the scheme can identify the cheaters no matter if she/he is the original secret image holder or a participant. In ZZDZ scheme, each participant chooses her/his own secret shadow, and there is no secret communication between the holder and the participants. The generated shadow images are made public, so the participants do not need to save shadow images. However, a secret sharing scheme is feasible only when the infeasible probability is taken as feasibility benchmark. Also, the scheme should resist most of the attacks. Based on these observations, the feasibility and security of ZZDZ scheme should be further analyzed.

The feasibility and security analysis of ZZDZ scheme is conducted in this paper. The rest of this paper is organized as follows: a brief review of ZZDZ scheme is given in Section 2. In Section 3, we theoretically analyze the feasibility and security of ZZDZ scheme. Some experiments are conducted to verify the theoretic results in Section 4. Finally, a conclusion is drawn in Section 5.

2. Review of ZZDZ scheme.

In this section, we briefly review ZZDZ scheme. In ZZDZ scheme, The original secret image holder H divides the original secret image P into n shadow images $P_1, P_2, \ldots, P_n$, then assign these n shadow images to n participants $M_1, M_2, \ldots, M_n$. The scheme contains three phases: Initialization phase, Construction phase and Reconstruction & Verification phase.

2.1. Initialization phase.

1) H chooses two prime numbers p and q, and computes $N = p.q$. Both p and q should satisfy the properties as the two primes used in RSA cryptosystem which can prevent anybody factor N efficiently.

2) H chooses an integer $g \in [N^{1/2}, N]$, such that g is relatively prime to p and q. Publishes $\{g, N\}$.

3) Each participant $M_i \in M$ randomly chooses her/his own secret shadow $s_i \in [2, N]$, and computes $R_i = g^{s_i} mod N$. Then M_i provides R_i to H. H must ensure that $R_i \neq R_j$, where $i \neq j$. Once $R_i = R_j$, H should demand M_i to choose new s_i. Finally, publishes R_i.

2.2. Construction phase.

1) H randomly chooses an integer $s_0 \in [2, N]$ such that s_0 is prime to $(p-1)$ and $(q-1)$. Then H computes f and makes $s_0 \times f = 1 \mod \varphi(N)$, where $\varphi(N)$ is the Euler phi-function.

2) H computes $R_0 = g^{s_0} \mod N$ and $I_i = R_i^{s_0} \mod N$. Publishes $\{R_0, f\}$.

3) Divide the secret image P into several sections. Each section contains t pixels, and each pixel of the secret image belongs to one and only one section.

4) For the section j, H constructs $(t-1)$ degree polynomial as follows:

$$h_j(x) = (b_0 + b_1 x + \ldots + b_{t-1} x^{t-1}) \mod 251 \tag{1}$$

Here $b_0, b_1, \ldots, b_{t-1}$ are the t pixels of the section j.

5) H evaluates $y_{ij} = h_j(I_i)$, $i = 1, 2, \ldots, n$. Assigns these n values $y_{1j}, y_{2j}, \ldots, y_{nj}$ to n shadow images $P_1, P_2, \ldots, P_n$ as the j-th pixel respectively.

6) H repeats steps 4) and 5), until all sections of secret image P are processed. Publishes n shadow images $P_1, P_2, \ldots, P_n$.

2.3. **Reconstruction & Verification phase.** Without loss of generality, the members of $M^{'} = M_1, M_2, \ldots, M_t$ can reconstruct the secret image P.

1) Each participant $M_i \in M^{'}$ computes her/his sub-secret $I_i^{'} = R_0^{s_i} \mod N$, where s_i is the secret shadow of M_i.

2) Verify $I_i^{'}$ provided by M_i: if $I_i^{'f} = R_i \mod N$, then $I_i^{'}$ is true; otherwise $I_i^{'}$ is false and M_i may be a cheater.

3) Reconstruct the secret image P: with the knowledge of t pairs of $(I_i^{'}, y_{ij})$ and the Lagrange interpolating polynomial, a $(t-1)$ degree polynomial can be uniquely determined as follows:

$$\begin{aligned} h_j(x) &= \sum_{i=1}^{t} y_{ij} \prod_{k=1,k\neq i}^{t} \frac{x - I_k^{'}}{I_i^{'} - I_k^{'}} \mod 251 \\ &= (b_0 + b_1 x + \ldots + b_{t-1} x^{t-1}) \mod 251 \end{aligned} \tag{2}$$

The coefficients $b_0, b_1, \cdots, b_{t-1}$ are the corresponding t pixel values of section j in P.

4) Repeat step 3), until all sections of secret image P are reconstructed.

3. Performance analysis.

3.1. **Preliminary knowledge.** Before the feasibility and security analysis, we introduce some elementary concepts in number theory.

Definition 3.1. [19] *Let $m > 0$. We write $a \equiv b \ (mod\ m)$ if $m|a-b$ and we say that a is congruent to b modulo m. Here m is said to be the modulus of the congruence.*

It is easy to prove that congruence is an equivalence relation.

Definition 3.2. [19] *Let $m > 0$ be given. For each integer a we define*

$$[a] = \{x : x \equiv a (mod\, m)\}$$

In other words, $[a]$ is the set of all integers that are congruent to a modulo m. We call $[a]$ the residue class of a modulo m. (For more information, please see Chapter 19 in [19]) In elementary algebra, the binomial theorem describes the algebraic expansion of powers of a binomial. According to the theorem, it is possible to expand any power of $(x + y)$ into a sum of the form:

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$$

Where $\binom{n}{k} = n!/(k!(n-k)!)$ denotes the corresponding binomial coefficient.

3.2. **Feasibility analysis.** Although Zhao et al. proved the feasibility of generation and verification process in [18], they did not analyze the feasibility of the polynomial-based secret sharing scheme, which is not the same as Shamirs scheme. It is claimed in [18] that ZZDZ scheme is $a(t, n)$ threshold scheme, which means any t participants can cooperate to reconstruct the secret image. However, its not always true. There is a situation where t participants cannot get the secret image. In this subsection, the feasibility of ZZDZ scheme is further discussed.

Proposition 3.1. *For any integer $a \in \{0, 1, \ldots, N-1\}$, $c = a \, mod \, 251$.then $h_j(a) = h_j(c)$ in Equation(1) with any section j.*

Proof: For any integer $a \in \{0, 1, \ldots, N-1\}$,let $c = a \, mod \, 251$.So a can be written in the form of $a = 251k + c$,where k is an integer and $c \in \{0, 1, \ldots, 250\}$.By binomial theorem,$a^p = (251k + c)^p = \sum_{l=0}^{p} \binom{p}{l} (251k)^{p-l} c^l$,for any $p \in \{1, 2, \ldots, t-1\}$. thus

$$\begin{aligned} b_p a^p \, mod \, 251 &= (\sum_{l=0}^{p} \binom{p}{l} b_p (251k)^{p-l} c^l) mod \, 251 \\ &= (\sum_{l=0}^{p-1} \binom{p}{l} b_p (251k)^{p-l} c^l + b_p c^p) mod \, 251 \\ &= b_p c^p mod \, 251 \end{aligned}$$

Therefore,

$$\begin{aligned} h_j(a) &= (b_0 + b_1 a + \cdots + b_{t-1} a^{t-1}) mod 251 \\ &= b_0 mod 251 + b_1 a mod 251 + \cdots + b_{t-1} a^{t-1} mod 251 \\ &= b_0 mod 251 + b_1 c mod 251 + \cdots + b_{t-1} c^{t-1} mod 251 \\ &= (b_0 + b_1 c + \cdots + b_{t-1} c^{t-1}) mod 251 = h_j(c) \end{aligned}$$

Proposition 3.2. *For any integer $a, b \in \{0, 1, \ldots, N-1\}$, if $a \equiv b (\mathrm{mod}\, 251)$,then the two shadow images generated with a and b by Equation(1) respectively, are identical.*

Proof: For any section j, let $c = a \, mod \, 251$. By Proposition 3.1,$h_j(a) = h_j(c)$. Since $a \equiv b (mod \, 251)$,b mod 251 is also equal to c. Also by Proposition 3.1, $h_j(b) = h_j(c)$. Therefore,$h_j(a) = h_j(b)$.Because $h_j(a)$ and $h_j(b)$ are assigned to two shadow images as the jth pixel respectively, the two shadow images have the same value of the jth pixel. Since for each section j,$h_j(a) = h_j(b)$, two shadow images generated with a and b by Equation (1) are identical.

Actually, in ZZDZ scheme,$I_i = R_i^{s_0} \mod N$,$i = 1, 2, \ldots, n$.So $I_i \in \{0, 1, \ldots, N-1\}$. Suppose $I_i \equiv I_j (\mathrm{mod}\ 251)$,that is, I_i and I_j both belong to residue class $[c]$ modulo 251, where $c = a \, mod \, 251$. By Proposition 3.2, two generated shadow images with I_i and I_j are identical. So in the reconstruction phase, the participants M_i and M_j can be treated as one participant. Therefore, if both M_i and M_j belong to a group with t participants, this group is infeasible to reconstruct the original secret image. Proposition 3.3 shows more theoretic analysis.

Proposition 3.3. *Let $M' = \{M_1, M_2, \ldots, M_t\}$ be a subset of all participants, and $a, b \in \{1, 2, \ldots, t\}$. If both the computed sub-secrets I_a' and I_b' belong to the residue class $[c]$ modulo 251, where $c = I_a' \, \mathrm{mod}\, 251$, then the probability of correctly reconstructing the original secret image is $(1/251)^{L \times W/t}$ at most, where $L \times W$ is the size of the secret image.*

Proof: With the correct secret shadows, the computed sub-secret I_i' is equal to I_i(proved in [18]). Without loss of generality, let us inspect how $h_j(x)$(for section j of the secret image) can be revealed. From Equation (1), to solve the t coefficients $b_0 \sim b_{t-1}$, we need t equations. Since the members of participants $M' = \{M_1, M_2, \ldots, M_t\}$ cooperate to reveal the secret image, with the knowledge of t pairs of $(I_i', h_j(I_i'))$, we can construct t equations in the form of:

$$(b_0 + b_1 I_i' + \cdots + b_{t-1} I_i'^{t-1}) \, mod \, 251 = h_j I_i'$$

Because the computed sub-secrets $I_a^{'}$ and $I_b^{'}$ both belong to the residue class $[c]$ modulo 251, by Proposition 3.2, we have:

$$\begin{aligned} h_j(I_a^{'}) &= (b_0 + b_1 I_a^{'} + \cdots + b_{t-1} I_a^{'t-1}) \; mod \; 251 \\ &= (b_0 + b_1 c + \cdots + b_{t-1} c^{t-1}) \; mod \; 251 \\ &= (b_0 + b_1 I_b^{'} + \cdots + b_{t-1} I_b^{'t-1}) \; mod \; 251 \\ &= h_j(I_b^{'}) \end{aligned}$$

Then, the two equations generated with pairs $(I_a^{'}, h_j(I_a^{'}))$ and $(I_a^{'}, h_j(I_b^{'}))$ are identical. Therefore, there are actually $t-1$ equations constructed. With these $t-1$ equations to solve the t coefficients in Equation (1) for section j, there are at least 251 possible solutions with equal probability. The probability of guessing the right solution is $1/251$ at most. Since there are $L \times W/t$ sections, the probability of correctly reconstructing the secret image is at most $(1/251)^{L \times W/t}$.

For example, suppose the secret image has 256×256 pixels, the members of participants $M^{'} = \{M_1, M_2, \ldots, M_t\}$ will cooperate to reconstruct the secret image. If there are two participants whose sub-secrets belong to a same residue class modulo 251, the probability of obtaining the correct image is just $(1/251)^{256 \times 256/t}$. Since $(1/251)^{256 \times 256/t}$ is a very small number, the members of participants $M^{'} = \{M_1, M_2, \ldots, M_t\}$ have almost no chance to obtain the correct secret image. Indeed, if there are $r (2 \leq r \leq t)$ participants whose sub-secrets belong to a same residue class modulo 251, the probability of correctly reconstructing the secret image is $(1/251)^{(r-1)L \times W/t}$.

By Proposition 3.3 ,a (t, n) threshold ZZDZ scheme is feasible only when all computed sub-secrets belong to different residue classes modulo 251. So the feasible choices of sub-secrets are $P(251, n) = 251!/(251-n)!$. Therefore, the infeasible probability of ZZDZ scheme is $P_{inv} = 1 - 251!/(251^n(251-n)!)$. The bigger n adopted in the scheme, the bigger infeasible probability has the scheme. Table 1 shows the infeasible probability with different n in ZZDZ scheme. As shown in Table 1, the infeasible probability reaches 96.26% when n is 40.

TABLE 1. The infeasible probability with different n in the ZZDZ scheme

n	2	3	5	10	20	30	40
Infeasible probability	0.40%	1.19%	3.93%	16.61%	54.04%	83.56%	96.26%

3.3. **Security analysis.** With secret protection in mind, a secret sharing scheme should resist most of the cryptanalytic attacks, and the key space should be large enough to make brute force attacks infeasible. In ZZDZ scheme, the generated shadow images are made public. Therefore, the security relies on the protection of n secret shadows held by n participants. Any t of the n participants with their secret shadows can reconstruct the secret image. Since $s_i \in [2, N]$,the possible combinations of any t secret shadows is $(N-1)^t$. However, the possible solutions to reveal secret image can be reduced significantly. In Proposition 3.4, we show that ZZDZ scheme can be cracked within limited solutions by a brute force attack.

Proposition 3.4. *By a brute force attack,a (t, n) threshold ZZDZ scheme can be cracked, within $P(251, t) = 251!/(251-t)!$ possible solutions.*

Proof: In the reconstruction phase, the participants provided their sub-secrets by computing $I_i^{'} = R_0^{s_i} \bmod N$. Without loss of generality, the members of participants

$M_1, M_2, \ldots, M_t$ should reconstruct the secret image. With t pairs of $(I_i^{'}, h_j(I_i^i))$, we can construct t equations to solve t coefficients $b_0 \sim b_{t-1}$ in Equation (1) for section j of the secret image. Let $c_i = I_i^{'} \bmod 251$, by Proposition 3.1, we have

$$\begin{aligned} h_j(I_i^{'}) &= (b_0 + b_1 I_i^{'} + \cdots + b_{t-1} I_i^{'t-1}) \; mod \; 251 \\ &= (b_0 + b_1 c_i + \cdots + b_{t-1} c_i^{t-1}) \; mod \; 251 \\ &= h_j(c_i) \end{aligned}$$

Therefore, we can construct equations with pairs of $(c_i, h_j(c_i))$ instead of $(I_i^{'}, h_j(I_i^{'}))$ Since $c_i \in 0, 1, \ldots, 250$, without $I_i^{'}$, the possible choice of c_i for participants M_i is 251. By Proposition 3.3, the scheme is feasible only when all sub-secrets belong to different residue classes modulo 251. So the possible combinations of t pairs of (c_i, y_i) are $P(251, t) = 251!/(251 - t)!$ Therefore, the scheme can be cracked by a brute-force attack within $251!/(251 - t)!$ possible solutions.

Actually,$251!/(251-t)!$ is not big enough as a key space for secret protection, especially when t is a small integer. ZZDZ scheme can be cracked simply by a brute-force attack within limited CPU time.

4. **Experimental results.** In this section, the weakness mentioned in Section 3 is shown by conducting the following experiments.

Experiment 1: To demonstrate the property of Proposition 3.3, a counter experiment is shown by $a(2, 3)$-threshold ZZDZ scheme. For simplicity, let $p = 89, q = 103$, then $N = pq = 9167$. Let $g = 269$. Choose integer $s_0 = 1723$, then $f = 547$ which makes $s_0 \times f = 1 \bmod \varphi(N)$. Three secret shadows $s_i (i = 1, 2, 3)$ and the computed values R_i, I_i and I_i mod 251 are shown in Table 2.

TABLE 2. Three secret shadows s_i and the computed values R_i, I_i, and I_i mod 251

i	1	2	3
s_i	1347	1625	1823
R_i	4838	701	7999
I_i	7836	5075	1604
I_i mod 251	55	55	98

In Fig. 1, a) shows the original secret image with 256×256 pixels; b)-d) are three shadow images generated by different secret shadows. As shown in Table 1, both I_1 mod 251 and I_2 mod 251 are equal to 55. The generated shadow image 1 and shadow image 2 are identical. Therefore, with the cooperation of participants 1 and 2, there is no sufficient information to reconstruct the secret image. This experimental result is guaranteed by Proposition 3.2.

Since the security of the scheme is based on RSA cryptosystem, the secret shadows should be typically 1024-2048 bits long. However, because the weaknesses mentioned above do not dependent on the length of the secret shadows, this experiment only take small value of N.

Experiment 2: To demonstrate the weakness of the security, we attack ZZDZ scheme by a brute-force attack. The experiment is done on the platform environment as: lenovo ThinkPad T61 with Intel Core2Duo 2.40GHz CPU, OS of Windows XP, 2.0Gbytes RAM,

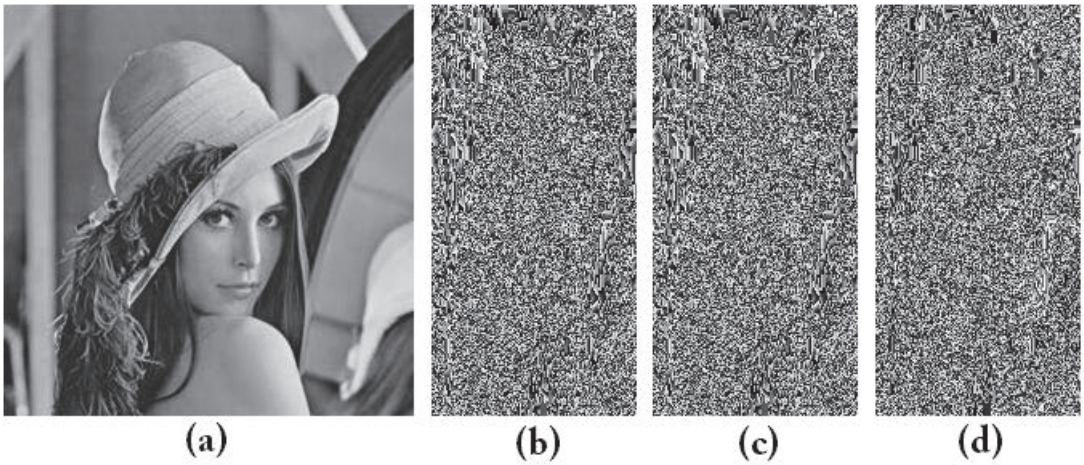

FIGURE 1. The experiment of image Lena. a) shows the original secret image with 256×256 pixels; b)-d) are three shadow images generated by secret shadow $s_1 = 1347$, $s_2 = 1625$ and $s_3 = 1823$, respectively.

and MATLAB 6.5.1 programming in use. In this experiment, shadow images 1 and 3 in Fig. 1 are chosen to reconstruct the secret image. With the correct secret shadows s_1 and s_3 , the secret image can be reconstructed in 0.094 second. Under a brute force attack by testing all possible combinations of $I_1^{'}$ and $I_3^{'}$ in the range of $\{0, 1, \ldots, 250\}$, the expected time to crack the scheme successfully is about 14 minutes. In another experiment of $(3, 5)$ threshold ZZDZ scheme on Lena image with 256×256 pixels, a brute force attack would be expected to reconstruct the secret image successfully in 440 hours.

Since the original secret is a natural image, it is easy to recognize the correct secret image by the correlations of adjacent pixels in the reconstructed images. If the chosen sub-secrets are not correct, the reconstructed image is like noise and meaningless, then the correlation coefficient of adjacent pixels is near to zero. In the correctly reconstructed image, the correlation coefficient is near to one.

Actually, the bigger t adopted in the scheme, the longer time needed to crack the scheme with a brute force attack. However, the scheme is not secure enough, especially when the threshold of the scheme is a small integer.

5. **Conclusions.** In this paper, we give a detailed analysis about the feasibility and security of ZZDZ scheme. It is proved that ZZDZ scheme may be infeasible with probability $1 - 251!/(251^n(251 - n)!)$. This probability increases with the big value of n, and reaches 96.26% when n is equal to 40. We also prove that the scheme cannot resist a brute force attack, especially when the threshold is a small integer. A (2, 3) threshold scheme can be cracked within 14 minutes in our experiment on the image Lena with 256×256 pixels. Theoretical analysis and experimental results prove these weaknesses. Therefore, ZZDZ scheme is insecure for secret sharing. A secure image secret sharing scheme to detect dishonest participant is still a challenge work in future.

Acknowledgment. This work is partially supported by the Fundamental Research Funds for the Central Universities (No.13MS107). The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

REFERENCES

[1] Z. Guan, F. Huang, and W. Guan, Chaos-based image encryption algorithm, *Journal of Physics Letters A*, vol. 346, no. 1-3, pp. 153-157, 2005.
[2] N. K. Pareek, V. Patidar, and K. K. Sud, Image encryption using chaotic logistic map, *Journal of Image and Vision Computing*, vol. 24, no. 9, pp. 926-934, 2006.
[3] T. Gao, and Z. Che, Image encryption based on a new total shuffling algorithm, *Chaos, Solitons & Fractals*, vol. 38, no. 1, pp. 213-220, 2008.
[4] M. Y. Wu, Y. K. Ho, and J. H. Lee, An iterative method of palette-based image steganography, *Journal of Pattern Recognition Letters*, vol. 25, no. 3, pp. 301-309, 2004.
[5] C. L. Liu, and S. R. Liao, High-performance JPEG steganography using complementary embedding strategy, *Journal of Pattern Recognition*, vol. 41, no. 9, pp. 2945-2955, 2008.
[6] A. Shamir, How to share a secret, *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, 1979.
[7] G. R. Blakley, Safeguarding cryptographic keys, *Proceedings of the National Computer Conference*, pp. 313-317, 1979.
[8] M. Naor, and A. Shamir, *Visual cryptography*, LNCS 950, springer, pp. 1-12, 1995.
[9] C. C. Lin, and W. H. Tsai, Visual cryptography for gray-level images by dithering techniques, *Journal of Pattern Recognition Letters*, vol. 24, no. 1-3, pp. 349-358, 2003.
[10] C. N. Yang, and T. S. Chen, Colored visual cryptography scheme based on additive color mixing, *Journal of Pattern Recognition*, vol. 41, no. 10, pp. 3114-3129, 2008.
[11] J. B. Feng, H. C. Wu, C. S. Tsai, Y. F. Chang, and Y. P. Chu, Visual secret sharing for multiple secrets, *Journal of Pattern Recognition*, vol. 41, no. 12, pp. 3572-3581, 2008.
[12] C. C. Thien, J. C. Lin, Secret image sharing, *Jpurnal of Computer & Graphics*, vol. 26, no. 5, pp. 765-770, 2002.
[13] J. B. Feng, H. C. Wu, C. S. Tsai, and Y. P. Chu, A new multi-secret images sharing scheme using Largranges interpolation, *Journal of Systems and Software*, vol. 76, no. 3, pp. 327-339, 2005.
[14] Y. S. Wu, C. C. Thien, and J. C. Lin, Sharing and hiding secret images with size constraint, *Journal of Pattern Recognition*, vol. 37, no. 7, pp. 1377-1385, 2004.
[15] C. S. Chan, C. C. Chang, and H. P. Vo, A user-friendly image sharing scheme using JPEG-LS median edge predictor, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 3, no. 4, pp. 340-351, 2012.
[16] Z. H. Wang, C. C. Chang, H. N. Tu, and M. C. Li, Sharing a secret image in binary images with verification, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 2, no. 1, pp. 78-90, 2011.
[17] R. Nishimura, S. I. Abe, N. Fujita, and Y. Suzuki, Reinforcement of VoIP security with multipath routing and secret sharing scheme, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 1, no. 3, pp. 204-219, 2010.
[18] R. Zhao, J. J. Zhao, F. Dai, and F. Q. Zhao, A new image secret sharing scheme to identify cheaters, *Journal of Computer Standards & Interfaces*, vol. 31, no. 1, pp. 252-257, 2009.
[19] W. E. Clark, *Elementary Number Theory*, Department of Mathematics, University of South Florida, USA, 2003.